STM JOURNALS

Journal of
Advanced Database
Management & Systems

ISSN: 2393-8730
Volume 13, Issue 1, 2026
January–April
DOI (Journal): 10.37591/JoADMS

https://journals.stmjournals.com/joadms

Review JoADMS

A Comprehensive Study of Risk-Adaptive Access Control in Advanced Database Management Systems

Manas Kumar Yogi*

Abstract

The current control methods for the accession of a crucial resource often struggle to provide adequate security in dynamic and complex advanced database management systems (DBMS). These static models lack the flexibility to adapt to evolving threats and contextual changes, leaving potential vulnerabilities. Risk-adaptive access control (RadAC) emerges as a sophisticated solution, integrating real-time risk assessment into authorization decisions to dynamically adjust access permissions. This review article provides a comprehensive study of RadAC in advanced DBMS, exploring its theoretical foundations, architectural components, and practical applications. We delve into the methodologies for risk quantification, the role of contextual factors, and the integration of machine learning techniques for enhanced adaptability. We have also analyzed the challenges associated with RadAC implementation, including performance overhead, complexity, and the need for transparent policy enforcement. By synthesizing recent scholarly work from the past five years, this article aims to offer a holistic understanding of RadAC, highlighting its potential to significantly enhance data security and compliance in modern database environments, while also identifying research directions and emerging trends.

Keywords: Access, advanced database management systems, attack, cyber threat, database, risk

INTRODUCTION

In the contemporary digital landscape, advanced database management systems (DBMS) form the backbone of virtually all critical applications, storing and managing vast quantities of sensitive information. The integrity, confidentiality, and availability of these data are paramount, from financial records and healthcare data to personal user information and intellectual property. Consequently, robust access control mechanisms are indispensable for safeguarding these valuable assets against unauthorized access, misuse, and cyberthreats [1]. However, traditional access control models, such as discretionary access control (DAC), mandatory access control (MAC), role-based access control (RBAC), and attribute-based access control (ABAC), while foundational, often exhibit limitations when confronted with the dynamic, heterogeneous, and increasingly complex nature of modern database environments [2, 3].

***Author for Correspondence**
Manas Kumar Yogi
E-mail: manas.yogi@gmail.com

Assistant Professor, Department of Computer Science and Engineering, Pragati Engineering College (A), Surampalem, Andhra Pradesh, India

Received Date: January 16, 2026
Accepted Date: January 29, 2026
Published Date: April 28, 2026

Citation: Manas Kumar Yogi. A Comprehensive Study of Risk-Adaptive Access Control in Advanced Database Management Systems. Journal of Advanced Database Management & Systems. 2026; 13(1): 19–28p.

Static access control policies, which define permissions based on pre-established roles, attributes, or rules, struggle to adapt to real-time changes in user behavior, environmental conditions, or evolving threat landscapes. An access request deemed legitimate under static policies might pose a significant risk under different contextual circumstances, such as unusual access times, unfamiliar locations, or compromised devices. This inherent inflexibility can lead to either overly permissive access, creating security vulnerabilities, or overly restrictive access, hindering legitimate business operations and user productivity [4].

To address these shortcomings, the risk-adaptive access control (RadAC) paradigm has emerged as a critical evolution in access control. RadAC is characterized by its ability to dynamically adjust authorization decisions based on a continuous assessment of the risks associated with each access request. Instead of relying solely on static rules, RadAC incorporates contextual information, user behavior analytics, and threat intelligence to compute a real-time risk score. This score then informs the access decision, allowing for a more granular, flexible, and proactive security posture [5]. For instance, a user attempting to access sensitive data from an unknown IP address outside business hours might be subjected to additional authentication challenges or have their access temporarily restricted, even if their role typically permits such access.

This review article undertakes a comprehensive study of RadAC in the context of advanced database management systems (DBMS). We aim to provide an in-depth analysis of its theoretical underpinnings, the architectural components required for its implementation, the various methodologies employed for risk quantification, and its practical applications across different database technologies. Furthermore, we will critically examine the challenges inherent in designing and deploying effective RadAC systems, including performance overhead, complexity, and the need for user acceptance. By synthesizing recent scholarly contributions from 2020 to 2026, this article seeks to offer a holistic understanding of RadAC, highlighting its transformative potential for enhancing data security and compliance in the face of persistent and evolving cyber threats. The subsequent sections will elaborate on the theoretical foundations, architectural considerations, risk factors, challenges, and prospects of RadAC [6, 7]

THEORETICAL FOUNDATIONS AND MODELS OF RISK-ADAPTIVE ACCESS CONTROL

RadAC fundamentally shifts the paradigm from static, rule-based authorization to dynamic, context-aware decision-making. This evolution is underpinned by several theoretical foundations and has led to the development of various models that integrate risk assessment into the access control process. Understanding these theoretical underpinnings is crucial for appreciating the sophistication and effectiveness of RadAC in securing advanced DBMS.

Core Principles of RadAC

The essence of RadAC lies in its ability to evaluate the risk associated with an access request in real time and adjust the access decision accordingly. This involves several core principles.

Dynamic Authorization

Unlike traditional models, where permissions are fixed, RadAC policies are fluid, adapting to changes in the environment, user behavior, and threat landscape [8].

Contextual Awareness

RadAC leverages a rich set of contextual information, including user identity, location, time of access, device posture, data sensitivity, and the nature of the requested operation to inform risk assessment [9].

Risk Quantification

A central tenet of RadAC is its ability to quantify risk. This involves assigning a numerical or qualitative risk score to each access attempt, which guides the authorization decision. This score is typically derived from a combination of factors, their associated probabilities, and impacts.

Continuous Monitoring and Assessment

RadAC systems are not one-time decision engines; they continuously monitor user activities and environmental factors, reassess risks, and adjust permissions throughout the session [10].

Adaptive Response

Based on the calculated risk, RadAC can trigger various adaptive responses, ranging from granting full access for low-risk requests to denying access, requesting additional authentication (e.g., multi-factor authentication, MFA), or escalating the request for human review for high-risk scenarios.

Risk Quantification Methodologies

The accuracy and effectiveness of RadAC are heavily dependent on the underlying risk quantification methodology. Various approaches have been proposed and implemented.

Probabilistic Models

These models use statistical methods to calculate the probability of a security breach, given certain contextual factors. Bayesian networks, for instance, can be employed to model the relationships between different risk indicators and their impact on the overall risk score [11].

Fuzzy Logic

Fuzzy logic provides a way to handle uncertainty and imprecision in risk assessment, which is often present in real-world applications. It allows for the definition of linguistic variables (e.g., "low risk," "medium risk," "high risk") and fuzzy rules to derive a risk score [12]. This approach is particularly useful when dealing with subjective or qualitative risk factors.

Machine Learning

Machine learning (ML) algorithms, including supervised and unsupervised learning techniques, are increasingly being used for risk quantification. They can learn patterns of normal and anomalous behaviors from historical data, enabling the system to detect deviations that indicate a higher risk. Techniques such as anomaly detection, classification, and regression can be applied to predict the risk level of an access request [13].

Utility-Based Models

These models consider not only the risk but also the utility or business value of granting access to data. A high-risk access request might still be granted if the potential business benefit outweighs the risk or if appropriate compensating controls are in place.

Integration with Existing Access Control Models

RadAC is not typically a standalone access control model but rather an enhancement that integrates with and extends existing models [14]. It is often layered on top of or complements:

Role-Based Access Control

RadAC can dynamically modify the permissions associated with a role or restrict a user from exercising certain role-based permissions if the risk context is changed.

Attribute-Based Access Control

RadAC can leverage the rich set of attributes in ABAC (user, resource, and environment attributes) to build more granular and context-aware risk assessment policies.

Zero Trust Architecture

RadAC is a fundamental component of the Zero Trust principles, which advocate for "never trust, always verify." In a zero trust architecture (ZTA), every access request is treated as untrusted until its risk is assessed and verified, aligning perfectly with RadAC's dynamic risk evaluation (Table 1).

ARCHITECTURE AND IMPLEMENTATION OF RadAC IN ADVANCED DBMS

The successful deployment of RadAC in advanced DBMS necessitates a robust architectural framework capable of collecting contextual information, assessing risk in real time, and enforcing adaptive policies. This section outlines the typical architectural components of a RadAC system and discusses its implementation considerations in various advanced DBMS environments.

Architectural Components of a RadAC System

A RadAC system typically comprises several interconnected components that work in concert to provide dynamic, risk-aware access control [14].

Table 1. Comparison of access control models and RadAC integration [15].

Access control model	Core principle	Limitations (addressed by RadAC)	RadAC integration
Discretionary access control (DAC)	The owner grants/revokes access to objects.	Lacks centralized control, prone to privilege escalation.	RadAC can monitor DAC decisions for high-risk patterns.
Mandatory access control (MAC)	The system enforces access based on security labels.	Rigid, complex to manage, not suitable for dynamic environments.	RadAC can dynamically adjust security labels or enforce stricter policies based on risk.
Role-based access control (RBAC)	Permissions assigned to roles, users assigned to roles.	Static, role explosion, cannot adapt to contextual changes.	RadAC dynamically modifies role permissions or restricts role activation based on real-time risk.
Attribute-based access control (ABAC)	Access is based on attributes of the user, resource, environment, and action.	Policy complexity, performance overhead for complex attribute evaluation.	RadAC uses ABAC attributes as inputs for risk assessment, enhancing granularity.
Risk-adaptive access control (RadAC)	Dynamic authorization based on real-time risk assessment.	(N/A—it is the solution)	Enhances all traditional models with dynamic, context-aware risk evaluation.

Context Collector/Sensor

This component is responsible for gathering relevant contextual information from different sources. This includes user attributes (e.g., role, department), environmental attributes (e.g., IP address, time of day, location, device type, network security posture), resource attributes (e.g., data sensitivity, classification), and action attributes (e.g., read, write, delete). In the context of a DBMS, this may involve monitoring database logs and network traffic and integrating with identity and access management (IAM) systems.

Risk Assessment Engine

Risk assessment engine (RAE) is the core intelligence of RadAC systems. It processes the collected contextual data and applies predefined risk models (probabilistic, fuzzy, and ML-based) to compute a real-time risk score for each access request. The RAE often maintains a risk profile for users and resources that is continuously updated.

Policy Decision Point

Policy decision point (PDP) receives the access request along with the calculated risk score from RAE. Subsequently, this information is evaluated against a set of risk-adaptive access policies. These policies define the actions to be taken (e.g., permit, deny, challenge) based on the risk level and other policy rules.

Policy Enforcement Point

Policy enforcement point (PEP) is responsible for enforcing the access decisions made by the PDP. In a DBMS, this component typically resides within or is closely integrated with the database engine. If the PDP decides to grant access, the PEP allows the operation. If the decision is to deny, the PEP blocks the request. For adaptive responses, the PEP might trigger additional authentication mechanisms (e.g., MFA) or initiate an alert to security administrators.

Feedback Loop/Learning Module

An essential aspect of adaptive systems, this component collects data on access decisions, user responses to challenges, and actual outcomes. This data is then fed back into the RAE, particularly for ML-based risk models, to continuously refine risk assessment algorithms and improve their accuracy over time.

Implementation in Advanced DBMS Environments

The integration of RadAC into advanced DBMS requires careful consideration of the specific characteristics of different database technologies [15].

Relational Database Management Systems

For traditional RDBMS, RadAC can be implemented as an external layer that intercepts SQL queries or API calls before they reach the database engine. The PEP can be a proxy or a database firewall, whereas the context collector integrates with existing security information and event management (SIEM) systems and IAM. Stored procedures or triggers within the database can also be used to enforce fine-grained access based on the risk scores.

NoSQL Databases

NoSQL databases (e.g., MongoDB, Cassandra, and Neo4j) often have different access control mechanisms than RDBMS, sometimes offering less granular control natively. Implementing RadAC in NoSQL environments may involve developing custom access control layers or integrating with API gateways that can perform risk assessments before forwarding requests to the database. The distributed nature of NoSQL databases also presents challenges in terms of consistent context collection and policy enforcement across nodes.

Cloud-Native Databases

Cloud-native databases (e.g., Amazon Aurora and Google Cloud Spanner) leverage cloud infrastructure for scalability and resilience. RadAC in these environments can benefit from integration with cloud-native security services such as identity providers, logging services, and threat detection tools. The API gateway of the cloud provider can serve as a natural PEP, and serverless functions can be used for context collection and risk assessment.

Distributed Ledger Technologies/Blockchain Databases

Although distributed ledger technologies (DLT) inherently offer immutability and decentralization, access control to the data stored on the ledger requires careful management. RadAC can be applied to control who can submit transactions or access specific data on a blockchain, with risk assessment based on the participant's reputation, transaction history, and network condition.

RISK FACTORS AND CONTEXTUAL AWARENESS IN RadAC FOR DBMS

The effectiveness of RadAC in advanced DBMS hinges on its ability to accurately identify and assess various risk factors and leverage contextual information. This section delves into the critical risk factors that influence access decisions and the mechanisms for achieving comprehensive contextual awareness within the DBMS environment.

Key Risk Factors

Risk in RadAC is a multifaceted concept, typically derived from the evaluation of several categories of factors. These factors contribute to the overall risk score associated with an access request [16].

User-Related Factors

These pertain to the identity and behavior of the individual or entity attempting access.

User Identity and Role

Although foundational, RadAC goes beyond static roles. Risk can be higher for privileged users (e.g., database administrators) or users with a history of policy violations.

User Behavior Analytics

Deviations from a user's typical access patterns (e.g., accessing unusual data at unusual times or with unusual frequency) can indicate compromised credentials or insider threats.

User Reputation/Trust Score

A dynamic score reflecting the historical trustworthiness of a user based on their past actions and compliance.

Environmental Factors

These relate to the conditions under which the access request originates.

Location

Access from unusual geographical locations, especially those associated with known threats or outside typical operational regions, significantly increases the risk.

Time of Access

Accessing outside normal business hours or during periods of low activity can be suspicious.

Device Posture

The security state of the device used for access (e.g., unpatched, jailbroken, lacking antivirus, or unmanaged device) is a critical risk indicator.

Network Conditions

Access originating from untrusted networks, public Wi-Fi, or IP addresses known for malicious activity raises the risk profile.

Resource-Related Factors

These concern the characteristics and sensitivity of the data or database object being accessed.

Data Sensitivity/Classification

Access to highly sensitive data (e.g., PII, financial records, and intellectual property) inherently carries a higher risk than access to public or less sensitive information.

Data Value/Criticality

The business impact of unauthorized access to a particular dataset or database can increase its risk.

Access Frequency/Volume

Unusual patterns in the volume or frequency of access to a specific resource can indicate data exfiltration attempts.

Action-Related Factors

These describe the nature of the operation being performed.

Type of Operation

Write or delete operations typically carry a higher risk than read operations, especially for critical data. Bulk data downloads also pose a higher risk [16].

Query Complexity/Content

Complex or unusual queries, especially those involving joins across sensitive tables or direct manipulation of system tables, can be flagged as high risk.

Achieving Contextual Awareness

Effective RadAC relies on a comprehensive and real-time understanding of the context of each access request. Contextual awareness is achieved through several mechanisms as discussed below.

Data Sources Integration

RadAC systems are integrated with a multitude of data sources, including identity providers (Lightweight directory access protocol (LDAP), Active Directory), network monitoring tools, endpoint detection and response (EDR) systems, geographical IP databases, threat intelligence feeds, and internal database audit logs.

Table 2. Common risk factors and their impact on authorization in RadAC for DBMS [17].

Risk factor category	Specific factors	Impact on access decision
User-related	User behavior anomaly, privileged user, historical trust score.	Higher risk for anomalous behavior or low trust; stricter controls for privileged users.
Environmental	Unusual location, time of access, unmanaged device, untrusted network.	Increased risk, potentially triggering MFA or access denial.
Resource-related	High data sensitivity, critical data value, unusual access volume.	Higher risk for sensitive/critical data; close monitoring for unusual access patterns.
Action-related	Write/delete operations, complex queries, and bulk data export.	Higher risk for data modification/exfiltration; additional scrutiny.

Real-time Data Processing

Given the dynamic nature of risk, contextual data must be processed in real-time or near-real-time. Stream processing technologies and in-memory databases are often employed to handle high volumes and velocities of contextual information.

User and Entity Behavior Analytics (UEBA)

UEBA tools are crucial for establishing the baseline normal behavior of users, applications, and devices. Any significant deviation from these baselines can be flagged as anomalous and contribute to a higher risk score.

Policy Orchestration

The contextual information is fed into a policy orchestration engine, which combines it with predefined risk policies and rules. This engine determines how different contextual factors contribute to the overall risk score and what adaptive actions should be taken (Table 2).

CHALLENGES AND MITIGATION STRATEGIES IN RadAC IMPLEMENTATION

Although RadAC offers significant advantages in enhancing database security, its implementation is not without challenges. These challenges span the technical, operational, and organizational domains, requiring careful planning and robust mitigation strategies. This section discusses the primary hurdles in deploying RadAC in advanced DBMS and potential approaches to overcome them.

Technical Challenges

Performance Overhead

Real-time risk assessment involves continuous monitoring, data collection, and complex computations, which can introduce significant latency and overhead in database operations. This is particularly critical for high-transaction-volume DBMS.

Mitigation: Efficient algorithms for risk calculation, leveraging in-memory computing, optimizing data collection mechanisms, and utilizing hardware acceleration is employed. Implement caching for frequently accessed risk scores and precompute risk for stable contexts.

Complexity of Risk Models

Designing accurate and comprehensive risk models that effectively capture all relevant contextual factors and their interdependencies is an inherently complex task. Overly simplistic models may overlook critical threats, whereas overly complex models can be difficult to manage and maintain.

Mitigation: Start with simpler models and refine them iteratively. Machine learning is used for automated risk model generation and adaptation. Expert systems and knowledge bases are employed to capture domain-specific risk intelligence.

False Positives and False Negatives

An inaccurate RadAC system can generate false positives (legitimate access requests flagged as high-risk) and false negatives (missed malicious requests). Both can lead to user frustration, operational disruptions, and security breaches.

Mitigation: Robust testing and validation of risk models should be implemented. Continuously fine-tune the thresholds and parameters. Human feedback was incorporated into the learning loop to reduce false alarms. Multiple risk indicators were used for cross-validation.

Data Integration and Heterogeneity

RadAC requires the integration of data from diverse sources (e.g., IAM, network logs, endpoint security, and threat intelligence feeds), which often come in different formats and protocols. Managing data heterogeneity and ensuring real-time synchronization are challenging.

Mitigation: Utilize data integration platforms, APIs, and standardized data formats. Data lakes or warehouses can be employed for centralized context storage. Implement robust data quality and validation checks.

Operational and Organizational Challenges

Policy Management and Governance

Defining, managing, and updating risk-adaptive policies can be complex, especially in large organizations with evolving security requirements. Ensuring policy consistency and avoiding conflicts are crucial.

Mitigation: Implement policy-as-code approaches, use centralized policy management tools, and establish clear governance processes for policy reviews and approvals. Formal methods are leveraged for policy verification.

User Acceptance and Transparency

Users may perceive dynamic access restrictions as intrusive or arbitrary, leading to resistance or attempts to circumvent the systems. A lack of transparency regarding how risk is assessed can erode trust.

Mitigation: Provide clear explanations of RadAC policies and their benefits. Offer mechanisms for users to understand why an access request is challenged or denied. Involve users in the design and testing phases of the system. User-friendly interfaces for adaptive authentication were implemented.

Skill Gap

Implementing and managing RadAC systems requires specialized skills in areas such as cybersecurity, data science, risk management, and database administration. However, a shortage of such expertise can hinder successful deployment.

Mitigation: Invest in training and upskilling of existing staff. Recruit talent with interdisciplinary expertise. Partner with security vendors or consultants specializing in RadAC.

Regulatory Compliance

Ensuring that RadAC implementations comply with various data protection regulations (e.g., general data protection regulation (GDPR), health insurance portability and accountability Act (HIPAA), and California consumer privacy act (CCPA)) while maintaining adaptability can be complex. The dynamic nature of RadAC may make it difficult to demonstrate compliance with static audit requirements [18].

Mitigation: Design the RadAC with compliance requirements in mind from the outset. Maintain detailed audit trails of all access decisions and risk assessments. Develop clear documentation of policies and their rationale (Table 3).

Table 3. Challenges and mitigation strategies in RadAC implementation for DBMS [19–20].

Challenge category	Specific challenge	Mitigation strategy
Technical	Performance overhead	Efficient algorithms, in-memory computing, hardware acceleration, and caching.
	Complexity of risk models	Iterative refinement, ML for model generation, expert systems.
	False positives/negatives	Robust testing, continuous fine-tuning, human feedback, multiple indicators.
	Data integration	Data integration platforms, APIs, standardized formats, and data quality checks.
Operational/ Organizational	Policy management	Policy-as-code, centralized tools, clear governance, and formal verification.
	User acceptance	Clear explanations, transparent feedback, user involvement, and user-friendly interfaces.
	Skill gap	Training, upskilling, talent recruitment, vendor partnerships.
	Regulatory compliance	Design for compliance, detailed audit trails, and clear documentation.

CONCLUSION

The proposed study acts as a pivotal advancement in securing advanced DBMS, moving beyond the inflexible methods of data acquisition to embrace flexible, context-aware authorization. This comprehensive study has explored the theoretical foundations of RadAC, highlighting its core principles of dynamic authorization, contextual awareness, risk quantification, and adaptive response. We have detailed the architectural components necessary for its implementation, including context collectors, risk assessment engines, policy decision points, and enforcement points, and discussed their integration into diverse DBMS environments, such as RDBMS, NoSQL, cloud-native, and blockchain databases. A thorough analysis of key risk factors—encompassing user, environmental, resource, and action-related attributes—underscores the multifaceted nature of risk assessment in RadAC. While the implementation of RadAC presents significant technical and operational challenges, including performance overhead, model complexity, and user acceptance, robust mitigation strategies are available through advanced technical solutions, clear governance, and user empowerment. The continuous evolution of cyber threats and the increasing complexity of data environments necessitate the adoption of such intelligent and adaptive security paradigms. Future research in RadAC will likely focus on enhancing the accuracy and explainability of AI/ML-driven risk models, developing standardized frameworks for interoperability, and exploring its application in emerging technologies like quantum computing and federated learning. Ultimately, RadAC is not merely an enhancement but a fundamental shift towards a more proactive, intelligent, and resilient approach to data security, crucial for protecting sensitive information in the ever-expanding digital landscape.

REFERENCES

1. Atlam HF, Azad MA, Alassafi MO, Alshdadi AA, Alenezi A. Risk-based access control model: A systematic literature review. Future Internet. 2020;12(6):103. doi: 10.3390/fi12060103.
2. Atlam HF, Yang Y. Enhancing healthcare security: A unified RBAC and ABAC risk-aware access control approach. Future Internet. 2025;17(6):262. doi: 10.3390/fi17060262.
3. Calvo M, Beltrán M. A model for risk-based adaptive security controls. Comput Secur. 2022;115:102612. doi: 10.1016/j.cose.2022.102612.
4. Dohare I, Singh K, Mohan Y. Fuzzy logic-based energy-efficient trust evaluation scheme in sensor assisted Industry 4.0. In: Ahmadian A, Srivastava S, Yadav AK, Kumar V, Kumar Srivastava P, editors. Smart Materials Engineering: Data-Driven Approaches and Multiscale Modelling. Cham: Springer; 2026. p. 103-124. doi: 10.1007/978-3-032-09540-4_6.

5. Farhadighalati N, Estrada-Jimenez LA, Nikghadam-Hojjati S, Barata J. A systematic review of access control models: Background, existing research, and challenges. IEEE Access. 2025;13:17777-17806. doi: 10.1109/ACCESS.2025.3533145.
6. Fleming C, Kundu A, Kompella R. Uncertainty-aware, risk-adaptive access control for agentic systems using an LLM-judged TBAC model. [Preprint]. 2025. arXiv:2510.11414. doi:10.48550/arXiv.2510.11414.
7. Hu VC. Access control on NoSQL databases. NIST Interagency/Internal Report (NISTIR) 8504. Gaithersburg (MD): National Institute of Standards and Technology; 2024 May. doi: 10.6028/NIST.IR.8504.
8. Kumar P. Next-generation secure authentication and access control architectures: Advanced techniques for securing distributed systems in modern enterprises. Int J Comput Exp Sci Eng. 2025;11(3):4966-4995. doi: 10.22399/ijcesen.3294.
9. Ugbaja US, Nwabekee US, Owobu WO, Abieba OA. Conceptual framework for role-based network access management to minimize unauthorized data exposure across IT environments. Int J Soc Sci Except Res. 2023;2(1):211-221. doi: 10.54660/IJSSER.2023.2.1.211-221.
10. Pu X, Jiang R, Song Z, Liang Z, Yang L. A medical big data access control model based on smart contracts and risk in the blockchain environment. Front Public Health. 2024;12:1358184. doi: 10.3389/fpubh.2024.1358184. PubMed PMID: 38605878.
11. Ross R, Pillitteri V, Graubart R, Bodeau D, McQuaid R. Developing cyber-resilient systems: A systems security engineering approach. NIST Special Publication 800-160, Volume 2, Revision 1. Gaithersburg (MD): National Institute of Standards and Technology; 2021 Dec. doi: 10.6028/NIST.SP.800-160v2r1.
12. Saura JR, Škare V, Dosen DO. Is AI-based digital marketing ethical? Assessing a new data privacy paradox. J Innov Knowl. 2024;9(4):100597. doi: 10.1016/j.jik.2024.100597.
13. Sifaoui A, Eastin MS, Wilcox GB, Doorey AM. The dark side of consumer privacy in the age of artificial intelligence. In: Scheinbaum AC, editor. The Darker Side of Social Media: Consumer Psychology and Mental Health. 2nd ed. New York: Routledge; 2024. p. 157-178. doi: 10.4324/9781003410058-11.
14. Soni V. AI and the personalization-privacy paradox: Balancing customized marketing with consumer data protection. Int J Comput Trends Technol. 2024;72(9):24-31. doi: 10.14445/22312803/IJCTT-V72I9P105.
15. Aljuaid TAYM, Wahab AWA, Idris MYII. Adaptable and dynamic access control decision-enforcement approach based on multilayer hybrid deep learning techniques in BYOD environment. Comput Mater Continua. 2024;80(3):4663-4686. doi: 10.32604/cmc.2024.055287.
16. Wang R, Li C, Zhang K, Tu B. Zero-trust based dynamic access control for cloud computing. Cybersecurity. 2025;8(1):12. doi: 10.1186/s42400-024-00320-x.
17. Vishwakarma RK, Pandey A, Kundnani P, Yadav AK, Singh N, Yadav S. Personalization vs. privacy: Marketing strategies in the digital age. J Mark Soc Res. 2025;2(5):177-191. doi: 10.61336/jmsr/25-05-20.
18. Ying S, Huang Y, Qian L, Song J. Privacy paradox for location tracking in mobile social networking apps: The perspectives of behavioral reasoning and regulatory focus. Technol Forecast Soc Change. 2023;190:122412. doi: 10.1016/j.techfore.2023.122412.
19. Zahedi SM, Fan S, Lee BC. Managing heterogeneous datacenters with tokens. ACM Trans Archit Code Optim. 2018;15(2):1-23. doi: 10.1145/3191821.
20. Ziv T, Whiteman JD, Sommerville JA. Toddlers' interventions toward fair and unfair individuals. Cognition. 2021;214:104781. doi: 10.1016/j.cognition.2021.104781. PubMed PMID: 34051419.

