International Journal of Computer Trends and Technology
ISSN: 2231–2803 / https://doi.org/10.14445/22312803/IJCTT-V72I4P105

Volume 72 Issue 4, 42-50, April 2024
© 2024 Seventh Sense Research Group®

Original Article

Real-Time Adaptive Access Control (RTAAC) for Enhanced Security and Privacy in Access Management

Saurav Bhattacharya[1], Puneet Gangrade[2], Dhruv Seth[3], Sriram Panyam[4]

[1]InfoSec Expert, Microsoft, Seattle, Washington, United States
[2]Privacy-Preserving Data Analytics Expert, LiveRamp, New York, New York, United States
[2]Solution Architect, Walmart Global Tech, Sunnyvale, California, USA
[4]Cloud/Data Engineering Expert, DagKnows Inc, Sunnyvale, California, USA

[1]Corresponding Author : online.saurav@gmail.com

Received: 09 February 2024 Revised: 16 March 2024 Accepted: 04 April 2024 Published: 15 April 2024

***Abstract** - Modern IT environments demand sophisticated access management strategies to balance security with operational efficiency. This paper explores the integration of the Least Privilege Principle and Just-in-Time (JIT) access to address the challenges of managing complex, dynamic systems. By granting only essential permissions for specific tasks and then promptly revoking them, this approach minimizes attack surfaces and reduces the risk of privilege creep. We present a theoretical framework for unifying these principles, along with strategies for dynamic access control, automated decision-making, and adaptive policies. This integrated model offers the potential to enhance security, streamline access, and improve operational efficiency. Though implementation challenges exist, proactive investment in tools, training, and process refinement can smooth the transition.*

***Keywords** - Access Management, Least Privilege Principle, Just-in-Time (JIT) Access Management, Privacy-Preserving Authorization, User-Initiated Access Requests, Automated Role Discovery, Proactive Monitoring, Operational Efficiency, Adaptive Policies, Security Enhancement Mechanisms.*

1. Introduction

In the dynamic landscape of Information Technology (IT) security, access management becomes a crucial component of defensive strategies against unauthorized access and data breaches. The complexity and fluidity of modern IT environments, characterized by cloud computing, mobile access, and interconnected systems, exacerbate the challenges of effective access rights management. Ensuring that users possess the appropriate level of access—neither insufficient to hinder productivity nor excessive to pose a security risk—demands a nuanced approach to access control. Central to this approach is the Least Privilege Principle, a security concept advocating that users and systems should have only the minimum level of access—or permissions—necessary to perform their functions [1]. This principle mitigates potential damage from accidents or attacks by restricting access rights to the bare minimum required to complete tasks. However, operationalizing this principle in complex IT environments necessitates sophisticated access management strategies.

Just-in-Time (JIT) access management complements the Least Privilege Principle by providing temporary access rights to resources based on real-time requests and assessments [2]. JIT access addresses the dynamic access needs of users while ensuring that such access is granted only when necessary and promptly revoked to minimize the window of opportunity for unauthorized use or exploitation.

This paper seeks to explore the integration of the Least Privilege Principle with JIT access, along with other innovative access management strategies such as usable interfaces, privacy-preserving authorization, user-initiated access requests, automated role discovery, and proactive monitoring for suspicious activities. By synthesizing insights from recent research, we propose a comprehensive framework for access management that balances security requirements with operational efficiency. Our contributions to the field include a detailed analysis of the challenges in current access management practices, an examination of the benefits and limitations of integrating Least Privilege and JIT access, and recommendations for implementing these principles in a unified access management strategy. Through this exploration, we aim to offer actionable insights for organizations seeking to enhance their IT security posture while maintaining the usability and flexibility required in today's fast-paced and constantly evolving technological landscape.

2. Existing Research on Least Privilege Principle, JIT Access, and Related Security Measures

The principle of least privilege and Just-in-Time (JIT) access management represent foundational elements in the design of secure information systems. Existing research in these areas spans theoretical frameworks, practical implementations, and assessments of their effectiveness in various IT environments.

Carter (2022) provides a comprehensive overview of the lifecycle and techniques for achieving the least privilege in access management. The paper emphasizes a balanced approach between Just-in-Time (JIT) access and long-standing permissions, advocating for iterative refinement based on the context of identity lifecycle and specific activities applicable across cloud, hybrid, and on-premises environments [1]. An illustration is shown in Figure 1.

Lang and Schreiner (2012) tackle the complexity of implementing least privilege in dynamic IT infrastructures, such as SOAs and clouds. They point out the need for access policies that go beyond traditional identity and roles, suggesting attribute-based (ABAC), resource-based (ResBAC), and authorization-based (ZBAC) controls to minimize excess access provisioning [3]. An illustration is shown in Figure 2.

Haber and Rolls (2019) detail the concept of JIT Access Management as a strategy to secure accounts by restricting real-time access based on behaviour, context, and other ephemeral properties.

This method aims to reduce risks associated with always-on accounts by establishing criteria for JIT access, emphasizing the importance of limiting account availability outside of necessary scenarios [2]. An illustration is shown in Figure 3.

Buyens, De Win, and Joosen (2008) address the challenge of supporting the principle of least privilege at the software architecture level. They propose guided architectural transformations to enhance security without compromising the semantics of the architecture, highlighting the lack of systematic application in practice [4]. An illustration is shown in Figure 4.

Steiner, De Leon, and Jillepalli (2018) discuss enforcing least privilege in web applications, particularly focusing on database management system (DBMS) access. They introduce Hierarchical Policy (HPol) as a formal access control modelling tool to prevent data breaches by applying the least privilege at all levels of a web application [5]. An illustration is shown in Figure 5.

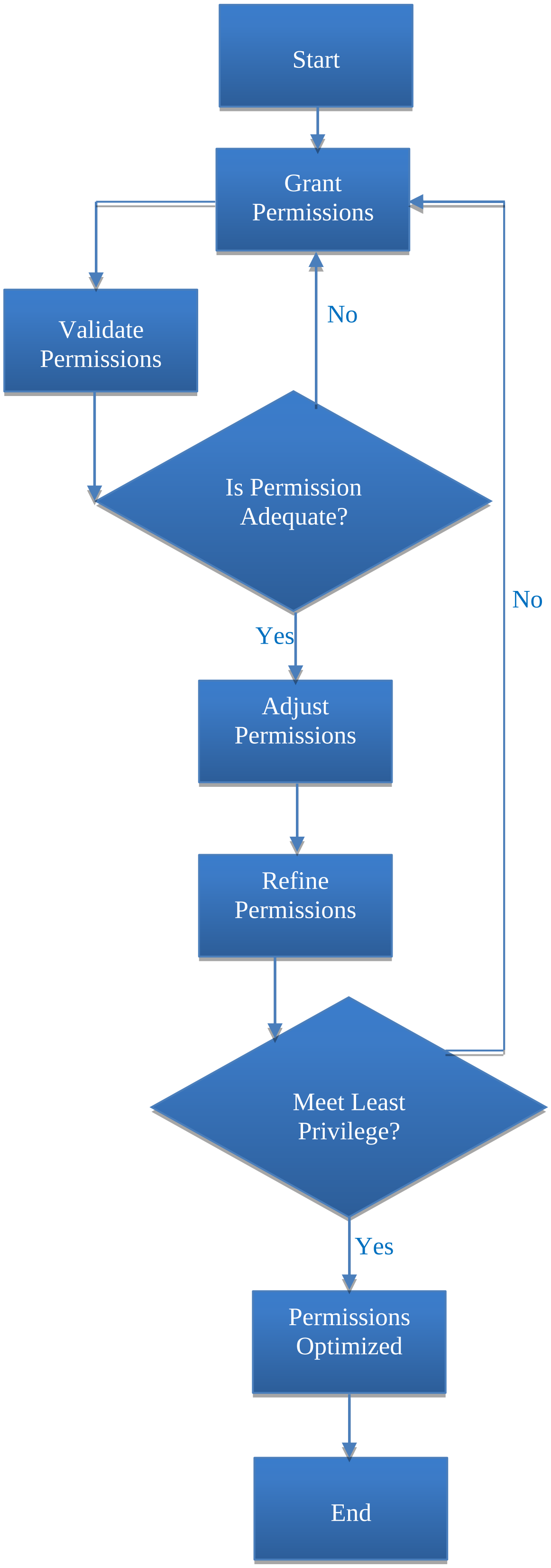

Fig. 1 Iterative refinement of Least privilege (Carter 2022)

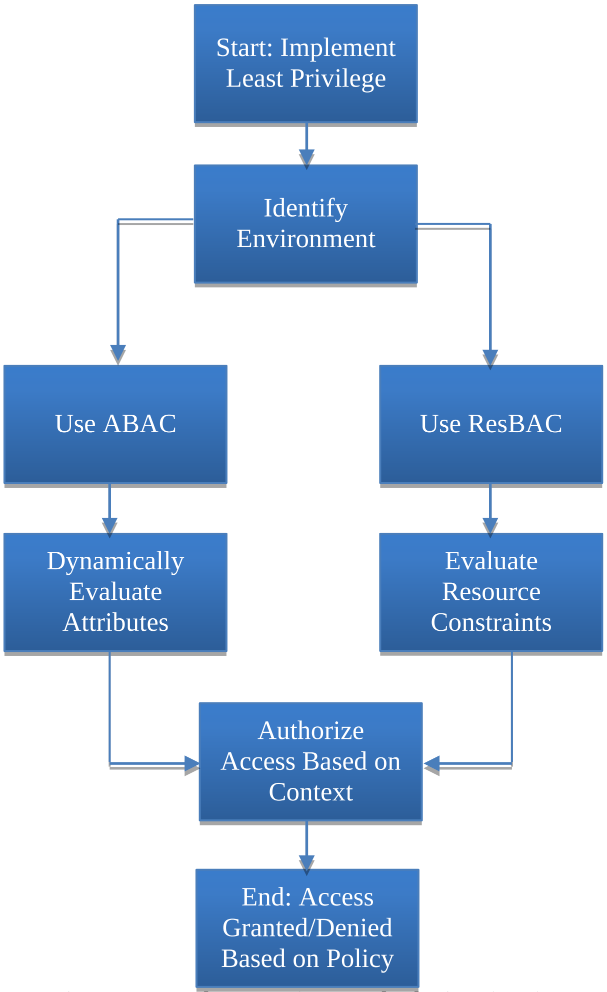
Start: Implement Least Privilege
Identify Environment
Use ABAC
Use ResBAC
Dynamically Evaluate Attributes
Evaluate Resource Constraints
Authorize Access Based on Context
End: Access Granted/Denied Based on Policy

Fig. 2 ABAC and ResBaC (Lang and Schreiner (2012)

3. Gaps in Current Approaches and the Need for an Integrated Strategy

While existing research provides significant insights into the least privileged and JIT access management, several gaps remain. Most notably, the application of these principles often lacks a systematic, integrated approach, especially in complex and dynamically changing IT environments.

The literature points to the need for fine-grained, context-aware access control mechanisms that can adapt to the evolving demands of users and systems. However, the practical implementation of such adaptive strategies remains challenging, with many organizations struggling to balance security with operational efficiency.

Furthermore, the research highlights a common shortfall in existing strategies: the difficulty of enforcing least privilege and JIT access uniformly across diverse systems and platforms. This inconsistency can lead to security vulnerabilities and inefficient access management practices. An integrated strategy that encompasses the entire IT ecosystem, leveraging automated policy generation, real-time access control, and continuous monitoring, is necessary to address these gaps effectively.

While the principles of least privilege and JIT access are well-established in the literature, there is a clear need for more cohesive, adaptive frameworks that can be systematically applied across various IT architectures. Such integrated strategies would not only enhance security and privacy but also support the operational agility required in today's fast-paced technological landscape.

4. Methodology

This section of our paper delineates the methodological approach undertaken to develop and evaluate a unified theoretical framework for integrating Least Privilege and JIT access management within IT security. Our methodology is bifurcated into two primary components: theoretical framework development and comparative analysis.

4.1. Theoretical Framework Development

To construct a unified theoretical framework that coherently integrates the principles of Least Privilege and JIT access management, we embarked on a multi-step process:

4.1.1. Literature Synthesis

We commenced by conducting a comprehensive review of existing literature encompassing Least Privilege and JIT access management theories, models, and implementations. This synthesis aimed to identify core components, benefits, challenges, and gaps within current theoretical and practical applications.

4.1.2. Conceptual Integration

Leveraging insights from the literature review, we developed a conceptual model that integrates the principles of Least Privilege and JIT access. This model posits a dynamic, context-aware system that adjusts access rights in real time based on predefined policies, current context, and risk assessments.

4.1.3. Formalization

The conceptual model was then formalized into a theoretical framework using mathematical and logical constructs. This formalization process involved defining key variables, relationships, and functions that govern the dynamic adjustment of access rights, ensuring adherence to Least Privilege and JIT principles.

4.1.4. Model Validation Criteria

We established theoretical validation criteria to assess the coherence, completeness, and applicability of the framework. These criteria serve as benchmarks for future empirical testing and theoretical refinement.

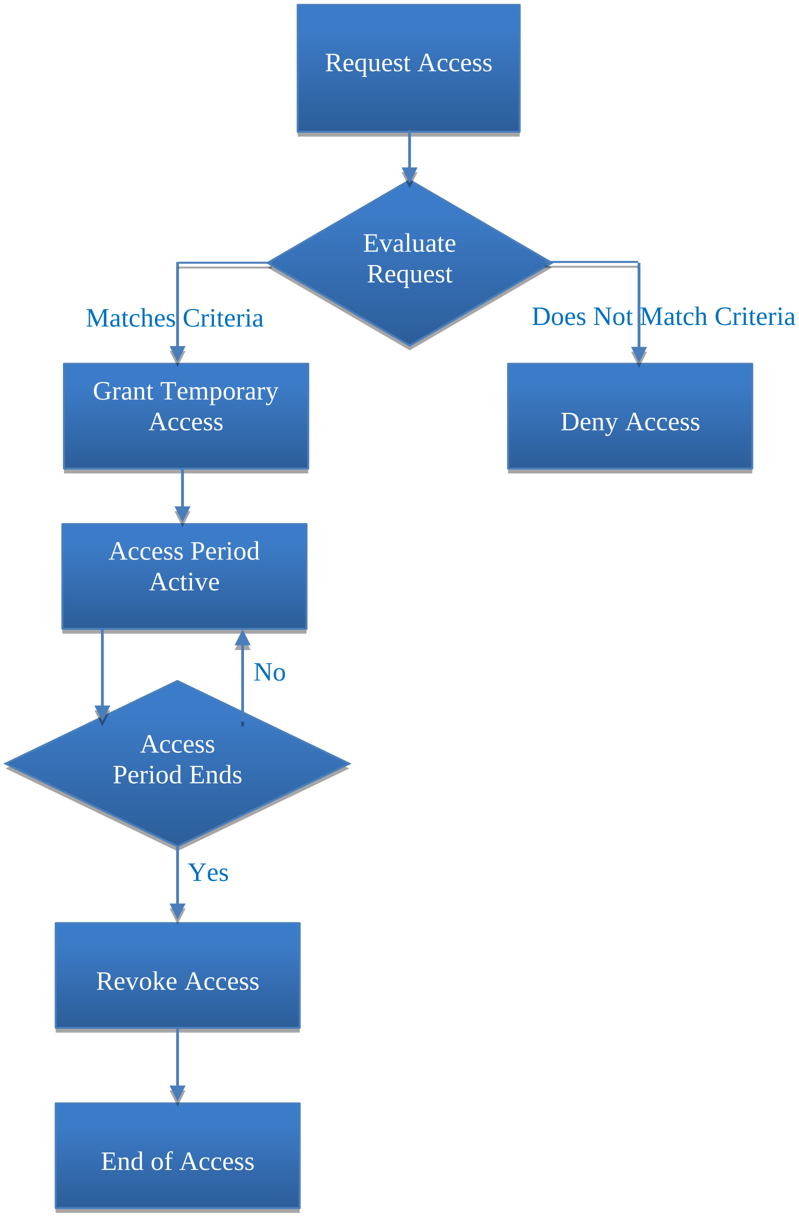

Fig. 3 JIT Access management

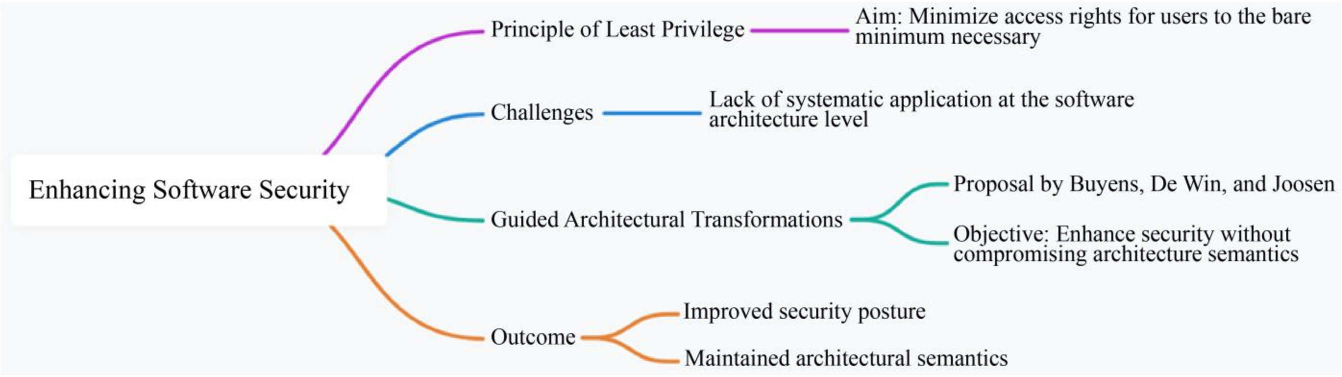
Enhancing Software Security
Principle of Least Privilege
Aim: Minimize access rights for users to the bare minimum necessary
Challenges
Lack of systematic application at the software architecture level
Guided Architectural Transformations
Proposal by Buyens, De Win, and Joosen
Objective: Enhance security without compromising architecture semantics
Outcome
Improved security posture
Maintained architectural semantics

Fig. 4 Principle of least privilege at the software architecture level

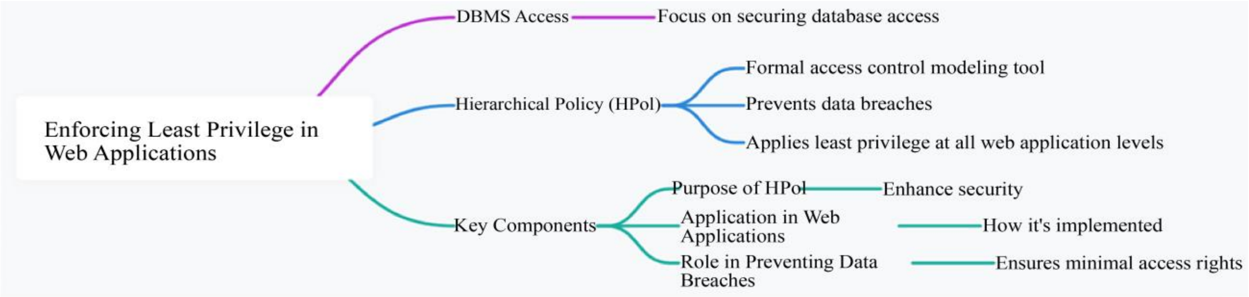
Enforcing Least Privilege in Web Applications
DBMS Access
Focus on securing database access
Hierarchical Policy (HPol)
Formal access control modeling tool
Prevents data breaches
Applies least privilege at all web application levels
Key Components
Purpose of HPol
Enhance security
Application in Web Applications
How it's implemented
Role in Preventing Data Breaches
Ensures minimal access rights

Fig. 5 Principle of least privilege for web applications

4.2. Comparative Analysis

To evaluate the proposed theoretical framework in relation to existing models and identify its potential advantages and limitations, we conducted a comparative analysis:

4.2.1. Selection of Comparative Models

We identified existing access management models from the literature that represent the current state-of-the-art, including static role-based access control (RBAC), attribute-based access control (ABAC), and others that incorporate elements of Least Privilege or JIT principles.

4.2.2. Criteria Development

Comparative criteria were developed based on several key dimensions, including security effectiveness, operational efficiency, adaptability, and ease of implementation. These criteria allow a nuanced comparison across models.

4.2.3. Theoretical Comparison

Utilizing the defined criteria, we conducted a theoretical comparison of the proposed framework against selected models. This comparison highlighted the theoretical enhancements offered by our framework, such as improved adaptability to dynamic IT environments and more effective minimization of excessive permissions.

4.2.4. Gap Analysis

The comparative analysis also facilitated a gap analysis, identifying areas where the proposed framework may require further theoretical development or adaptation to address specific challenges not fully mitigated by existing models. The methodology outlined provides a robust theoretical foundation for the development and evaluation of a unified access management framework. By synthesizing existing literature, formalizing a conceptual integration, and conducting a comparative analysis, this approach not only advances the theoretical discourse in IT security access management but also sets the stage for empirical validation and practical implementation of the proposed framework.

5. Findings

5.1. Integrated Model Proposition

Our theoretical exploration led to the development of an integrated access management model that harmonizes the principles of Least Privilege and JIT access within a unified framework for Real-Time Adaptive Access Control (RTAAC). This model is characterized by its dynamic, context-aware capabilities, enabling real-time adjustments to access rights based on a comprehensive analysis of user behaviour, risk assessment, and the specific requirements of the task at hand. An illustration of the RTAAC framework is shown in Figure 6.

5.1.1. Dynamic Access Control

At the core of the model lies a dynamic access control mechanism that operates on real-time data, assessing and adjusting user permissions as necessary. This mechanism is designed to ensure that access rights are always aligned with the current context, minimizing the risk of over-privileged access.

5.1.2 Adaptive Policies

The framework supports the development and implementation of adaptive policies that can evolve based on ongoing assessments of access patterns and security incidents. These policies are key to maintaining the balance between operational efficiency and security imperatives.

5.1.3. Risk Assessment Integration

Risk assessment is integral to the model, with access decisions being informed by a continuous evaluation of potential threats and vulnerabilities. This approach ensures that decisions regarding access rights are always made with security considerations at the forefront.

5.2. Security Enhancement Mechanisms

The proposed model theoretically enhances IT security by implementing several key mechanisms:

5.2.1. Minimization of Privilege Creep

By adhering to the Least Privilege principle in a dynamic manner, the model minimizes the occurrence of privilege creep, where users accumulate more permissions than necessary over time.

5.2.2. Reduction in Attack Surface

JIT access management reduces the window of opportunity for attackers by ensuring that access is granted only when necessary and promptly revoked, thereby minimizing the attack surface.

5.2.3. Continuous Authentication and Authorization Monitoring

Combining Just-in-Time (JIT) access management with continuous authentication and authorization monitoring creates a robust security system for user access within IT environments. This approach goes beyond traditional login checks by constantly verifying user legitimacy and adjusting access rights based on real-time factors.

5.3. Operational Efficiency

The model's impact on operational efficiency is multifaceted, offering significant improvements over traditional static access control systems:

5.3.1. Streamlined Access Management

By automating the process of adjusting access rights in real time, the model streamlines access management, reducing the administrative burden on IT staff.

5.3.2. Enhanced User Productivity

Users benefit from an access management system that adapts to their needs without unnecessary delays or hurdles, thereby enhancing overall productivity.

5.3.3. Faster Response to Changing Business Needs

Organizations can quickly adapt to changing business requirements with JIT. For example, if a project requires immediate access to certain resources, JIT can facilitate this access in real-time, ensuring that bureaucratic processes do not delay business operations.

5.3.4. Reduced Risk of Human Error

Automating the access management process reduces the risk of human errors, such as accidentally granting excessive privileges or failing to revoke access when it's no longer needed. This not only enhances security but also improves overall operational reliability.

6. Discussion

6.1. Theoretical Implications

The theoretical framework presented in this paper contributes to the field of IT security access management by offering a novel approach that integrates Least Privilege and JIT principles. This integrated model addresses several identified gaps in current practices, particularly in terms of adapting to dynamic IT environments and managing access rights in real time.

6.2. Limitations and Assumptions

While the proposed model offers a comprehensive theoretical foundation, it is not without limitations and assumptions. The effectiveness of the model is predicated on the accuracy of risk assessments and the ability to dynamically adjust policies based on real-time data, which may be challenging in practice. Future empirical research is needed to validate these aspects and refine the model accordingly.

6.3. Integration Challenges

Integrating the proposed model into existing IT infrastructures poses significant challenges, including the need for extensive customization and potential compatibility issues with legacy systems. Theoretical strategies for overcoming these challenges include phased implementation plans and the development of middleware solutions that can facilitate integration.

The development of an integrated access management model that combines Least Privilege and JIT principles represents a significant theoretical advancement in the field of IT security. This model offers a promising foundation for enhancing security and operational efficiency in dynamic IT environments. Future research should focus on empirical validation of the model and exploring practical implementation strategies to realize its full potential.

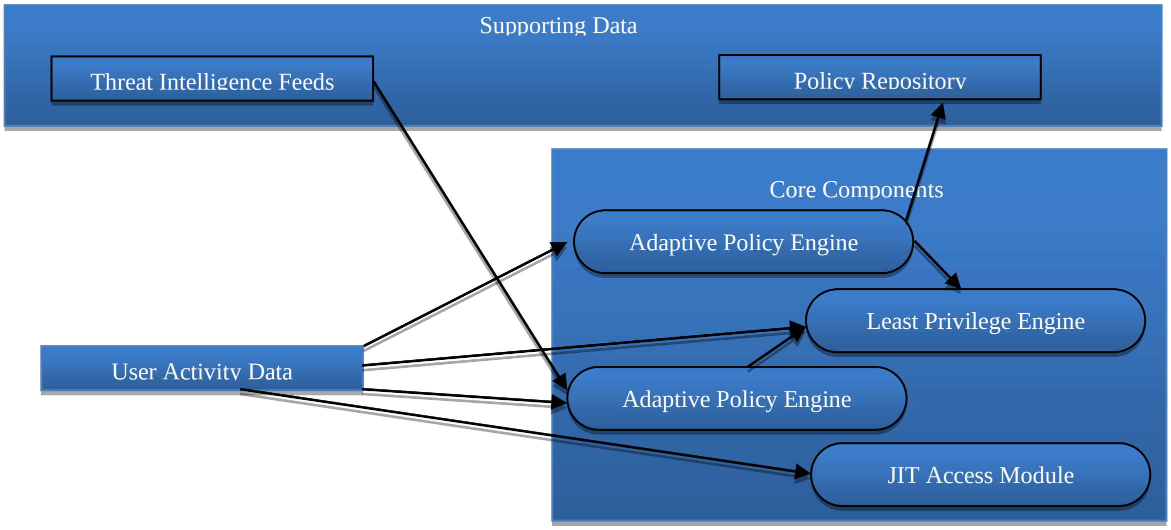

Fig. 6 RTAAC framework

7. Theoretical Implications for Practice

The proposed integrated access management model, grounded in the principles of Least Privilege and Just-in-Time (JIT) access, offers several theoretical implications for practice that can guide organizations in enhancing their IT security posture:

- Adaptive Security Posture: Organizations should adopt an adaptive security posture that dynamically adjusts access rights in real time based on context and risk assessments. This approach requires a shift from static, role-based access controls to more fluid, context-aware strategies.
- Continuous Risk Assessment: Continuous risk assessment should be embedded into the access management process, enabling organizations to make informed decisions about granting or revoking access rights based on the current threat landscape and user behavior.
- Automation of Access Decisions: Automation plays a crucial role in the proposed model, allowing for the efficient management of access rights without manual intervention. Organizations should invest in technologies that enable automated policy enforcement and real-time access adjustments.
- Self-Sovereign Identity for User-Centric Access: Adopting self-sovereign identity principles, where users own and control their identity and access rights, can empower them and enhance privacy. This user-centric approach aligns with Just-in-Time (JIT) and Least Privilege principles by ensuring that access rights are closely tied to the user's current context and needs.

While the benefits are many, there are implementational and organizational challenges in implementing JIT access:

- Implementation Complexity**:** Integrating JIT access with Principles of Least Privilege (POLP) needs a thorough understanding of specific access needs required within the organizations (and by various roles and actors within an organization). Organizational size and diversity only exacerbate this complexity proportionally. For example, determining exact timing and permission (types and scopes) for various roles can become a complex and expensive task especially with environments that integrate several systems from several vendors.
- Monitoring and Auditing**:** JIT access and Principles of Least Privilege (POLP) also needs to be continuously monitored and audited - especially for security and compliance (e.g. auditing every instance of an access grant/denial to detect abuses or anomalies). These processes can themselves be resource-intensive and demand sophisticated tools and expertise for effective oversight.
- Integration with Existing Systems**:** As organizations grow, their ecosystem is littered with ever-growing legacy systems and applications. These may not support the dynamic nature of JIT nor enforce POLP. Integrating or replacing them can be very expensive, if not impossible. Upgrading or modifying them may be a very resource-intensive endeavor.
- Compliance and Policy Enforcement: The nature of regulation and compliance (especially across jurisdictions) is dynamic and ever-changing. This places extra burden and complications on ensuring that JIT access and POLP are complied with. For example, in GDPR or HIPAA regulations, where access to sensitive information must be strictly controlled and audited, requiring robust mechanisms can be challenging and error-prone.
- Impact on User Experience: If not designed and balanced carefully, users may incur delays and degraded experiences in accessing resources they require for their jobs, impacting productivity.
- Scalability Issues**:** Requiring JIT access while ensuring POLP could also be challenging both technically (needing reliable tools and platforms) and in its implementation (e.g. onboarding, training etc.), especially for organizations with diversity in their workforce. For example, ensuring contractors have the right access during the right window would require systems with high levels of consistency and availability.

8. Guidelines for Implementation

Implementing the integrated access management model within an organization involves several key steps:

8.1. Assessment and Planning

Begin with a comprehensive assessment of current access management practices and IT infrastructure. Identify areas where the principles of Least Privilege and JIT access can be integrated and develop a phased implementation plan.

8.2. Policy Development

Develop adaptive access management policies that reflect the organization's security requirements, operational needs, and risk tolerance. These policies should be flexible enough to accommodate changes in the IT environment and threat landscape.

8.3. Technology Investment

Invest in technologies that support dynamic access control, such as identity and access management (IAM) solutions that offer real-time risk assessment, automated policy enforcement, and seamless integration with existing systems.

8.4. Training and Awareness

Educate IT staff and users about the new access management model, focusing on the importance of security, the rationale behind dynamic access controls, and their roles in maintaining a secure IT environment.

8.5. Monitoring and Evaluation

Implement continuous monitoring mechanisms to track the effectiveness of the new access management strategies. Regularly evaluate the system's performance, adjusting policies and technologies as needed.

8.6. Detailed Document

Maintain comprehensive documentation of access management policies, procedures, and configurations. This documentation is crucial for training, troubleshooting, compliance audits, and future policy revisions.

9. Impact on IT Security Policies

The adoption of the proposed integrated access management model necessitates revisions to existing IT security policies:

9.1. Inclusion of Dynamic Access Controls

IT security policies should explicitly include provisions for dynamic access control, outlining the criteria for real-time adjustments to access rights and the mechanisms for continuous risk assessment.

9.2. Emphasis on Least Privilege and JIT Principles

Policies should emphasize the organization's commitment to the principles of Least Privilege and JIT access, detailing the strategies for their implementation and enforcement.

9.3. Guidance on Automation and Technology Use

Provide guidelines on the use of automation and technology in access management, specifying approved tools, platforms, and practices that support the integrated model.

9.4. Compliance and Regulatory Considerations

Update policies to ensure compliance with regulatory requirements related to access management and data protection. This includes specifying how the integrated model aligns with standards such as GDPR, HIPAA, and ISO/IEC 27001.

10. Privacy-Preserving Data Analytics: Bridging Secure Access and Data Utilization

This section delineates the extension of Least Privilege and Just-in-Time Access principles to the domain of data analytics, focusing on the integration of Privacy-Enhancing Technologies (PETs). It elaborates on deploying differential privacy, federated learning, and secure multi-party computation techniques within data analytics frameworks to safeguard sensitive information. This emphasizes the imperative of balancing data utility against privacy concerns, illustrating how the principles outlined in the preceding sections can inform the development of data analytics solutions prioritizing user privacy. This approach ensures a seamless transition from the foundational discussion on security and privacy in access management to the broader application of these principles in data analytics.

10.1. Principle-Based Approach to PETs

Privacy-enhancing technologies ensure people's private information stays private. This lets businesses do new things they couldn't before because they were worried about sharing personal details. Adopting a principle-based approach to PETs means aligning the deployment of these technologies with core system design principles like Least Privilege and Just-in-Time Access.

This approach ensures that access to data and its processing is tightly controlled and limited to only what is necessary for a specific task and only for the duration required. By embedding these principles at the heart of PET integration, organizations can achieve more data privacy and security. This method restricts access to sensitive data and minimizes the risk of unauthorized data exposure.

By leveraging these system design principles, PETs can be more effectively implemented, ensuring that privacy measures are not an afterthought but a foundational component of the data analytics process. This strategic alignment enhances the overall security posture of data analytics operations, making privacy-preserving data analytics a more attainable goal.

10.2. Application of Principles and Access by the Wider Team

Practitioners employ the Least Privilege principle and access management to ensure users and processes have only the necessary data access for their tasks, enhancing security and efficiency. This includes analyzing and modeling data, implementing and monitoring security policies, ensuring compliance with laws, and making decisions based on data insights. Each role balances data access needs with privacy and security requirements, contributing to a secure and efficient data utilization framework.

10.3. Benefits of Data Minimization Principles

When applied to use cases, data minimization principles offer several benefits, including enhancing privacy and security by limiting the amount of data collected and retained to what is strictly necessary. This approach reduces the risk of data breaches and unauthorized access, as less data is vulnerable to exploitation. Furthermore, data minimization simplifies compliance with privacy regulations, making it easier for organizations to adhere to legal requirements. It also improves data management efficiency, as less data requires less storage and processing power, leading to cost savings and faster processing times. Overall, data minimization enhances the trust of stakeholders and users by demonstrating a commitment to privacy and responsible data handling.

11. Conclusion

The integration of the Least Privilege Principle with Just-in-Time access presents a compelling framework for addressing the complexities of secure system management within dynamic IT environments. This approach offers a marked improvement over traditional access control models by minimizing attack surfaces, preventing privilege creep, and streamlining access management processes. Effective implementation hinges on several key elements: context-aware access controls that incorporate real-time assessments, adaptive policies that evolve alongside organizational needs, and automated decision-making to reduce administrative overhead.

Organizations must invest in the necessary technologies and training to facilitate a successful transition to this model, proactively addressing potential challenges such as legacy system integration, the maintenance of high-quality data for accurate risk assessments, and ensuring user adoption. While the theoretical benefits are evident, future research should centre on empirical validation of the model across diverse IT environments. This validation will refine the approach, establish best practices for specific organizational contexts, and ultimately promote the wider adoption of this integrated strategy for robust IT security.

Funding Statement

This publication was funded by a grant from The New World Foundation.

Acknowledgments

We would like to extend our heartfelt thanks to Pradeep Chintale, Cloud Solutions Architect, SEI Investment Company, Downingtown, Pennsylvania, United States; Gaurav Deshmukh, No Code Low Code Software Automation expert, Guidewire Software, Los Angeles, California; and Robin Verma, Data Engineering/Cloud Expert, Wells Fargo, Telangana, Hyderabad, India, for their insightful comments and constructive feedback on our manuscript. Their expertise and thoughtful critique have significantly contributed to the enhancement of this work. We deeply appreciate the time and effort dedicated to reviewing our paper and guiding us toward a more rigorous and polished final product. Thank you.

References

[1] Matthew Keith Carter, “Techniques To Approach Least Privilege,” *IDPro Body of Knowledge*, vol. 1, no. 9, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[2] Morey J. Haber, and Darran Rolls, *Just-in-Time Access Management*, Identity Attack Vectors, Apress, Berkeley, CA, pp. 151-155, 2019.[CrossRef] [Google Scholar] [Publisher Link]

[3] Ulrich Lang, and Rudolf Schreiner, *Implementing Least Privilege for Interconnected, Agile SOAs/Clouds*, ISSE 2012 Securing Electronic Business Processes, Springer Vieweg, Wiesbaden, pp. 89-102, 2012. [CrossRef] [Google Scholar] [Publisher Link]

[4] Koen Buyens, Bart De Win, and Wouter Joosen, “Improving Least Privilege in Software Architecture by Guided Automated Compartmentalization,” *Proceedings of the 6th International Workshop on Security in Information Systems*, pp. 145-150, 2008. [CrossRef] [Google Scholar] [Publisher Link]

[5] Stuart Steiner, Daniel Conte de Leon, and Ananth A. Jillepalli, “Hardening Web Applications using the Least Privileged DBMS Access Model,” *Proceedings of the Fifth Cybersecurity Symposium*, Coeur d' Alene Idaho, pp. 1-6, 2018. [CrossRef] [Google Scholar] [Publisher Link]