REVIEW ON ROLE-BASED ACCESS CONTROL (RBAC) AND THIRD-PARTY AUDITING (TPA) BASED SECURITY

Ved Prakash Khatik[1], Suraj Yadav[2]
M. Tech Scholar[1], Assistant Professor[2]
[1,2]Department of Computer Science, Jagannath University Jaipur (Rajasthan)

Abstract: Role-Based Access Control (RBAC) and Third-Party Auditing (TPA) are two significant approaches utilized in information security to establish effective access control and accountability across various systems and applications. RBAC offers a structured framework for managing access privileges based on user roles, while TPA involves independent auditing by a third party to ensure compliance and reinforce security measures. This research paper aims to provide a comprehensive examination of RBAC and TPA-based security, encompassing their underlying principles, advantages, challenges, and recent advancements. Additionally, it explores the potential synergies and integration of RBAC and TPA to bolster overall security and address potential vulnerabilities. The insights derived from this review will benefit researchers, practitioners, and decision-makers by providing a deep understanding of the strengths and limitations of RBAC and TPA, aiding in the design of robust security protocols.

Keywords: Role Based Access, RBAC, TPA

1. INTRODUCTION

In today's age of ubiquitous information systems and widespread data sharing, ensuring proper access control and maintaining security has become of utmost importance. Unauthorized access to sensitive information can result in data breaches, privacy violations, and significant financial losses. To tackle these challenges and enhance system security, two prominent approaches are widely employed: Role-Based Access Control (RBAC) and Third-Party Auditing (TPA). [1]

RBAC provides a structured framework for managing access privileges based on users' roles within an organization. By assigning permissions to roles rather than individual users, RBAC offers a flexible and scalable approach that simplifies the administration of access control. Extensively researched and deployed in various domains, such as healthcare, finance, and government sectors, RBAC models and architectures have proven to be effective in ensuring secure information access. [1]

On the other hand, TPA involves independent auditing by a third party to assess the compliance and security of a system or organization. This auditing process evaluates whether the implemented security measures align with established standards and regulations. TPA adds transparency, accountability, and confidence to an organization's security posture through an external evaluation. [2]

The objective of this paper is to provide a comprehensive review of RBAC and TPA-based security, delving into their underlying principles, advantages, challenges, and recent advancements. By examining the strengths and limitations of RBAC and TPA, the paper aims to shed light on their individual contributions to information security. Furthermore, it investigates the potential synergies and integration of RBAC and TPA to achieve enhanced security measures, effectively addressing vulnerabilities that may arise when using either approach independently. [2]

2. ROLE-BASED ACCESS CONTROL (RBAC)

2.1 Definition and Components of RBAC

Role-Based Access Control (RBAC) is a widely adopted access control mechanism that provides a structured approach to managing access privileges in computer systems and applications. Instead of assigning permissions directly to individual users, RBAC assigns permissions to roles, simplifying the administration of access control in complex environments. The key components of RBAC include: [3]

2.1.1 Roles:

Roles represent collections of permissions or activities grouped based on common job functions or responsibilities within an organization. Roles are defined based on the tasks and responsibilities associated with specific user roles. [3]

2.1.2 Permissions:

Permissions define the actions or operations that can be performed on system resources. These can include read, write, execute, create, delete, or modify permissions, among others.

2.1.3 Users:

Users are individuals who interact with the system and are assigned specific roles based on their job functions or responsibilities within the organization.

2.1.4 Relationships:

RBAC establishes relationships between roles, permissions, and users. Users are assigned roles, and roles are associated with specific permissions. This relationship ensures that users inherit the permissions associated with their assigned roles. [3]

2.2 RBAC Models and Architectures

RBAC can be implemented using various models and architectures that define the structure and behavior of the RBAC system. Some commonly used RBAC models include: [4]

2.2.1 Hierarchical RBAC:

This model organizes roles in a hierarchical manner, where higher-level roles inherit permissions from lower-level roles. It provides a natural representation of organizational structures.

2.2.2 Static RBAC:

In this model, role assignments are fixed and do not change frequently. The permissions associated with roles are defined statically, and user-role assignments are typically made during the user provisioning process.

2.2.3 Dynamic RBAC:

Dynamic RBAC allows for more flexibility by enabling role changes and reassignments during runtime. Users can be assigned or removed from roles dynamically based on their changing responsibilities. [4]

2.2.4 Constraint-Based RBAC:

This model incorporates constraints that define additional conditions or rules for role activations or role permissions. Constraints can be used to enforce separation of duties or other security policies.

RBAC architectures provide guidelines and frameworks for implementing RBAC in a specific environment. Some commonly used RBAC architectures include NIST RBAC, ANSI RBAC, and Chinese Wall Model. [4]

2.3 Advantages and Limitations of RBAC

RBAC offers several advantages in managing access control:

- Simplified administration: RBAC reduces administrative overhead by centralizing permission management and simplifying user-role assignments. It allows for efficient role-based provisioning and deprovisioning of user accounts.
- Granular access control: RBAC enables fine-grained access control by defining permissions at the role level. This allows for more precise control over who can access specific resources and perform certain actions.
- Improved security: RBAC helps enforce the principle of least privilege by granting users only the permissions necessary for their roles. This reduces the risk of unauthorized access and potential misuse of privileges.
- Scalability: RBAC is scalable, making it suitable for organizations of varying sizes and complexities. It allows for easy role creation, modification, and assignment, accommodating changes in organizational structure and user responsibilities. [4]

However, RBAC also has some limitations:

- Role explosion: In large organizations with diverse roles, the number of roles can proliferate rapidly, leading to role explosion. Managing a large number of roles and their relationships can become challenging.
- Lack of context-awareness: RBAC primarily focuses on roles and permissions and may not consider contextual factors

such as time, location, or user attributes during access control decisions.

- Role creep and conflicts: Over time, roles may accumulate additional permissions, resulting in role creep. Role conflicts can also arise when a user is assigned conflicting roles that grant contradictory permissions.

2.4 RBAC Implementation Challenges

Implementing RBAC effectively can pose certain challenges:

- Role engineering: Designing and defining roles that accurately reflect user responsibilities and align with organizational needs requires thorough analysis and understanding of user tasks and system requirements.
- Role mapping and assignment: Mapping user roles to corresponding job functions and assigning roles to users can be complex, especially in large organizations with multiple departments and varying access requirements.
- Change management: Adapting RBAC to evolving organizational structures, user responsibilities, and system requirements requires effective change management processes to ensure the RBAC system remains up to date. [5]

2.5 Recent Advances in RBAC

RBAC continues to evolve with advancements in technology and emerging security requirements. Recent research and developments in RBAC include:

- Attribute-Based Access Control (ABAC): ABAC extends RBAC by incorporating user attributes as additional factors for access control decisions. This enables more fine-grained and context-aware access control.
- Risk-Based RBAC: This approach incorporates risk assessment and analysis to determine role assignments and permissions. It considers the sensitivity of resources and the potential impact of access decisions on system security.
- Hybrid RBAC models: Hybrid models combine RBAC with other access control mechanisms, such as attribute-based or rule-based access control, to provide enhanced security and flexibility.
- RBAC in cloud environments: Research has focused on adapting RBAC to cloud computing environments, addressing the challenges of multi-tenancy, scalability, and dynamic resource provisioning. [5]

3. THIRD-PARTY AUDITING (TPA)

3.1 Overview and Principles of TPA

Third-Party Auditing (TPA) is an independent assessment process that evaluates the compliance, security, and integrity of systems or organizations. It involves engaging an external auditing entity to provide an objective evaluation of security controls, policies, and practices. The key principles of TPA include: [6]

- Independence: The auditing entity must be independent and impartial, ensuring unbiased assessments and evaluations.

- Expertise: The auditors should possess the necessary knowledge, skills, and expertise in relevant security standards, regulations, and auditing methodologies.

- Objectivity: TPA should be conducted objectively, free from conflicts of interest or undue influence, to ensure fair and accurate evaluations.

- Transparency: The auditing process should be transparent, with clear communication of findings, recommendations, and remediation measures to the audited organization. [6]

3.2 TPA Process and Workflow

The TPA process typically follows a structured workflow with the following steps:

- Planning: Defining the scope, objectives, and criteria for the audit. Collaborating with the audited organization to establish an audit plan, including timelines and required resources.

- Pre-audit assessment: Conducting a preliminary assessment to gather information about the audited organization's security controls, policies, and practices. Identifying areas of focus and potential risks.

- On-site evaluation: Visiting the audited organization's premises to conduct on-site evaluations. Reviewing documentation, interviewing personnel, inspecting physical security measures, and assessing technical controls to determine compliance and security posture. [7]

- Data analysis: Analyzing collected data, comparing it against established standards, regulations, and best practices. Identifying areas of non-compliance, vulnerabilities, or weaknesses that require attention.

- Reporting: Preparing a comprehensive report summarizing findings, including identified deficiencies, risks, and recommendations for improvement. Assessing the organization's overall compliance and security effectiveness.

- Remediation and follow-up: The audited organization addresses identified deficiencies and implements remediation measures based on recommendations. Conducting follow-up assessments to verify the effectiveness of remediation efforts. [7]

3.3 Benefits and Challenges of TPA

TPA offers several benefits for organizations seeking to enhance security and compliance:

- Independent evaluation: TPA provides an unbiased assessment conducted by external experts, offering an objective view of security controls and compliance status.

- Accountability and transparency: TPA promotes accountability by holding organizations responsible for their security practices. The auditing process enhances transparency by providing stakeholders visibility into the organization's security posture.

- Compliance assurance: TPA helps ensure adherence to security standards, regulations, and industry best practices, reducing the risk of non-compliance and associated penalties.

- Risk identification and mitigation: TPA identifies vulnerabilities, weaknesses, and potential risks, enabling proactive mitigation and strengthening of security measures. [8]

However, TPA also presents some challenges:

- Cost and resource implications: TPA can be resource-intensive and require significant financial investment to engage reputable auditing entities. Organizations need to allocate resources for implementing remediation measures based on audit findings.

- Coordination and cooperation: Effective TPA requires close collaboration between auditors and the audited organization, with the organization providing necessary access, information, and cooperation throughout the auditing process.

- Scope and coverage limitations: TPA focuses on a specific period and scope defined in the audit plan, potentially overlooking emerging threats or evolving security challenges.[8]

3.4 TPA Standards and Compliance

TPA is guided by various standards, frameworks, and regulations that establish criteria for evaluation and compliance. Commonly referenced TPA standards include:

- ISO/IEC 27001: An international standard for establishing, implementing, maintaining, and continually improving an Information Security Management System (ISMS). TPA can assess compliance with ISO/IEC 27001 requirements.

- Payment Card Industry Data Security Standard (PCI DSS): A set of security standards for organizations handling cardholder information. TPA helps assess compliance with PCI DSS requirements for ensuring cardholder data security.

- General Data Protection Regulation (GDPR): GDPR outlines data protection and privacy requirements for organizations handling personal data of European Union citizens. TPA can assess compliance with GDPR regulations.

Compliance with these standards provides organizations with a framework to demonstrate their commitment to security and privacy best practices. [9]

3.5 Recent Developments in TPA

TPA continues to evolve in response to emerging security challenges and advancements in technology. Recent developments in TPA include:

- Continuous auditing: A shift towards near real-time auditing to provide more timely detection of security gaps and vulnerabilities.

- Automation and machine learning: Incorporation of automation and machine learning techniques to analyze large volumes of data, detect anomalies, and identify potential security threats more efficiently.

- Supply chain auditing: Expansion of TPA focus to include auditing security practices and compliance throughout the entire supply chain.

- Blockchain-based auditing: Exploration of blockchain technology to enhance the transparency and trustworthiness of auditing processes, providing immutable records and verifiable evidence of compliance.

These recent developments aim to enhance the effectiveness, efficiency, and relevance of TPA in addressing the evolving security landscape and meeting increasing demands for accountability and compliance. [10]

4. RELATED WORK

S. R. Shree et al., in their 2020 study [11], emphasize the significance of optimization in achieving accurate outcomes. They highlight the dependence of security measures for data stored in remote servers on secret keys used for encryption and decryption. Various cryptographic key generation algorithms, such as RSA and AES, are available for key production.

In another study by A. Thakare et al., in 2020 [12], the focus is on the Azure Internet of Things (IoT) platform. They discuss how tasks in Azure IoT are isolated within groups using job-based access control (RBAC), ensuring that clients are granted appropriate levels of access for specific tasks. However, they highlight that a similar validation and endorsement process is also applied based on the "type of customer," leading to additional strain on the cloud worker.

In the research conducted by H. Belkhiria et al. in 2020 [13], they discuss the increasing presence of Smart Living Spaces (SLS) in functional applications, including domestic devices and healthcare systems. SLS applications aim to improve users' quality of life by meeting their needs and promoting energy-efficient utilization in living spaces.

A. Suganthy and V. Prasanna Venkatesan, in their 2019 paper [14], explore RBAC models and their extensions in various contexts. They analyze the access control models, their applications, and limitations in practical scenarios, considering the dynamic roles that users acquire based on the context in which they make access requests. The main objective of their study is to examine different access control models and identify their applications and limitations in real-world scenarios.

Table 1. Approaches in Related Papers

Paper	Focus	Proposed Solution
S. R. Shree et al., 2020 [15]	Optimization for improved security in data storage	Technique based on cuckoo search algorithm (CSA) to enhance secrecy
A. Thakare, et al., 2020 [16]	Job-based access control in Azure IoT	Smart access control model designed for a large-scale clinical scenario in Azure IoT, addressing issues with RBAC structure and task management
H. Belkhiria, et al., 2020 [17]	Role-Based Access Control (RBAC) in Smart Building	RBAC with domains and a third-party evaluation engine to enforce authorized access to devices in a Smart Building
A. Suganthy and V. Prasanna Venkatesan, 2019 [18]	Analysis of RBAC models and their applications	Examination of RBAC models and their extensions, analyzing their applications and limitations in real-world scenarios

5. CONCLUSION

In an era where securing sensitive information and ensuring proper access control are of utmost importance, Role-Based Access Control (RBAC) and Third-Party Auditing (TPA) emerge as crucial components of information security. This comprehensive review provides a detailed examination of RBAC and TPA-based security, covering their fundamental principles, key components, advantages, limitations, implementation challenges, adherence to standards, and recent advancements.

RBAC offers a structured approach to access control by assigning permissions to roles instead of individual users. It simplifies administration, enables fine-grained access control, enhances security, and supports scalability. However, challenges such as role explosion, lack of context-awareness, and role creep must be carefully addressed during RBAC implementation.

TPA, on the other hand, provides an independent evaluation of an organization's security controls, compliance, and data integrity. TPA ensures accountability, transparency, and compliance assurance by identifying vulnerabilities and mitigating risks. Nonetheless, implementing TPA may involve costs, coordination, and limitations in terms of scope and coverage.

The integration of RBAC and TPA brings forth synergistic benefits by combining structured access control with independent auditing. The collaboration between RBAC and TPA can enhance security measures, providing a comprehensive approach to access control, accountability, and compliance.

Recent advancements in RBAC include Attribute-Based Access Control (ABAC), risk-based RBAC, and hybrid RBAC models, catering to evolving security requirements. TPA has witnessed developments in areas such as continuous auditing, automation, machine learning, supply chain auditing, and blockchain-based auditing. These advancements aim to improve efficiency, accuracy, and transparency in the auditing process.

As organizations face increasingly complex security challenges, understanding the principles, benefits, and limitations of RBAC and TPA becomes paramount. This comprehensive review serves as a valuable resource for researchers, practitioners, and decision-makers, providing guidance in designing robust security measures and making informed choices regarding RBAC, TPA, and their integration.

In conclusion, RBAC and TPA play vital roles in achieving secure and accountable access control in systems and organizations. The continuous evolution of RBAC and TPA, along with the potential for integration, offers promising avenues for advancing information security practices and safeguarding critical assets in an ever-changing threat landscape. By embracing these security measures and staying informed about emerging trends and developments, organizations can proactively protect their systems, data, and stakeholders from potential threats and vulnerabilities.

REFERENCES

1. C. Liu, S. Cheng, Y. Luo and F. Jiang, "Behavior Recognition Based on RBAC-Ensemble Model," *2019 11th International Conference on Knowledge and Smart Technology (KST)*, Phuket, Thailand, 2019, pp. 29-34.

2. M. Ghafoorian, D. Abbasinezhad-Mood and H. Shakeri, "A Thorough Trust and Reputation Based RBAC Model for Secure Data Storage in the Cloud," in *IEEE Transactions on Parallel and Distributed Systems*, vol. 30, no. 4, pp. 778-788, 1 April 2019.

3. Y. Zou, J. Deng, C. Xu, X. Liang and X. Chen, "Semantic Rule Based RBAC Extension Model for Flexible Resource Allocation," *2019 12th International Symposium on Computational Intelligence and Design (ISCID)*, Hangzhou, China, 2019, pp. 221-224.

4. K. Soni and S. Kumar, "Comparison of RBAC and ABAC Security Models for Private Cloud," *2019 International Conference on Machine Learning, Big Data, Cloud and Parallel Computing (COMITCon)*, Faridabad, India, 2019, pp. 584-587.

5. K. R. Rao, I. G. Ray, W. Asif, A. Nayak and M. Rajarajan, "R-PEKS: RBAC Enabled PEKS for Secure Access of Cloud Data," in *IEEE Access*, vol. 7, pp. 133274-133289, 2019.

6. S. Long and L. Yan, "RACAC: An Approach toward RBAC and ABAC Combining Access Control," *2019 IEEE 5th International Conference on Computer and Communications (ICCC)*, Chengdu, China, 2019, pp. 1609-1616.

7. R. Akkaoui, X. Hei, C. Guo and W. Cheng, "RBAC-HDE: On the Design of a Role-based Access Control with Smart Contract for Healthcare Data Exchange," *2019 IEEE International Conference on Consumer Electronics - Taiwan (ICCE-TW)*, Yilan, Taiwan, 2019, pp. 1-2.

8. J. Chen, S. Qi and J. Jia, "The Comparisons between TPA and Cloude-Pottier Alpha Angle," *2019 SAR in Big Data Era (BIGSARDATA)*, Beijing, China, 2019, pp. 1-4.

9. L. Chen, Y. Ma and C. Zhou, "RBAC Model Based on Workflow for Power Marketing Field Terminals," *2018 3rd International Conference on Smart City and Systems Engineering (ICSCSE)*, Xiamen, China, 2018, pp. 203-207.

10. J. P. Cruz, Y. Kaji and N. Yanai, "RBAC-SC: Role-Based Access Control Using Smart

Contract," in *IEEE Access*, vol. 6, pp. 12240-12251, 2018.

11. S. R. shree, A. ChilambuChelvan and M. Rajesh, "Optimization of Secret Key using cuckoo Search Algorithm for ensuring data integrity in TPA," *2020 International Conference on Computer Communication and Informatics (ICCCI)*, Coimbatore, India, 2020, pp. 1-5.

12. A. Thakare, E. Lee, A. Kumar, V. B. Nikam and Y. Kim, "PARBAC: Priority-Attribute-Based RBAC Model for Azure IoT Cloud," in *IEEE Internet of Things Journal*, vol. 7, no. 4, pp. 2890-2900, April 2020.

13. H. Belkhiria, F. Fakhfakh and I. B. Rodriguez, "Resolving Multi-user Conflicts in a Smart Building using RBAC," *2020 IEEE 29th International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE)*, Bayonne, France, 2020, pp. 181-186.

14. A. Suganthy and V. Prasanna Venkatesan, "An Introspective Study on Dynamic Role-Centric RBAC Models," *2019 IEEE International Conference on System, Computation, Automation and Networking (ICSCAN)*, Pondicherry, India, 2019, pp. 1-6.