

Analyzing Identity and Access Management (IAM) Misconfigurations in Cloud Databases

Aljazi Almarri ^{1,†}, Asayil Alawadh ^{1,†}, Maha Alsayed ^{1,†} and Muhammad Aasim Rafique ^{2,*}

¹ Department of Computer Science, College of Computer Sciences and Information Technology, King Faisal University, Al-Ahsa 36362, Saudi Arabia; 225000676@student.kfu.edu.sa (A.A.); 225002218@student.kfu.edu.sa (A.A.); 225128358@student.kfu.edu.sa (M.A.)

² Department of Information Systems, College of Computer Sciences and Information Technology, King Faisal University, Al-Ahsa 36362, Saudi Arabia

* Correspondence: mrafique@kfu.edu.sa

† These authors contributed equally to this work.

Abstract

Enterprises are more inclined towards cloud adaptation for services including cloud databases, but there is persistent concern about data security. One of the major data security vulnerabilities arises from misconfigurations in authorization and authentication mechanisms of data management system. Identity and Access Management (IAM) serves as a general framework for security configuration in cloud database services, yet its manual and static policy administration results in misconfigurations, which include excessive rights, policy drift, illegal access, and so on. Thus, comprehensive reporting and a deeper understanding of the efficacy of alternative IAM security procedures in reducing security risks are needed. This study adopts a systematic process that looks at common IAM misconfiguration patterns in cloud database systems and examines relevant studies published between 2016 and 2026 to assess the effectiveness of automated IAM configurations. The literature advocates that manual IAM configurations significantly contribute to privilege escalation and security violations in cloud database services, whereas automated IAM approaches provide stronger protection through continuous enforcement, real-time monitoring, and improved visibility into access behaviors. Furthermore, the study identifies critical research gaps in real-time remediation and DBaaS-aware automation, which are necessary to mitigate security risks faced by enterprises, reduce IAM-related vulnerabilities, and enhance confidence in adopting cloud database services.

Keywords: Identity and Access Management (IAM); cloud database security; Database-as-a-Service (DBaaS)

Academic Editor: Teng Zhou

Received: 16 May 2026

Revised: 11 June 2026

Accepted: 22 June 2026

Published: 26 June 2026

Copyright: © 2026 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the [Creative Commons Attribution \(CC BY\)](https://creativecommons.org/licenses/by/4.0/) license.

1. Introduction

According to Eurostat (<https://ec.europa.eu/eurostat/en/>, accessed on 21 June 2026), the usage of cloud computing services has increased by 7.42 percent in 2025, and more than half, 52.74 percent, of European enterprises are using paid cloud services. The trend is similar worldwide, and cloud computing has taken a significant role in technology development, deployment, and its usage, as it provides computing resources over the internet.

A key benefit for organizations and customers is the reduction of IT infrastructure costs with improved operational efficiency and support for rapid technological advancements. Albeit meritorious usages the cloud services are vulnerable, and users' confidence is reducing with the increasing breaches reported in 2025 (<https://owasp.org/>). Furthermore, users' concern about data breaches, unauthorized access, insecure APIs, and multi-tenancy risks has increased [1,2]. The security concerns arising from the widespread use of cloud computing need to be addressed as more businesses rely on cloud services to store and manage sensitive data.

Cloud database services, which include infrastructure usage for deployments of a DBMS to a managed DBMS in the form of Database-as-a-Service (DBaaS) platform, are widely adopted. The increase in their use also exposes vulnerabilities and security loopholes. The causes of most of the breaches are identified as simple misconfigurations, which elevate as a major security challenge in cloud database systems. Misconfigurations occur when security settings are improperly defined and left overly permissive, potentially exposing sensitive data to unauthorized access and resulting in confidentiality loss. Prior research indicates that many of these vulnerabilities stem from human errors during deployment and maintenance, such as publicly exposed databases, incorrect IAM roles, and disabled encryption [3].

Cloud infrastructure is dynamic and complex and is vulnerable to incorrect configurations, which include excessively permissive access controls. The flaw may remain undetected for long periods, thereby increasing the risk of large-scale data breaches. Although proprietary cloud providers offer security configuration tools such as AWS Config, Azure Security Center, and so on, to detect misconfigurations. The off-the-shelf solutions are mostly reactive and rely heavily on manual monitoring, which limits their ability to keep up with constantly evolving cloud environments [3]. Identity and Access Management (IAM) is a general framework for security configuration, but often organizations encounter implementation skills issues within cloud environments. They expose the environment to vulnerabilities related to unauthorized access, reputational damage, and regulatory compliance. Although cloud service providers offer an extensive range of permission settings, organizations must implement numerous authentication and authorization protocols to implement complete security [4]. It also requires robust IAM practices to mitigate the risk of unauthorized users gaining access to sensitive information stored in the cloud [5].

Security and safety are primary concerns which reduces the confidence of users in cloud adoption. A volatile scenario is presented in Section 1.1 to explain the challenges that arise from misconfigurations only. IAM frameworks are well understood and in use by the system and database administrators. Figure 1 presents a simple and standard IAM access architecture. However, the cloud has its own challenges, which are new for the administrators of systems and DBMS. A comprehensive understanding of the new challenges in the cloud popularity era is imperative to increase the confidence of users in the cloud. This study explores a focused area of vulnerabilities in cloud services for databases, i.e., the misconfigurations in cloud systems. A systematic approach is adopted in this study to collect and analyze the literature to respond to users' questions about IAM misconfiguration patterns in manual usage, the available alternative of automated configurations, and the effectiveness of automated configurations.

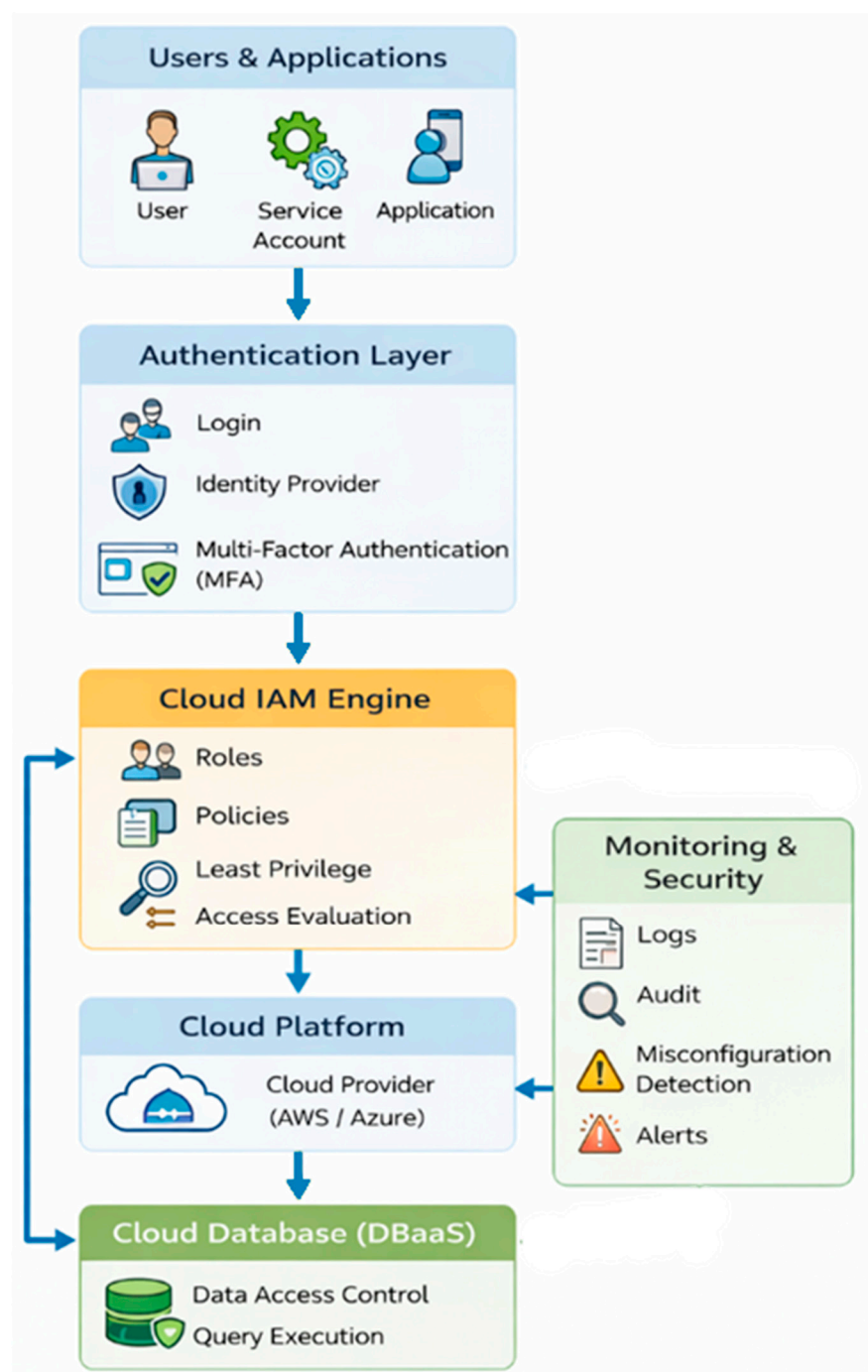


Figure 1. This figure illustrates the IAM architecture for secure access to cloud Database-as-a-Service (DBaaS) environments. Users and applications authenticate through an identity provider with multi-factor authentication (MFA). Access requests are evaluated by the IAM engine based on roles and policies following the least-privilege principle. Authorized requests are granted access to cloud database resources, while monitoring and logging components enable the detection of misconfigurations and unauthorized activities.

1.1. A Scenario to Explain IAM Misconfiguration

A healthcare service provider decides to migrate to the cloud to benefit from economies of scale, and the IT team commissions DBaaS to migrate all applications' data. Many applications are using Databases, and for operational convenience, a database administrator simply grants excessive permissions to an application service. As migrations from on-premises to the cloud are always cumbersome, during the course of migration new

permissions are added as new services are implemented, but old privileges never get revoked because of status quo bias. The patching paradox causes the service account to be bloated with excessive permissions and breaks the least privilege principle. If account credentials are found through even simpler social engineering methods, the attacker can take control of sensitive patient records, change contents in databases, and steal confidential information.

Such privilege accumulation may go unnoticed and often overlooked for longer stretches of time in a classic IAM management environment due to limited audits, fatigued resources, known lapses, and laziness. On the other hand, an automated approach is not affected by human factors and is proactive in nature. Furthermore, automation is always active and can incorporate changes seamlessly, monitor access behavior over time, assign privileges and track them in real-time, understand policy drift, and send alerts when excessive permissions are identified. In addition, advancements in AI can benefit IAM systems. This example sets the basis to explore the detailed analysis of DBaaS environments that may breed IAM misconfigurations and the merits and demerits of automated IAM configuration solutions in the cloud. The scenario is depicted in Figure 2 for visualization.

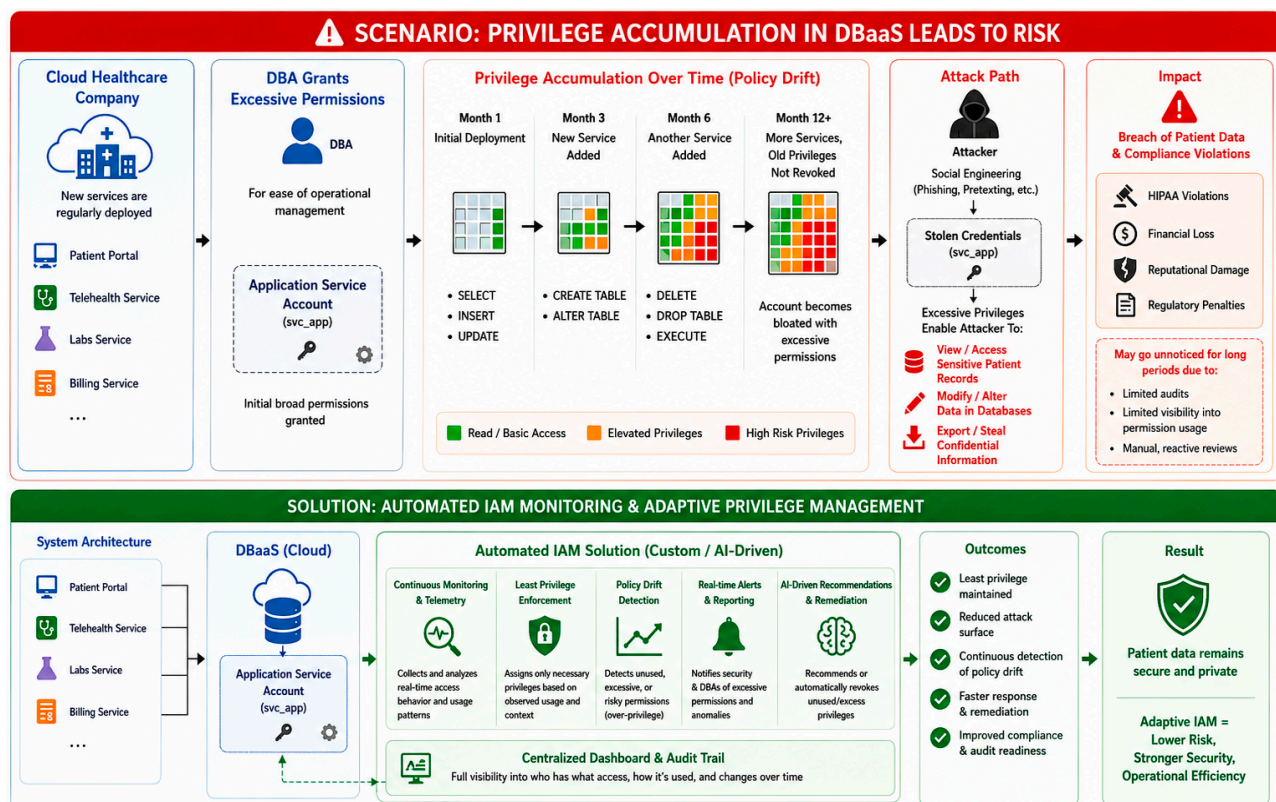


Figure 2. An example of healthcare information systems migration from premises to cloud DBaaS.

1.2. Novelty and Contributions

This study bridges the literature review gaps that remain unattended in earlier attempts to cover the challenges in cloud security and IAM mechanisms for database services in the cloud environment. Primarily, it focuses on IAM misconfigurations particular to DBaaS in cloud environments. Moreover, it is found that the existing surveys in the literature look at cloud security in a customary manner, whereas, with a new phenomenal transformation of on-premises to cloud migrations, a detailed application-specific analysis is required. This study covers the ground to help in circumvention of threats by providing common IAM misconfigurations reported in the literature and security risks in cloud-

hosted database systems. Another significant contribution is a unique three-prong strategy for literature review. Firstly, it opted for a PICOC strategy for a systematic literature review of IAM misconfigurations in DBaaS platforms. Second, it drills down and identifies the prevalent IAM misconfiguration patterns reported in the literature, such as over-provisioned privileges, policy drift, poorly configured roles, and orphaned service accounts. Third, it contrasts manual IAM configuration with automated IAM approaches to understand their strengths, weaknesses, and effect on security governance. Furthermore, the study integrates existing evidence on the effectiveness of using automated IAM mechanisms to lower misconfiguration-related risks and highlights research gaps in DBaaS-aware IAM automation, real-time remediation, and intelligent access governance directions for future studies.

The rest of the study is organized as follows: Section 2 provides the background of the available studies exploring similar problems. Section 3 provides the methodology adopted in this study for the systematic review and its results. Section 4 summarizes the selected literature, and Section 5 details the findings of the study with discussion and identifying future directions. Section 6 summarizes and concludes our study.

2. Literature Review

Cloud security is a wide discipline, and this study is pertinent to IAM misconfiguration issues in cloud environments, with a particular focus on DBaaS platforms. Its primary focus is DBaaS and IAM concepts, and it compiles the related literature to serve as a basis for the comprehensive literature review that follows. This review emphasizes the importance of understanding IAM in cloud databases to effectively identify risks, misconfigurations, and mitigation strategies.

DBaaS refers to cloud-based database systems designed with virtual environments, enabling scalable and on-demand data storage and management [6]. The operational advantages of DBaaS, such as cost savings, high availability, performance optimization, and scalability, increase confidence in usability [7]. However, the literature clearly advocates for the security risks in DBaaS, as outsourcing database management to cloud providers reduces organizational authority over access management, configuration, and auditing procedures. This leads to significant exposure to misconfigurations and access-related vulnerabilities [7]. The security issues have motivated many studies to strengthen IAM systems to protect DBaaS platforms. IAM is crucial for regulating access in cloud databases by defining authentication, authorization, and privilege boundaries for users, applications, and services. IAM is recognized as an essential element of comprehensive cloud security frameworks, especially in zero trust systems where contextual access decisions and identity verification are constantly enforced. Integrating authentication, authorization, identity federation, lifecycle management, and auditing with unified governance structures across multi-cloud environments is essential for effective cloud security are inherent in IAM [8].

Modern IAM systems offer fine-grained access control capabilities in the cloud. However, their complexity frequently results in configuration problems in peculiar cloud environments [3]. Consequently, a weak IAM design, incorrect role assignment, and inadequate enforcement of security measures result. Multi-factor authentication (MFA) and role-based access control (RBAC) are among the main causes of unauthorized access and data leakage in cloud systems. The dynamic workloads, continuously evolving user roles, and the increasing use of non-human identities such as service accounts and application credentials exacerbate the challenges. As cloud infrastructures grow, manual updates in static IAM policies stop adaptation to the changing access requirements, which leads to policy drift and privilege accumulation over time [9]. Consequently, misconfigurations creep into IAM, causing security issues, which is not an absence of security controls.

IAM security is widely covered in the literature, and [10] presents a systematic review of IAM requirements in enterprises, highlighting the potential of self-sovereign identity to enhance cloud security and user authentication. Another work presents distributed ledger technology (DLT) as a promising approach for decentralized identity management [11]. Also, adaptive IAM systems are presented in the literature that use contextual data to dynamically adjust access policies, offering more situation-aware security in environments with rapidly changing user contexts and roles [12].

The rapid evolution of technology introduces challenges in managing large-scale, heterogeneous devices, requiring conceptual frameworks that ensure both security and scalability. IAM frameworks that align security policies with organizational goals are presented in [13,14]. Furthermore, the integration of Artificial Intelligence (AI) in IAM has been explored to enhance threat detection and mitigate anomalous behavior to prevent fraudulent activities in large-scale user environments, thereby improving the accuracy of access control mechanisms [15,16]. Additional studies highlight the role of Explainable AI (XAI) to enhance transparency and trust in automated authentication decisions. It bridges the gap between machine-driven access decisions and human oversight [15]. AI-driven IAM significantly improves data security and reduces fraud in critical systems like finance, healthcare, and education, and highlights the important role of automated access management [17].

Previous research increasingly highlights IAM misconfigurations, rather than the lack of IAM tools, as the primary cause of cloud database security in dynamic cloud infrastructure. This observation necessitates a systematic review of IAM misconfigurations and mitigation techniques in DBaaS systems.

3. Methodology

Security in cloud-hosted databases in diverse deployment configurations remains a concern for both organizations and users. To address the challenges arising from rapid technological advancement and widespread cloud adoption, this study employs a systematic research design aimed at providing clear and evidence-based answers to emerging security questions. The primary focus of the study is IAM misconfigurations in cloud databases. Another objective is to identify improved configuration strategies for IAM control mechanisms and to mitigate security risks. The study adopts a comprehensive PICOC framework to structure the research questions and to ensure methodological rigor and quality in this investigation.

3.1. PICOC Framework

The PICOC framework structured our study in a systematic and organized manner. Given that cloud services, security, and databases are broad domains, the focus can be easily diverted. The PICOC maintains conceptual clarity and research direction by identifying keywords related to population, intervention, comparison, outcome, and context. Moreover, the framework defines the scope of the study and supports the formulation of precise research questions. Furthermore, it specifies the target population, remediation approaches for addressing IAM misconfigurations, comparison baselines, expected outcomes, and the relevant operational context. PICOC enables the decomposition of the study into clearly defined and measurable components. It also supported the systematic identification of relevant literature addressing IAM misconfigurations in cloud database environments.

Table 1 presents the outcomes of the PICOC exercise, including the mappings and associated synonym terms used to construct the research questions outlined in Table 2, as well as the search strings developed to identify relevant literature. The identified keywords guarantee an organized and methodical description of the review scope, which is

necessary for carrying out a targeted and repeatable survey in the field of cloud database security. Numerous discussions and brainstorming sessions helped to select the keywords related to the topic. IAM misconfigurations are interleaved with organizational, technological, and contextual components. The focus is closely associated with DBaaS platforms by explicitly specifying the population as Cloud DBMS environments.

Table 1. The PICOC mapping and associated synonym terms identified for the design of this study.

PICOC Element	Example (PICOC)	Example (Synonyms)
Population	Cloud DBMS	Cloud databases, managed database services
Intervention	Automated IAM Security	Automated access control, IAM security automation, policy analyzers
Comparison	Manual Configurations	Manual IAM setup, manual access control
Outcome	Secure Configurations	Reduced misconfigurations, improved IAM reliability
Context	Cloud-based Database Environments	DBaaS environments, cloud-hosted DB systems

Table 2. The research questions formulated from keywords identified in Table 1.

Question ID	Research Question
RQ1	What IAM misconfigurations arise in Cloud DBMS when manual configuration is used?
RQ2	How effective are automated IAM security mechanisms in improving secure configurations in Cloud DBMS?
RQ3	To what extent do automated techniques outperform manual configurations in reducing misconfigurations in Cloud DBMS environments?

Automation is ubiquitous, and instead of manual IAM configuration procedures, security research is increasingly focusing on automated IAM security measures. Therefore, it is reflected in the intervention component. Since manual security settings are the simplest and most widely used methods, it is also adopted in cloud deployments. Moreover, they are often stated as a primary cause of IAM misconfigurations, and thus purposefully selected for the comparison baseline. Secure configurations and reduced misconfigurations are highlighted in the outcome section, which directly relates to the assessment goals of this study. Finally, freezing the context guarantees the analysis is bounded to IAM issues specific to DBaaS.

3.2. Research Questions

The essence of an effective study is posing precise questions, and a systematic framework like PICOC leverages this articulation. This study formulates research questions based on the PICOC exercise and the terms identified as the result of the exercise (Table 1). The formulated questions are articulated in Table 2 and guide the systematic literature review by focusing on key aspects of IAM misconfigurations, their impact, and existing mitigation approaches in cloud database environments.

The research questions individually target a specific dimension of security-related challenges of IAM in cloud DBMS environments and enable a structured synthesis of existing studies. Particularly, RQ1 focuses on finding IAM misconfigurations that result from manual configuration procedures. Previous research identifies human-driven policy management as a primary source of security vulnerabilities in cloud databases. This inquiry helps to identify recurrent misconfiguration patterns and creates a baseline understanding of the problem. Whereas RQ2 probes the efficacy of automated IAM security procedures to keep up with the growing trend in the literature towards automation, AI-assisted analysis, and continuous enforcement. Lastly, RQ3 offers a comparative analysis

of manual and automated configuration settings that enables this study to integrate conceptual and empirical information from prior investigations.

3.3. Selection of Digital Libraries

Appropriate digital libraries were selected to ensure the inclusion of relevant and credible sources in this review. The selected databases provided access to high-quality, peer-reviewed publications in computer science, cybersecurity, and information systems. Table 3 summarizes the selected digital libraries and their respective areas of expertise.

In order to guarantee thorough coverage of excellent, peer-reviewed research in database systems, cloud computing security, and IAM, appropriate digital libraries were chosen for this evaluation as shown in Table 3. The selected libraries are well known for indexing reputable journal articles and conference proceedings in computer science. As IAM misconfigurations in the cloud DBMS context span various domains of the CS discipline like software engineering, cloud infrastructure, database security, and access control research, these databases are deliberately chosen. Moreover, the use of a variety of digital libraries reduces the possibility of publication bias and guarantees the inclusion of both conceptual surveys and empirical studies. Additionally, advanced search and filtering capabilities made it possible to execute PICOC-guided search strings precisely, increasing recall and accuracy during study identification. The selected digital libraries as a whole provide a strong foundation for the systematic search approach and guarantee that the final dataset appropriately represented the state of the research on IAM misconfigurations in cloud database environments.

Table 3. List of the chosen libraries to search authentic literature for this study.

Database	URL	Area	Advanced Search
IEEE Xplore	https://ieeexplore.ieee.org	Cloud Computing, Cybersecurity	Yes
ACM Digital Library	https://dl.acm.org	Computer Science	Yes
Scopus	https://www.scopus.com	Engineering, Technology	Yes
Web of Science	https://www.webofscience.com	Interdisciplinary	Yes
Science Direct	https://www.sciencedirect.com	Data Security, Information Systems	Yes

Search Strategy

To ensure comprehensive coverage of relevant studies, search queries are constructed based on the PICOC framework by combining keywords related to cloud cybersecurity, DBaaS, and IAM. Moreover, Boolean operators (AND, OR) are used to expand and refine the search across the selected digital libraries.

The primary search string used in this study is given in Table 4. The search is applied to titles, abstracts, and keywords in all libraries listed in Table 3. The same query can be used to reproduce the results and build on this study. A total of 115 studies are found with this query, which were later filtered with exclusion and inclusion criteria and quality check.

Table 4. The query used to search the related literature for the planned study.

Query
("Cyber security" OR "Cloud security" OR "Cloud computing security")
AND ("Database as a Service" OR DBaaS OR "Cloud database")
AND ("Identity and Access Management" OR IAM)
AND (misconfiguration OR "access control issues" OR "security challenges" OR automation)

3.4. Inclusion and Exclusion Criteria

The study's effectiveness and relevance are ensured with clear and rigorous filtering criteria. The inclusion and exclusion criteria are strictly followed as listed in Table 5. It ensures objectivity by considering factors like period, language, type of literature, source type, impact source, accessibility, and relevance.

Table 5. The inclusion and exclusion criteria defined for this study.

Criteria Type	Example
Period	Inclusion: 2016–2025; Exclusion: before 2016
Language	Exclusion: Non-English publications
Type of Literature	Exclusion: Reports, newsletters, blogs
Source Type	Inclusion: Articles from Conferences or Journals Exclusion: Articles from books
Impact Source	Exclusion: Low-impact journals (IF < 0.5)
Accessibility	Exclusion: Restricted or unavailable sources
Relevance	Exclusion: Unrelated topics

The criteria enforce methodological consistency, relevance, and rigor for the systematic study. As the cloud is a relatively new phenomenon, omitting the publication period to 2020–2025 was considered at first, which was later revised with the inclusion of an extended four-year period. This ensured the collection of enough literary work. The collection is concentrated on modern cloud-native architectures and misconfiguration vulnerabilities applicable to DBaaS systems. The peer-reviewed journal and conference articles are subject to rigorous academic scrutiny; restricting the review to these sources improved the findings' credibility. Moreover, non-English publications were excluded to ensure consistency and accurate interpretation of technical content. Gray literature, including reports, newsletters, Q&A, and blogs, was excluded because of unauthentic peer-reviewed validation. Furthermore, to preserve methodological and scholarly quality, publications from low-impact journals were excluded. To guarantee the review's reproducibility and transparency, restricted and unavailable sources were excluded. Additionally, only studies that directly addressed IAM, access control, or misconfigurations in cloud database systems were included because of the application of relevance-based filtering.

3.5. Quality Assessment Criteria

The purpose of the Quality Assessment (QA) checklist is to evaluate the methodological rigor, reliability, and relevance of each selected study. The QA approach applied in this research ensured that only studies with clearly defined objectives, sound methodologies, and meaningful contributions to cloud database security and IAM were included in the final analysis. Each criterion in the checklist assessed key aspects of study quality, including methodological soundness, empirical or theoretical validation, research clarity, and the discussion of limitations. The quality of each study was evaluated using a standardized scoring scheme (0 = No, 0.5 = Partially, 1 = Yes), as presented in Table 5. This structured and transparent assessment process supported the consistent selection of high-quality studies and strengthened the reliability and evidence-based nature of the review findings.

The Quality Assessment (QA) checklist used in this study is presented in Table 6. It is designed to further strengthen the filtering process and ensures that only methodologically rigorous and thematically relevant studies were included in the review. The selected literature after QA assessment is pertinent to IAM misconfigurations in cloud database environments, and it removes weak and ambiguous research designs from the searched literature. Furthermore, with the QA, this review remains tightly focused on DBaaS-specific access control challenges rather than general cloud security issues. The adopted scoring scheme

provides a transparent and consistent evaluation process, enabling objective comparison across studies while minimizing subjective bias during the selection process.

Table 6. Quality Assessment (QA) Checklist Rendered in this Study.

QA Question	Example	Level of Participation
Do the authors clearly define their research objectives?	Yes, objectives are explicitly stated.	0 = No; 0.5 = Partially; 1 = Yes
Is the methodology well described and justified?	Clear explanation of approach used.	0 = No; 0.5 = Partially; 1 = Yes
Does the paper specifically address IAM misconfigurations in cloud database environments?	Focused on IAM misconfigurations in cloud database environments	0 = No; 0.5 = Partially; 1 = Yes
Are findings supported by empirical or theoretical evidence?	Data or analysis results are presented.	0 = No; 0.5 = Partially; 1 = Yes
Do the authors discuss limitations or threats to validity?	Limitations acknowledged in discussion.	0 = No; 0.5 = Partially; 1 = Yes
Is the study's contribution relevant to the research questions?	Provides applicable results for IAM security.	0 = No; 0.5 = Partially; 1 = Yes

3.6. Data Extraction Process

Data Extraction is a crucial exercise for the analysis and to provide responses to the RQs posed in Table 2. This study uses a form with the fields given in Table 7 to systematically collect and organize essential information from the studies filtered after the QA. This examines how different studies contributed to understanding IAM misconfigurations in cloud database environments. The extracted data includes the study type, research objectives, employed technologies, IAM processes examined, evaluation methods, key findings, and identified challenges and research gaps.

Table 7. Data extraction form designed for this study.

Classification/Field	Description and Example
Research Type	Theoretical or empirical; e.g., theoretical survey paper for IAM misconfiguration.
By Process Phase or Stage	Refers to the IAM lifecycle stages such as manual configuration, automated enforcement, monitoring, auditing, or remediation.
By Technology or Framework	Automated IAM tools, access control analyzers, or automation-based security frameworks.
By Application Field or Domain	Cloud DBMS and database access control environments.
Gaps and Challenges	Limitations of manual IAM configurations and challenges in automating IAM security in Cloud DBMS
Findings and Results	Outcomes such as improved detection accuracy, reduced privilege escalation or enhanced policy enforcement.
Evaluation Method	Type of validation performed, e.g., simulation, benchmark testing, prototype testing, or case study.

Table 7 lists fields in the form to systematically capture the key characteristics and contributions of each selected study related to IAM misconfigurations in cloud database environments. Classifying studies by research type enabled differentiation between theoretical analyses and empirical evaluations, supporting a balanced synthesis of conceptual understanding and practical evidence. Categorizing studies according to IAM misconfiguration stages allows the review to trace how misconfigurations arise across the IAM lifecycle, from manual configuration to automated enforcement, monitoring, and remediation. The inclusion of technology- and framework-related fields facilitates the identification of automation-based solutions, access control analyzers, and security frameworks

proposed to address IAM configuration challenges. Furthermore, extracting information on application domains ensures that the findings remain focused on cloud DBMS and database access control contexts rather than general cloud security domains. Finally, classification fields related to identified gaps, challenges, findings, and evaluation methods support cross-study comparison, enabling the review to highlight recurring limitations of manual IAM practices, assess the effectiveness of automated approaches, and identify opportunities for further research in IAM governance tailored to DBaaS environments.

4. Synthesis of Selected Studies

This section synthesizes results from previous studies indicating recurrent security issues, IAM misconfiguration patterns, and mitigation strategies in cloud and DBaaS environments. Existing literature extensively examines security issues in cloud environments, emphasizing how challenging it is becoming to implement uniform security rules across various service types like SaaS, PaaS, and IaaS. Confidentiality, integrity, and authentication are still fundamental security principles, but several studies show that malware, DDoS attacks, insecure APIs, and configuration-related vulnerabilities commonly undermine these goals [1]. The shared responsibility model between cloud service providers and clients is strengthened by survey-based research, which highlights that cloud security risks go beyond conventional threats and include insider misuse, multi-tenancy vulnerabilities, compliance gaps, and emerging AI-driven attack vectors [2].

In addition to these challenges, insider misuse, configuration weaknesses, inadequate monitoring across service layers, and insecure APIs pose ongoing security risks to cloud-based software systems. In-depth polls also highlight the need for cloud security management to incorporate encryption, IAM, and continuous monitoring in order to handle both established and new threats, including supply-chain attacks, ransomware, and container vulnerabilities [18].

Recent surveys and systematic studies determine that misconfigurations and human error are the main causes of cloud security problems. A significant percentage of high-impact security events are still caused by misconfigured resources, excessive privileges, and incorrect access control settings, despite the fact that mechanisms like encryption and multi-factor authentication (MFA) greatly lower breach rates [3]. Further research supports these conclusions by demonstrating how, even with the implementation of technical safeguards like encryption, auditing, and anomaly detection systems, misconfigured cloud resources, inaccurate IAM policies, and inadequate monitoring continue [6,19]. When taken as a whole, this body of literature emphasizes that a major flaw in cloud security architectures is still misconfigurations rather than a lack of security measures [20].

Within cloud database and DBaaS environments, the literature shows that decreased organizational control over access management and auditing procedures and outsourced administration have increased security risks. According to surveyed studies, cloud databases are especially vulnerable to weak access restrictions, misconfigured database services, unsecured APIs, and insufficient auditing procedures, all of which can lead to policy violations, unauthorized access, and data leaks [21]. These risks are further increased by the shared infrastructure and multi-tenant characteristics of DBaaS platforms, which provide cross-tenant exposure in the event that identity and access restrictions are not configured correctly.

Although tenant-level access separation, encryption, continuous monitoring, and automated auditing tools are frequently suggested mitigation techniques, research shows that their efficacy is strongly correlated with proper IAM policy configuration and enforcement. As a result, IAM becomes essential for securing cloud database setups. As a fundamental element of IAM security in cloud environments, several studies also concentrate on strengthening authentication procedures. Traditional single-factor authentication

is inadequate against contemporary cloud risks, including identity theft and session hijacking, according to Alsirhani et al. To improve defense against unwanted access, their work suggests sophisticated authentication techniques like multi-factor authentication and context-aware identity verification. Even in intricate and dynamic cloud systems, these strategies seek to strengthen IAM security by lowering the possibility of identity misuse [22].

Across the surveyed literature, security breaches in cloud and DBaaS systems are frequently attributed to IAM misconfigurations. Excessive permissions, unmanaged service accounts, lax enforcement of least-privilege principles, policy drift, and inadequate segregation of roles are among the often-cited problems [23–25]. Especially in dynamic and distributed cloud infrastructures, these misconfigurations frequently result in privilege escalation and illegal data access. Several studies further investigate how IAM misconfigurations can lead to privilege escalation attacks, demonstrating real-world exploitation scenarios and proposing automated techniques to detect and repair such vulnerabilities [26,27]. The issue is made worse in cloud environments, where managing access control policies and identity assignments becomes more challenging, increasing the probability of inaccurate configurations and improper access control mechanisms [5,27].

The limits of traditional methods in obtaining scalable tenant isolation and fine-grained governance are highlighted by research on identity management and access control for multi-tenant DBaaS settings. This study highlights challenges such as weak access control mechanisms, data breaches, malicious insider activities, and cross-tenant leakage. To improve isolation and security in shared DBaaS infrastructures, existing approaches indicate the use of enhanced access control mechanisms, encryption techniques, and multi-layered security strategies [28].

Despite improvements in access visibility enabled by privilege monitoring, anomaly detection, and continuous auditing, the literature identifies a number of enduring constraints despite improvements in visibility into access behaviors brought about by advancements in privilege monitoring, anomaly detection, and continuous auditing. Current methods often depend on reactive alerts, human inspection, or static baselines, which limits their capacity to proactively and widely prevent misconfigurations. Survey results increasingly indicate that traditional, manually managed IAM systems are inadequate for upholding secure access control governance as cloud environments continue to change [4,5,29].

Current methods for fine-grained access control in relational database management systems concentrate on incorporating policy enforcement right into the query processing phase. QFilter, a framework created to effectively enforce fine-grained access control policies during query execution, is proposed by Mirabi and Binnig. Instead of applying all permission rules for each query, the method blends control checks with query processing to analyze only pertinent policies. The system dramatically lowers enforcement overhead while maintaining query efficiency by improving policy evaluation during execution and filtering policies based on query attributes. Such database-level enforcement systems can provide scalable and effective authorization in environments with multiple access control policies, according to experimental results [30].

To secure sensitive data in large-scale cloud data settings, fine-grained access control and privacy protection measures are crucial. Elangovan and Umamaheswari talk about how cloud data protection frameworks combine access control, authentication, and encryption to prevent unwanted access to private data kept in cloud infrastructures. Their study emphasizes the significance of granular access control strategies that govern user interactions with protected information while guaranteeing data integrity and confidentiality. These frameworks provide safe data storage and exchange in cloud-based data

platforms while preserving system efficiency and usability by integrating robust encryption techniques with access control enforcement and monitoring systems [31].

According to recent studies, AI-driven analytics can improve IAM security in cloud environments by detecting threats in an adaptable manner. Real-time anomalies, including insider threats, privilege abuse, and abnormal access activities, are detected by AI-enhanced security frameworks that examine identity behavior, access patterns, and contextual data. These methods enhance detection accuracy and allow for automated reaction mechanisms and scalable monitoring in large-scale multi-tenant systems by continually learning from dynamic cloud workloads [32].

For multi-cloud systems, Gurram suggests a single IAM governance framework that combines policy harmonization, adaptive authentication, automated lifecycle control, centralized identity management, and AI-enhanced monitoring. The study highlights the role of intelligent IAM automation in lowering security misconfigurations by showing that organizations lacking unified identity systems are 81% more susceptible to credential-based attacks, while automation lowers orphaned accounts by 83% and privilege escalation risks by 67% [33].

Although Attribute-Based Access Control (ABAC) has become a popular methodology for implementing fine-grained authorization in complex systems, it can be challenging and error-prone to manually define and maintain a large number of access control policies. Automated policy mining methods that extract ABAC rules directly from authorization data and access logs have been the subject of recent research. Perez-Haro and Díaz-Pérez suggest a method that uses affiliation networks and biclique analysis to examine user, resource, and permission relationships in order to automatically generate compact and consistent ABAC policies. The approach eliminates the need for human policy engineering while enabling the creation of context-aware and fine-grained authorization rules by analyzing recurrent access patterns and attribute correlations. In complicated systems with substantial amounts of authorization data, such automated policy mining techniques can facilitate scalable IAM [34].

IAM is becoming less of a stand-alone control mechanism and more of an essential part of cloud security automation. Pitkar shows how AI-driven correlation and orchestration are used by contemporary cloud security architectures to narrow the gap between threat detection and response. AI-powered orchestration platforms enable real-time access policy enforcement, quicker containment, and improved visibility across dynamic cloud infrastructures by connecting identity behavior with security events through the integration of IAM telemetry into continuous security pipelines. This method lessens the need for human involvement while promoting adaptive security governance [35].

Automated risk detection and remediation techniques greatly enhance cloud security governance, according to recent research on Cloud Security Posture Management (CSPM). According to Boamah's analysis, CSPM platforms carry out automated remediation in multi-cloud setups, continually monitor cloud resources, identify misconfigurations, and evaluate compliance standards. The study highlights CSPM as a workable method for handling configuration drift, excessive privileges, and policy violations in dynamic cloud infrastructures by reporting significant decreases in misconfiguration events and detection times [36].

In addition, IAM is recognized as a fundamental pillar of cloud security, overseeing authentication, authorization, and access control in distributed environments. IAM frameworks provide structured mechanisms for managing identities, roles, and permissions. These frameworks allow secure authentication and authorization processes across complex and distributed systems using interoperable and scalable identity management [37].

The reviewed IAM studies conclude that the primary source of significant risks in cloud-based IAM management systems is misconfiguration. Moreover, automated IAM

mechanisms and least-privilege-oriented approaches are identified as essential for mitigating misconfiguration-driven risks and strengthening system security. Incorrect role definitions, over-privileged identities, unmanaged service accounts, and policy drift enable unauthorized access and privilege escalation, even in the presence of robust security controls such as encryption and multi-factor authentication. In the context of shared responsibility models, outsourced administration, limited visibility, and inadequate auditing significantly expand the attack surface and increase the likelihood of sensitive data disclosure. In DBaaS environments, where responsibility is shared and administrative control is partially outsourced, these IAM weaknesses significantly expand the attack surface and increase the likelihood of sensitive data exposure.

5. Analysis of Selected Studies

An elegant approach to assess the correct inclusion of literature using a systematic literature review is the analysis of the frequently used terms and phrases in the filtered literature. Figure 3 shows a keyword co-occurrence network created with VOSviewer for the selected studies. The network identifies IAM and cloud computing as the two most prevalent and closely related research themes in the examined literature. It is also evident that identity governance techniques are crucial for protecting distributed cloud infrastructures, which is visible in strong semantic linkages found between IAM, access control, security, identity management, data protection, and auditing.

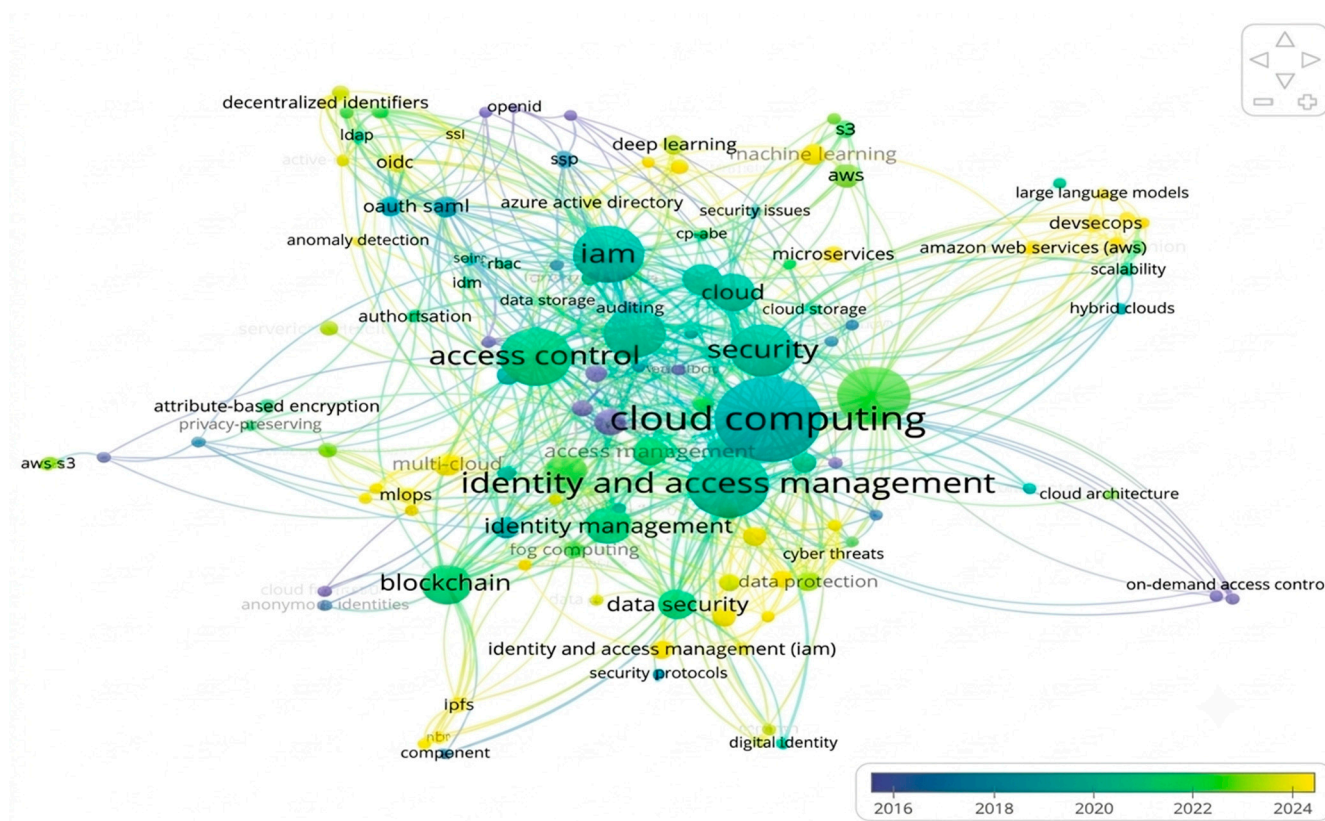


Figure 3. Keyword Co-occurrence Analysis of the Selected Studies for this Review.

Figure 3 also provides evidence in support of the three research questions addressed in this study. The frequency depicted by the sphere size and the correlations depicted by connections show IAM, access control, security, auditing, and cloud computing appearances. It reinforces that IAM governance is currently an important research direction for

cloud environments and supports RQ1 on common IAM misconfigurations. The increasing number of terms specific to automation, machine learning, identity governance, and multi-cloud security means that research interest in automated IAM approaches is emerging, supporting RQ2. In addition, the identified transition from static identity management concepts towards intelligent and adaptive security mechanisms points out a much wider trend: the shift away from manual IAM administration to more automatic governance models emphasizing further support for similarities provided in RQ3.

The chronological progression of study subjects from 2016 to 2025 is further demonstrated by the overlay color gradient. Prior research (blue–purple nodes) mostly concentrated on fundamental authorization standards and identity protocols like LDAP, SAML, OAuth, and OpenID. On the other hand, more recent articles (green–yellow nodes) place a greater emphasis on new paradigms, such as multi-cloud governance, DevSecOps, hybrid cloud environments, decentralized IDs, and machine learning-driven security measures.

This progression suggests a transition from conventional identity provisioning models to intelligent, automated, and adaptive access control frameworks created to handle changing security issues, such as IAM misconfigurations, risks of privilege escalation, and the difficulties of enforcing policies in cloud and DBaaS environments. This systematic literature review examined IAM misconfigurations in cloud and DBaaS environments to address the three research questions defined in Section 3. After applying the inclusion, exclusion, and quality assessment criteria, a total of 20 primary studies were selected for analysis. The PRISMA-Style flow graph depicting the process to apply exclusion criteria and quality assessment is given in Appendix B. The results indicate that manual IAM configurations are frequently associated with policy drift, excessive privileges, misapplied role assignments, and insufficient privilege separation, which collectively contribute to privilege escalation and unauthorized access in distributed cloud environments

5.1. RQ1: Common IAM Misconfigurations in Cloud DBMS

The literature research repeatedly shows that the limitations of manual configuration procedures when applied to dynamic and large-scale systems are the main cause of IAM misconfigurations in cloud DBMS environments. Static IAM policies are challenging to accurately maintain in cloud DBMS platforms due to rapid changes in users, services, workloads, and access requirements, in contrast to traditional on-premises environments. Role-related problems, such as too permissive roles, improper role inheritance, and poorly defined privilege boundaries, are among the most common misconfiguration types. In DBaaS platforms, where access control is externally maintained by cloud providers, manual role assignment frequently breaks the principle of least privilege by providing more access than necessary and directly exposing sensitive database resources [21].

Another major source of misconfiguration is identity and account management issues. Non-human identities, such as service accounts and application credentials, are often overprivileged and under-monitored, according to several studies. Due to the lack of systematic review procedures, these identities frequently face challenges beyond their operational requirement, resulting in persistent attack vectors that are rarely found by manual audits [23]. Furthermore, in manual IAM setups, policy lifecycle mismanagement becomes a serious problem. Despite changing workloads and access patterns, IAM policies frequently stay the same after they are implemented. This increases the risk of privilege escalation and unauthorized data access in cloud DBMS systems by causing policy drift and privilege accumulation over time. Finally, audit and monitoring gaps are highlighted in the literature as an important weakness in manual IAM management. Timely detection of misconfigurations is difficult due to limited runtime visibility, delayed log analysis, and inadequate tenant-level isolation, especially in DBaaS systems where organizations do not

have direct control over infrastructure-level access enforcement [7]. The results show that manual IAM settings are impractical due to the size, complexity, and ongoing expansion of cloud-hosted database systems, making misconfigurations a permanent and systemic security risk.

5.2. RQ2: Effectiveness of Automated IAM Security Tools

The analyzed studies show that traditional, manually managed IAM techniques lack the flexibility and visibility needed to secure modern cloud environments, building on the limitations identified in the previous section. In distributed cloud infrastructures, incorrect access permissions can go undetected until exploitation takes place since static regulations and recurring audits are insufficient [5]. By facilitating regular policy evaluation, real-time monitoring, and dynamic enforcement of least-privilege principles, automated IAM security methods overcome these constraints. Automation of IAM strategies effectively reduces human error, policy drift, and excessive privilege accumulation. The automation often uses modification of access rules in response to shifts in workloads, identities, and usage patterns. Nonetheless, automation operates under certain assumptions that may result in an optimization-enforcement tradeoff in DBaaS. For instance, currently some automation strategies assume that identities are stable and access patterns are predictable. Moreover, it ensures that identity and permissions across disparate cloud resources are identically distributed. Whereas DBaaS platforms support dynamic workloads, multi-tenant architectures, and database-specific privilege models that evolve. Thus, correct evaluation of the access relationships and enforcement of the least-privilege principles increase the complexity of optimization.

Alternatively, AI-driven automation improves IAM efficacy by facilitating proactive detection of anomalous access behaviors and erroneous configurations. However, rule-based and policy template-based tools dominate existing IAM security to identify misconfigurations. Although these approaches are effective in identifying known violations, they have limited capacity to spot unseen privilege relationships, access requirements depending on context, and authorization relating specifically to tenants. Consequently, these rule-based systems are prone to crucial false positives by classifying valid access patterns as threats and are unable to identify surfacing configuration weaknesses.

Machine learning and graph-based analysis have proven the modeling of the complex permission linkages and finding hidden privilege escalation channels that are often missed in manual examinations [38]. For instance, Raja Mohan et al. demonstrate that incorporating Natural Language Processing (NLP) and Graph Neural Networks (GNNs) into IAM configuration analysis automatically detects incorrect role settings and permissions in AWS environments [38]. Similarly, graph-based security analysis approaches have demonstrated the ability to model complex permission dependencies and to identify high-risk privilege relationships and attack paths in large-scale cloud environments [39].

The trade-off between precision and false positive rates surfaces with complex automated IAM governance. Overly sensitive detection mechanisms may result in higher security visibility but also inundate administrators with frequent irksome alerts. Alternatively, conservative detection thresholds can help mitigate alert fatigue but increase the risk of missing dangerous misconfigurations that carry high security risks. Hence, future DBaaS IAM solutions need to balance detection accuracy with context and the operational scalability of an entire application ecosystem while reducing administrative overhead.

In summary, it is emphasized that existing automated IAM solutions have merits and costs. Most tools in practice are rule-based and lack a thorough understanding of database-level access patterns, multi-tenant behaviors, and privilege semantics unique to DBaaS. This leads to reactive security measures, and misconfigurations are discovered

after incidents. Nonetheless, the examined literature advocates for automated IAM security for improved resilience, scalability, and visibility over manual configurations in cloud DBMS environment security.

5.3. RQ3: Comparison: Manual vs. Automated Configurations

RQ3 can be best answered by clearly enumerating the key differences between manual and automated IAM configuration strategies. It also reinforces the deliberation articulated in Sections 5.1 and 5.2. Table 8 enlists a one-to-one comparative analysis of manual and automated IAM configurations in cloud DBMS environments. The comparison highlights key aspects related to security effectiveness, error susceptibility, monitoring capabilities, and scalability in cloud DBMS environments, demonstrating how automated IAM approaches outperform traditional manual IAM configurations by providing stronger protection and more reliable access control.

Table 8. Comparison of manual and automated IAM configurations.

Security and Management Aspect	Manual IAM Configuration	Automated IAM Configuration
Configuration approach	Static, human-dependent	Continuous, policy-driven
Error rate	High susceptibility	Low susceptibility
Policy drift control	Limited	Continuous
Least-privilege enforcement	Inconsistent	Dynamic
Runtime visibility	Minimal	Real-time
Privilege escalation risk	High	Low
Scalability	Limited	High

The comparison highlights the inherently static and human-dependent nature of manual IAM configurations. Consequently, it has limited scalability in dynamic cloud environments and increases error susceptibility. Whereas automated IAM techniques enforce least-privilege rules and reduce risks of escalation. Moreover, it addresses long-standing misconfigurations by enabling continuous enforcement, real-time visibility, and adaptive policy management. The comparison demonstrates that manual IAM procedures are fundamentally unsynchronized with the operational features of cloud DBMS systems. Though they are effective for simple and static environments, automated IAM configurations offer the efficiency and scalability demanded in cloud database systems.

The analysis of reviewed studies clearly implies the superiority of automated IAM approaches, but a direct quantitative comparison of the two is extremely challenging. A noticeable bias is the unavailability of open challenges to test, and the included studies used different datasets, cloud platforms, evaluation methods, and performance measures. Therefore, it is a tough decision to call a single winner with a clear quantitative comparison. Thus, the reported comparison of automated IAM strategies should be considered in light of the aforementioned qualitative and experimental evidence rather than read as a blanket percentage improvement.

6. Discussion

Building on the results presented in Sections 5.1 and 5.2, a clear distinction emerges between manual and automated IAM configuration approaches in cloud DBMS environments. Manual IAM configurations are predominantly static, human-driven, and reactive, making them poorly suited to the complexity, scalability, and continuous change inherent in cloud-based database platforms. As discussed in Section 5.1, these limitations frequently lead to role misassignments, unmanaged service accounts, policy drift, and limited audit visibility, significantly increasing the risk of privilege escalation and unauthorized data access.

These challenges are further intensified in DBaaS environments, where multi-tenant architectures, shared responsibility models, and externally managed access layers reduce direct organizational control over low-level configurations. In such contexts, manual IAM administration becomes increasingly ineffective at maintaining accurate and secure access control policies.

Automated IAM configurations address these limitations by enabling continuous policy evaluation, real-time monitoring, and adaptive enforcement mechanisms. By dynamically enforcing least-privilege principles, periodically reassessing role assignments, and providing runtime visibility into access behaviors, automated solutions enable earlier detection of misconfigurations and abnormal privilege usage. As illustrated in Section 5.2, AI-enabled IAM approaches further enhance these capabilities by identifying complex privilege relationships and escalation paths that are difficult to detect through manual inspection. The reviewed literature consistently indicates that automated IAM configurations offer superior scalability, reduced error rates, improved policy drift control, and stronger protection against privilege escalation compared to traditional manual IAM management. Consequently, automation is not merely a complementary enhancement but a foundational requirement for achieving secure and resilient IAM governance in modern cloud DBMS environments.

6.1. Frequency Analysis of Nomenclature in Literature

To further analyze research trends in the selected studies, the abstracts of the primary papers were collected and combined into a single text corpus. A word cloud was generated to visualize the most frequently occurring terms across the literature. The visualization highlights dominant research themes such as IAM, access control, cloud, security, misconfiguration, automation, and privilege management, confirming the strong focus of existing research on access governance and automated security mechanisms in cloud database environments. Figure 4 depicts a word cloud illustrating the most frequently occurring terms across the abstracts of 20 primary studies selected in this study. The visualization highlights dominant concepts such as access, IAM, security, cloud, policies, and privilege, indicating that existing research primarily focuses on access control and identity governance in cloud environments. The word cloud analysis complements the findings of the systematic review by highlighting the key concepts addressed among those studies. The presence of common keywords is the same which appeared in the detailed VOS viewer graph. It reinforces the earlier stated observations to respond to the research questions.

6.2. Comparative Analysis of Selected Studies

Table 9 presents a comparative analysis of IAM approaches identified in the reviewed literature and highlights key security trends in cloud DBMS and DBaaS environments. Most previous studies concentrate on IAM misconfiguration detection and mitigation using automated monitoring, rule-based enforcement, machine learning, graph-based analysis, policy mining, and cloud security automation. Compared to traditional manual IAM management, these approaches generally provide greater scalability, visibility, and detection capabilities. While these advantages have contributed to the growth of IAM solutions, numerous limitations remain in existing approaches. Instead, a large variety of solutions are evaluated in the context of certain cloud platforms like AWS and Azure that may rarely apply to heterogeneous multi-cloud environments. Moreover, many of these methods are based on predefined rules, past datasets, or platform-specific inference assumptions, which limits their capabilities to detect previously unseen misconfiguration patterns.



Figure 4. Word cloud of abstracts from selected primary studies.

The reviewed literature indicates that DBaaS-specific IAM challenges are insufficiently addressed by published IAM approaches. Moreover, they tackle cloud IAM security at a higher level of abstraction and do not consider the challenges inherent in complex systems like DBaaS. In addition, remediation is often not a priority, and the existing techniques primarily target detection of security risks and misconfigurations. There are few proactive strategies with adaptive policy correction and real-time remediation, but they are mostly incorporated in grey literature. The analysis lays a foundation for the requirements of future DBaaS-aware and advocates that IAM frameworks should enforce automated detection, context-aware policy analysis, adaptive governance and real-time remediation mechanisms in order to improve security assurances in cloud database environments.

Table 9. Comparative analysis of IAM approaches in cloud DBMS and DBaaS environments.

IAM Approach	Key Advantages	Key Limitations	DBaaS Suitability
Manual IAM Configuration	Administrator control and simple deployment	Human error, policy drift, excessive privileges	Low
Rule-Based IAM Automation	Effective for known policy violations	Poor detection of unseen threats and contextual access requirements	Medium
Adaptive IAM	Context-aware access decisions and dynamic policy adjustment	Increased implementation complexity	High
AI-Based IAM	Anomaly detection, adaptive threat identification, reduced human intervention	Requires training data and computational resources	High
Graph-Based IAM Analysis	Detects hidden privilege escalation paths and permission dependencies	Computational overhead and limited remediation capabilities	High
CSPM-Based Security Automation	Continuous monitoring and automated remediation	Focuses primarily on infrastructure-level security posture	Medium
ABAC Policy Mining	Fine-grained authorization and reduced manual policy engineering	Dependent on authorization data quality	High

6.3. Deployment Challenges

Automation has advantages but there are some challenges for a pragmatic solution in security. First and foremost is the scalability. As cloud infrastructures continue to scale, IAM systems are required to handle millions of identities, services and permissions on continuous basis. They are added, updated and removed at a high volume with complex access-control information, and it exacerbate with a real-time processing demand. Another important requirement is interoperability. Organizations rarely deploy on a homogeneous resource to avoid vendor lock-in, and besides standard terminology, vendors have varying IAM architectures, policy models, and authorization mechanisms. Hence, using automated IAM solutions across different cloud environments can be challenging and might result in non-uniform policy enforcement if not considered in advance.

Another issue is the trade-off of false positives and false negatives. If detection mechanisms are extremely sensitive, they generate false positives and flag legitimate access activities as possible security breaches. This is often unacceptable and leads to overwhelming alerts for administrators. Alternatively, permissive methods frequently overlook critical misconfigurations, escalation paths, and unauthorized access. Lastly, performance overhead is a prominent concern, as the advanced IAM solutions based on machine learning, graph analysis, and continuous monitoring often require substantial computational resources. Therefore, it is worth highlighting that future IAM research should target the best trade-off between detection performance and cost of operation, false-alarm reduction as well as resource consumption.

6.4. Research Gaps and Future Directions

The reviewed studies indicate that a significant portion of IAM misconfigurations in cloud DBMS environments stems from reliance on traditional manual IAM configuration mechanisms, which are inherently error-prone and difficult to manage in dynamic and distributed cloud systems. A key research gap identified in the literature is that many misconfigurations are detected only at runtime, rather than being proactively prevented through continuous monitoring and enforcement mechanisms. Although automated IAM approaches demonstrate clear improvements over manual IAM configurations, current solutions remain constrained by static rule-based logic and limited awareness of DBaaS-specific architectures and privilege models.

Although cloud security automation technologies provide sophisticated real-time detection and response, database-level access semantics are still not well linked with them. There is a research gap for DBaaS-aware IAM automation that can explain tenant isolation and fine-grained database access because the majority of automation frameworks function at the infrastructure and application layers [36]. Furthermore, most existing IAM security solutions focus primarily on misconfiguration detection rather than real-time prevention and automated remediation. Many tools lack sufficient contextual understanding of multi-tenant DBaaS environments, database-specific access control semantics, and dynamic workload behavior, which limits their effectiveness in preventing privilege escalation and unauthorized data access. In addition, the absence of standardized datasets and evaluation benchmarks tailored to cloud DBMS environments makes it difficult to objectively compare and validate existing IAM security approaches.

Future research should therefore focus on the development of advanced autonomous IAM frameworks that integrate artificial intelligence (AI) and machine learning (ML) techniques to enable proactive threat detection, adaptive policy enforcement, and real-time response mechanisms [5]. Such frameworks should be DBaaS-aware, capable of reasoning about tenant isolation, database-level privileges, and evolving access patterns. Addressing these gaps is essential to achieving resilient, scalable, and secure IAM governance in next-generation cloud database platforms.

6.5. Validity of the Review

PICOC systematic literature review strategy guides this study to compile valuable results by adopting effective quality assessment criteria. However, it is hard to collect a complete set of impartial literature. One potential source of bias, studies reporting positive outcomes of automated IAM approaches are more likely to be published than studies reporting negative or inconclusive results. This is often unavoidable because of the process of generating results. However, a study to compile the reports from the gray literature, like blogs, Q&A portals, open service desk logs, etc., can be helpful. But this is often discouraged in systematic literature reviews. Another noticeable aspect is that the cloud is a commercial venture which may impact the literature. It is carefully considered in this study to include the literature that provides a no-conflict-of-interest statement. Even then, a concern specific to the topic of the study is the inclusion of studies in the review using a particular cloud environment, dataset, or organizational context. Thus, the discussion is kept vendor-neutral, and focus is kept on IAM configuration in DBaaS in the cloud. Finally, the evolving nature of cloud computing, IAM technologies, and AI-based security mechanisms and cybersecurity may impact the reported findings. The evolving security models, automation frameworks, and cloud-native access control architectures may challenge the analysis of currently included literature. Nevertheless, these limitations do not significantly affect the reliability and transparency of the review findings because of the rigorous systematic review methodology adopted in this study, particularly the use of effective selection criteria and quality assessment.

7. Conclusions

This study examined IAM misconfigurations in cloud Database-as-a-Service (DBaaS) environments, with particular emphasis on the effectiveness of automated security mechanisms and the limitations associated with manual IAM configurations. The survey findings indicate that manual IAM practices, which largely rely on static policies and human intervention, frequently lead to excessive privileges, policy drift, and an increased risk of privilege escalation. In contrast, automated IAM systems demonstrate greater effectiveness by enabling continuous policy enforcement, real-time monitoring, and enhanced visibility into access behaviors, thereby reducing misconfigurations and unauthorized access. Despite these advancements, the study identifies notable gaps in DBaaS-specific automation, real-time remediation capabilities, and standardized evaluation frameworks, particularly as much of the existing work is reported in gray literature. To strengthen IAM control and ensure secure, scalable cloud database systems, more systematic and rigorous research is required.

Author Contributions: Conceptualization, A.A. (Aljazi Almarri), A.A. (Asayil Alawadh), M.A. and M.A.R.; methodology, A.A. (Aljazi Almarri), A.A. (Asayil Alawadh), M.A. and M.A.R.; validation, A.A. (Aljazi Almarri), A.A. (Asayil Alawadh), M.A. and M.A.R.; formal analysis, A.A. (Aljazi Almarri), A.A. (Asayil Alawadh), M.A. and M.A.R.; writing—original draft preparation, A.A. (Aljazi Almarri), A.A. (Asayil Alawadh) and M.A.; writing—review and editing, M.A.R.; supervision, M.A.R.; project administration, M.A.R. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by the Saudi National Institute of Health Grant No. PRI01-2401-KFU15-46632810.

Data Availability Statement: No new data were created or analyzed in this study. Data sharing is not applicable to this article.

Conflicts of Interest: The authors declare no conflicts of interest. The funders had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript; or in the decision to publish the results.

Appendix A

Appendix A.1. PRISMA Checklist [40]

Topic	No.	Item	Location Where Item Is Reported
TITLE			
Title	1	Identify the report as a systematic review.	Page 1, lines 21–23
ABSTRACT			
Abstract	2	See the PRISMA 2020 for Abstracts checklist	
INTRODUCTION			
Rationale	3	Describe the rationale for the review in the context of existing knowledge.	Page 2, lines 73–84
Objectives	4	Provide an explicit statement of the objective(s) or question(s) the review addresses.	Page 6–7, Table 2, Figure 2
METHODS			
Eligibility criteria	5	Specify the inclusion and exclusion criteria for the review and how studies were grouped for the syntheses.	Page 9, Table 5
Information sources	6	Specify all databases, registers, websites, organisations, reference lists and other sources searched or consulted to identify studies. Specify the date when each source was last searched or consulted.	Page 8, Table 3
Search strategy	7	Present the full search strategies for all databases, registers and websites, including any filters and limits used.	Section Search Strategy, Table 4
Selection process	8	Specify the methods used to decide whether a study met the inclusion criteria of the review, including how many reviewers screened each record and each report retrieved, whether they worked independently, and if applicable, details of automation tools used in the process.	Implicit with equal contribution statement
Data collection process	9	Specify the methods used to collect data from reports, including how many reviewers collected data from each report, whether they worked independently, any processes for obtaining or confirming data from study investigators, and if applicable, details of automation tools used in the process.	Section 3.6
Data items	10a	List and define all outcomes for which data were sought. Specify whether all results that were compatible with each outcome domain in each study were sought (e.g., for all measures, time points, analyses), and if not, the methods used to decide which results to collect.	Section 3.5, Quality Assessment (QA)
	10b	List and define all other variables for which data were sought (e.g., participant and intervention characteristics, funding sources). Describe any assumptions made about any missing or unclear information.	Page 10–11, Table 7, lines 354–358
Study risk of bias assessment	11	Specify the methods used to assess risk of bias in the included studies, including details of the tool(s) used, how many reviewers assessed each study and whether they worked independently, and if applicable, details of automation tools used in the process.	Implicit in the Review Process and QA Criteria

Effect measures	12	Specify for each outcome the effect measure(s) (e.g., risk ratio, mean difference) used in the synthesis or presentation of results.	Not applicable
Synthesis methods	13a	Describe the processes used to decide which studies were eligible for each synthesis (e.g., tabulating the study intervention characteristics and comparing against the planned groups for each synthesis (item 5)).	Section 3.5, Quality Assessment (QA)
	13b	Describe any methods required to prepare the data for presentation or synthesis, such as handling of missing summary statistics, or data conversions.	Section 3.5, Quality Assessment (QA)
	13c	Describe any methods used to tabulate or visually display results of individual studies and syntheses.	Figure 3, VOS Viewer
	13d	Describe any methods used to synthesize results and provide a rationale for the choice(s). If meta-analysis was performed, describe the model(s), method(s) to identify the presence and extent of statistical heterogeneity, and software package(s) used.	Figure 3, VOS Viewer
	13e	Describe any methods used to explore possible causes of heterogeneity among study results (e.g., subgroup analysis, meta-regression).	Not applicable
	13f	Describe any sensitivity analyses conducted to assess robustness of the synthesized results.	Section 3.5, Quality Assessment (QA)
Reporting bias assessment	14	Describe any methods used to assess risk of bias due to missing results in a synthesis (arising from reporting biases).	Inherent in the review process
Certainty assessment	15	Describe any methods used to assess certainty (or confidence) in the body of evidence for an outcome.	Search criteria and query, Table 4
RESULTS			
Study selection	16a	Describe the results of the search and selection process, from the number of records identified in the search to the number of studies included in the review, ideally using a flow diagram.	Appendix A
	16b	Cite studies that might appear to meet the inclusion criteria, but which were excluded, and explain why they were excluded.	Section 3.4, Table 5
Study characteristics	17	Cite each included study and present its characteristics.	Section 4.
Risk of bias in studies	18	Present assessments of risk of bias for each included study.	Not Applicable
Results of individual studies	19	For all outcomes, present, for each study: (a) summary statistics for each group (where appropriate) and (b) an effect estimate and its precision (e.g., confidence/credible interval), ideally using structured tables or plots.	Section 4
Results of syntheses	20a	For each synthesis, briefly summarise the characteristics and risk of bias among contributing studies.	Section 4
	20b	Present results of all statistical syntheses conducted. If meta-analysis was done, present for each the summary estimate and its precision (e.g., confidence/credible interval) and measures of statistical heterogeneity. If comparing groups, describe the direction of the effect.	Figure 3. VOS Viewer
	20c	Present results of all investigations of possible causes of heterogeneity among study results.	Section
	20d	Present results of all sensitivity analyses conducted to assess the robustness of the synthesized results.	Inherent in the review process
Reporting biases	21	Present assessments of risk of bias due to missing results (arising from reporting biases) for each synthesis assessed.	Not Applicable
Certainty of evidence	22	Present assessments of certainty (or confidence) in the body of evidence for each outcome assessed.	Section 4
DISCUSSION			

Discussion	23a	Provide a general interpretation of the results in the context of other evidence.	Section 5
	23b	Discuss any limitations of the evidence included in the review.	Section 6
	23c	Discuss any limitations of the review processes used.	Section 6
	23d	Discuss implications of the results for practice, policy, and future research.	Section 6
OTHER INFORMATION			
Registration and protocol	24a	Provide registration information for the review, including register name and registration number, or state that the review was not registered.	Not registered
	24b	Indicate where the review protocol can be accessed, or state that a protocol was not prepared.	Not Applicable
	24c	Describe and explain any amendments to information provided at registration or in the protocol.	Not Applicable
Support	25	Describe sources of financial or non-financial support for the review, and the role of the funders or sponsors in the review.	No conflict of interest
Competing interests	26	Declare any competing interests of review authors.	No conflict of interest
Availability of data, code and other materials	27	Report which of the following are publicly available and where they can be found: template data collection forms; data extracted from included studies; data used for all analyses; analytic code; any other materials used in the review.	Reproducible with adopted PICOC strategy

Appendix A.2. PRISMA Abstract Checklist

Topic	No.	Item	Reported?
TITLE			
Title	1	Identify the report as a systematic review.	Yes
BACKGROUND			
Objectives	2	Provide an explicit statement of the main objective(s) or question(s) the review addresses.	Yes
METHODS			
Eligibility criteria	3	Specify the inclusion and exclusion criteria for the review.	Yes
Information sources	4	Specify the information sources (e.g., databases, registers) used to identify studies and the date when each was last searched.	Yes
Risk of bias	5	Specify the methods used to assess risk of bias in the included studies.	No
Synthesis of results	6	Specify the methods used to present and synthesize results.	Yes
RESULTS			
Included studies	7	Give the total number of included studies and participants and summarise relevant characteristics of studies.	Yes
Synthesis of results	8	Present results for main outcomes, preferably indicating the number of included studies and participants for each. If meta-analysis was done, report the summary estimate and confidence/credible interval. If comparing groups, indicate the direction of the effect (i.e., which group is favoured).	Yes
DISCUSSION			
Limitations of evidence	9	Provide a brief summary of the limitations of the evidence included in the review (e.g., study risk of bias, inconsistency and imprecision).	Yes
Interpretation	10	Provide a general interpretation of the results and important implications.	Yes
OTHER			
Funding	11	Specify the primary source of funding for the review.	Yes
Registration	12	Provide the register name and registration number.	No

Appendix B. PRIMA Flow Graph

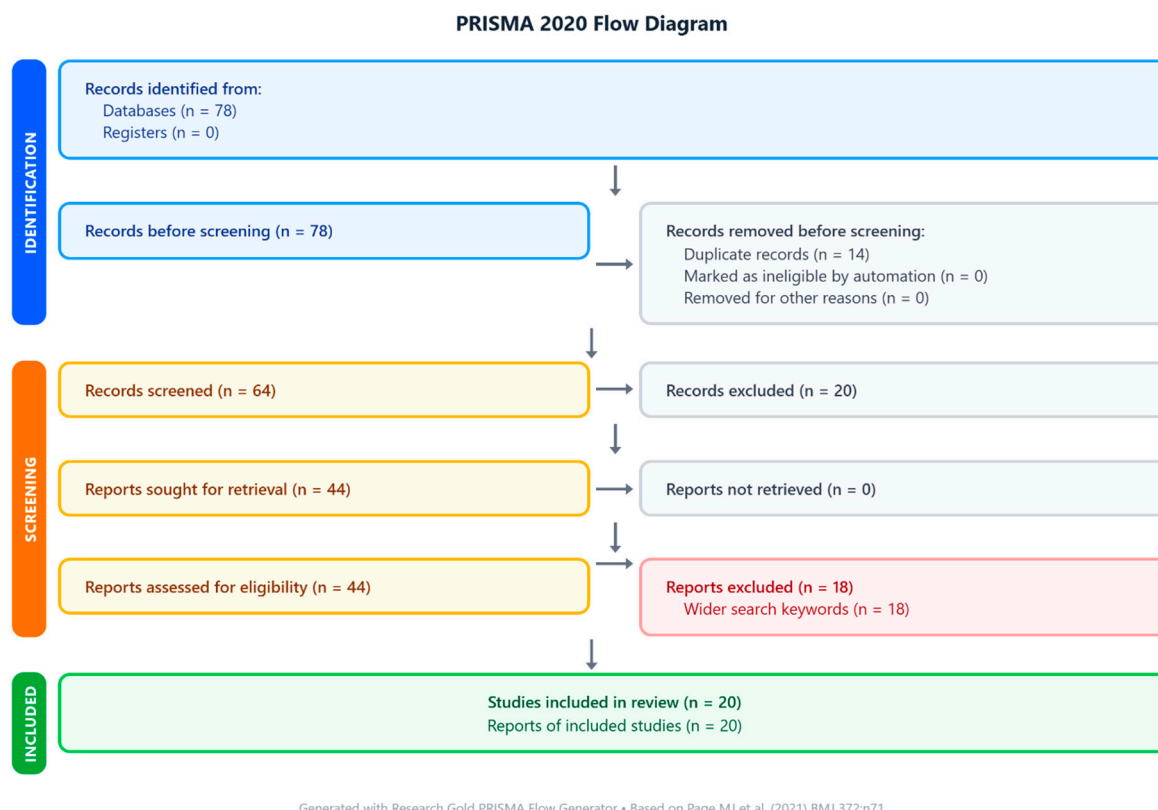


Figure A1. PRISMA flow graph generated using PRIMA flow generator [40].

References

- Islam, R.; Patamsetti, V.V.; Gadhi, A.; Gondu, R.M.; Bandaru, C.M.; Kesani, S.C.; Abiona, O. The future of cloud computing: Benefits and challenges. *Int. J. Commun. Netw. Syst. Sci.* **2023**, *16*, 53–65.
- Raktate, P.; Chaudhari, N.; Pawar, A.; Giri, S. A survey on security issues and challenges in cloud computing. *Int. J. Res. Anal. Rev.* **2024**, *11*, 104–112.
- Zakiyyah, R.; Permana, D.; Valenecio, D.; Chowanda, A.; Muliono, Y.; Z. N. Izdihar. Security challenges and issues in cloud computing. In Proceedings of the International Symposium on Networks, Computers and Communications (ISNCC), Washington, DC, USA, 22–25 October 2024.
- Singh, A.P.; Kuzminykh, I.; Ghita, B. Industry perception of security challenges with identity access management solutions. In Proceedings of the 2024 IEEE International Black Sea Conference on Communications and Networking (BlackSeaCom), Tbilisi, Georgia, 24–27 June 2024.
- Jimmy, F. AI-Driven Identity and Access Management: Opportunities, Challenges, and Future Directions. *J. Artif. Intell. Gen. Sci.* **2025**, *8*, 224–244. <https://doi.org/10.60087/jaigs.v8i02.418>.
- Sharma, C.; Sharma, C. Cloud computing security: Threats and mitigation strategies. In Proceedings of the International Conference on Signal Processing and Advance Research in Computing (SPARC), Lucknow, India, 12–13 September 2024; pp. 1–6. <https://doi.org/10.1109/SPARC61891.2024.10829335>.
- Alfarhan, A.; Alhussain, R.; Rassam, M. Cloud database security issues and challenges: A review. *J. Innov. Inf. Commun. Technol.* **2021**, *1*, 21–31.
- Indu, I.; Anand, P.M.R.; Bhaskar, V. Identity and access management in cloud environment: Mechanisms and challenges. *Eng. Sci. Technol. Int. J.* **2018**, *21*, 574–588. <https://doi.org/10.1016/j.jestch.2018.05.010>.
- Ike, J.E.; Kessie, J.D.; Okaro, H.E.; Ezeife, E.; Onibokun, T. Identity and Access Management in Cloud Storage: A Comprehensive Guide. *Int. J. Multidiscip. Res. Growth Eval.* **2025**, *6*, 245–252. <https://doi.org/10.54660/IJMRGE.2025.6.2.245-252>.
- Glöckler, J.; Sedlmeir, J.; Frank, M.; Fridgen, G. A systematic review of IAM requirements and self-sovereign identity. *Bus. Inf. Syst. Eng.* **2023**, *66*, 421–440. <https://doi.org/10.1007/s12599-023-00830-x>.

11. Ghaffari, F.; Gilani, K.; Bertin, E.; Crespi, N. Identity and access management using distributed ledger technology: A survey. *Int. J. Netw. Manag.* **2022**, *32*, e2180. <https://doi.org/10.1002/nem.2180>.
12. Hummer, M.; Kunz, M.; Netter, M.; Fuchs, L.; Pernul, G. Adaptive identity and access management using contextual policies. *J. Inf. Secur. Appl.* **2022**, *65*, 103012. <https://doi.org/10.1016/j.jisa.2022.103012>.
13. Aramide, O.O. Identity and access management for IoT in 5G. *Open Access Res. J. Sci. Technol.* **2022**, *5*, 96–108. <https://doi.org/10.53022/oarjst.2022.5.2.0043>.
14. Devlekar, S.; Ramteke, V. Identity and access management: High-level conceptual framework. *Cardiometry* **2022**, *24*, 123–134. <https://doi.org/10.12710/cardiometry.2022.24.123>.
15. Tamraparani, V. Leveraging AI for fraud detection in identity and access management. *J. Comput. Anal. Appl.* **2023**, *31*, 719–727.
16. Wairagade, A.; Ranjan, S. AI in Identity and Access Management (IAM) for Enterprise Systems: A Comparative Analysis. *Procedia Comput. Sci.* **2025**, *263*, 167–174. <https://doi.org/10.1016/j.procs.2025.07.021>.
17. Muppa, K.R. Enhanced Identity and Access Management with Artificial Intelligence: A Strategic Overview. *Int. J. Inf. Secur. Cybercrime* **2024**, *13*, 9–17.
18. Alibadi, Z.J. Security challenges and solutions in cloud-based software systems. *Int. J. Comput. Trends Technol.* **2024**, *72*, 160–172.
19. Torkura, K.A.; Akpon, S.G.; Meinel, C. Continuous auditing and threat detection in multi-cloud environments. In Proceedings of the International Conference on Cloud Security and Management (CSM '21); Academic Conferences International, Online, 17–18 October 2021; pp. 233–240.
20. Ahmadi, S. Systematic literature review on cloud computing security: Threats and mitigation strategies. *J. Inf. Secur.* **2024**, *15*, 148–167. <https://doi.org/10.4236/jis.2024.152010>.
21. Akhtar, N.; Kerim, B.; Perwej, Y.; Tiwari, A.; Praveen, S. A comprehensive overview of privacy and data security for cloud storage. *Int. J. Sci. Res. Sci. Eng. Technol.* **2021**, *8*, 113–152. <https://doi.org/10.32628/IJSRSET21852>.
22. Alsirhani, A.; Ezz, M.; Mostafa, A.M. Advanced authentication mechanisms for identity and access management in cloud computing. *Comput. Syst. Sci. Eng.* **2022**, *43*, 967–984. <https://doi.org/10.32604/csse.2022.024854>.
23. van Ede, T.; Khasuntsev, N.; Steen, B.; Continella, A. Detecting Anomalous Misconfigurations in AWS Identity and Access Management Policies. In Proceedings of the 2022 Cloud Computing Security Workshop (CCSW '22), Los Angeles, CA, USA, 7–11 November 2022. <https://doi.org/10.1145/3560810.3564264>.
24. Kumar, K.A.; Zolkipli, M.F. Review on identity and access management for digital environment security. *Borneo Int. J.* **2024**, *7*, 43–48.
25. Ghadge, N. Use of blockchain technology to strengthen identity and access management. *Int. J. Inf. Technol.* **2024**, *1*, 3. <https://doi.org/10.2139/ssrn.4854174>.
26. Hu, Y.; Wang, W.; Khurshid, S.; McMillan, K.L.; Tiwari, M. Fixing privilege escalations in cloud access control with MaxSAT and graph neural networks. In Proceedings of the 38th IEEE/ACM International Conference on Automated Software Engineering (ASE '23), Luxembourg, 11–15 September 2023; pp. 1–11. <https://doi.org/10.1109/ASE56229.2023.00167>.
27. Haimed, I.B.; Albahar, M.; Alzubaidi, A. Exploiting misconfiguration vulnerabilities in Microsoft Azure Active Directory for privilege escalation attacks. *Future Internet* **2023**, *15*, 226. <https://doi.org/10.3390/fi15070226>.
28. Sanjeetha, M.B.F.; Siriwardane, M.S.M.; Rajakaruna, R.J.P.K.; Haddela, P.S. Database-as-a-Service (DBaaS) in Cloud Computing: Security Issues and Policies. *Asian J. Comput. Sci. Technol.* **2025**, *14*, 15–19. <https://doi.org/10.70112/ajcst-2025.14.1.4322>.
29. Singh, C.; Warraich, J.; Thakkar, R. IAM identity access management: Importance in maintaining security systems within organizations. *Eur. J. Eng. Technol. Res.* **2023**, *8*, 30–38.
30. Mirabi, M.; Binnig, C. QFilter: Towards a Fine-Grained Access Control for Aggregation Query Processing over Secret-Shared Data. In Proceedings of the VLDB 2023 Workshops (CloudDB Workshop), CEUR Workshop Proceedings, Vancouver, BC, Canada, 28 August–1 September 2023.
31. Elangovan, K.A.R.; Umamaheswari, J. Data Privacy and Security in Cloud Computing Environments. *E3S Web Conf.* **2023**, *399*, 04040.
32. Mala, M.K.; Yadhukrishna, M.R.; Jyothi, B.; Pradeep, M. AI-Enhanced Cloud Security: A Dynamic Framework for Adaptive Threat Intelligence. In Proceedings of the 2025 International Conference on Computing Technologies (ICOCT) (2025), Bengaluru, India, 13–14 June 2025; pp. 1–7. <https://doi.org/10.1109/ICOCT64433.2025.11118731>.
33. Gurram, S. Identity and access management in multi-cloud environments. *World J. Adv. Res. Rev.* **2025**, *26*, 2894–2902. <https://doi.org/10.30574/wjarr.2025.26.1.1329>.
34. Perez-Haro, A.; Díaz-Pérez, A. ABAC Policy Mining through Affiliation Networks and Biclique Analysis. *Information* **2024**, *15*, 45.

35. Pitkar, H. Cloud security automation through symmetry: Threat detection and response. *Symmetry* **2025**, *17*, 859. <https://doi.org/10.3390/sym17060859>.
36. Boamah, K.G. Cloud Security Posture Management: A Comprehensive Analysis of Automated Risk Identification and Mitigation in Multi-Cloud Environments. *Int. J. Res. Innov. Soc. Sci. (IJRISS)* **2025**, *9*, 4458–4471. <https://doi.org/10.47772/IJRISS.2025.91100349>.
37. Pöhn, D.; Hommel, W. Universal identity and access management framework for future ecosystems. *Future Internet* **2021**, *13*, 69. <https://doi.org/10.3390/fi13030069>.
38. Dhanushkodi, R.M. AI-driven integration of legacy IAM services into AWS cloud-based microservice architectures. *International J. Innov. Res. Sci. Eng. Technol.* **2025**, *14*, 11351–11358. <https://doi.org/10.15680/IJIRSET.2025.1405005>.
39. Noel, S.; Jajodia, S.; O'Berry, B.; Jacobs, M. Automatic analysis of attack graphs for risk mitigation and prioritization on large-scale and complex networks. *Int. J. Inf. Secur.* **2021**, *20*, 38–407. <https://doi.org/10.1007/s10207-020-00520-8>.
40. Page, M.J.; McKenzie, J.E.; Bossuyt, P.M.; Boutron, I.; Hoffmann, T.C.; Mulrow, C.D.; Shamseer, L.; Tetzlaff, J.M.; Akl, E.A.; Brennan, S.E.; et al. The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. *MetaArXiv* **2020**. <https://doi.org/10.31222/osf.io/v7gm2>.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.