Asian Journal of Computer Science and Technology
ISSN: 2249-0701 (P); 2583-7907 (E)
Vol.14 No.1, 2025, pp.15-19

www.crijournals.org
DOI: https://doi.org/10.70112/ajcst-2025.14.1.4322

Database-as-a-Service (DBaaS) in Cloud Computing: Security Issues and Policies

Mohamed Buhary Fathima Sanjeetha*[1], Manamalage Sandali Miurusari Siriwardane[2], Rajakarunalage Jayani Prabhashini Kumari Rajakaruna[3] and Prasanna Sumathipala Haddela[4]

[1]Department of MIT, Faculty of Management and Commerce, South Eastern University of Sri Lanka, Oluvil, Sri Lanka
[2,3&4]Faculty of Graduate Studies and Research, Sri Lanka Institute of Information Technology, Malabe, Sri Lanka
E-mail: sandalisiriwardane7@gmail.com, jayaniprabhashini@gmail.com, prasanna.s@sliit.lk
*Corresponding Author: sanjeetha.mit@seu.ac.lk
(Received 20 December 2024; Revised 26 January 2025, Accepted 13 February 2025; Available online 27 February 2025)

Abstract **- The growing adoption of Database-as-a-Service (DBaaS) has revolutionized data management by offering scalability, cost-efficiency, and adaptability, particularly for multi-tenant platforms. However, significant security challenges remain unresolved. This study aims to identify and analyze the security concerns associated with DBaaS and propose effective policies and techniques to mitigate these risks. A systematic review of the literature and an evaluation of real-world implementations were conducted to investigate common security vulnerabilities and potential remedies. The research highlights key security threats, including data breaches, malicious insider activities, and inadequate access controls. It also underscores best practices, such as multi-layered security strategies and encryption techniques, to address these challenges. This study provides a framework for DBaaS providers and users to enhance the security and reliability of cloud databases by addressing critical security issues.**
Keywords: **Database-as-a-Service (DBaaS), Security Challenges, Data Breaches, Encryption Techniques, Multi-Tenant Platforms**

I. INTRODUCTION

Cloud computing is a trending topic in the field of information technology. Various cloud computing service models exist, including Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), and Database as a Service (DBaaS) [1]. Among these, DBaaS is a multi-tenant platform that enables users to leverage cloud database services with high performance and reduced operational costs. Users only pay for their usage, such as software licensing and administrative costs [2], as the infrastructure is owned by another party. Users are responsible only for the applications and processes that operate on the infrastructure [3]. Consequently, hardware and software infrastructure requirements, as well as database maintenance tasks like backups and software upgrades, are no longer concerns for users. These advantages, among others discussed later in this paper, contribute to the growing popularity of DBaaS.

The concept of DBaaS has evolved over several years but gained traction with the advent of cloud computing. DBaaS was first introduced with Amazon Web Services' Relational Database Service (RDS) in 2009. Today, many cloud service providers, such as Microsoft Azure and Google Cloud, offer advanced database services, including relational databases and NoSQL databases like MongoDB and Cassandra [4]. Users can now choose database services tailored to their specific requirements. DBaaS provides significant benefits, including cost savings, scalability, and ease of use, making it an attractive option for businesses of all sizes. However, DBaaS also faces challenges, particularly in terms of security and privacy [5].

Users often store both sensitive and non-sensitive data in cloud databases. Ensuring the security of sensitive data is critical, as data breaches or losses pose significant risks to business operations. To attract more users to DBaaS, cloud service providers must address security concerns through robust security policies and mechanisms. For instance, encrypting data stored in databases is a widely used security measure. Researchers have identified various security issues in DBaaS and proposed policies to mitigate these risks, which are reviewed in subsequent sections of this paper.

II. ARCHITECTURE OF DBaaS

As mentioned earlier, DBaaS is a multi-tenant platform [2]. This architecture allows multiple servers to operate virtually on a single physical server. Each customer is allocated a virtual server, enabling a single multi-tenant cloud to serve multiple customers. All virtual servers on a physical server share the same physical processor, memory, and other resources. Cached data is stored in the physical memory of the server, accessible by all virtual servers. As a result, each virtual server can potentially access the memory address space of others, creating a risk of unauthorized access to confidential information. This shared memory model is a significant reason why DBaaS faces security challenges.

The primary elements that make up the database-as-a-service (DBaaS) architecture are depicted in Fig. 1 and are as follows:

1. *Database Management System (DBMS):* The DBMS is the software responsible for managing the database, including data storage, retrieval, and manipulation.

Commonly used DBMSs in DBaaS include MySQL, Oracle, PostgreSQL, MongoDB, and Microsoft SQL Server.

2. *Cloud:* The cloud infrastructure provides the physical resources required to operate the DBMS, such as computing power, storage, and networking. This infrastructure is typically provided by cloud service providers such as Amazon Web Services (AWS), Microsoft Azure, or Google Cloud Platform (GCP).

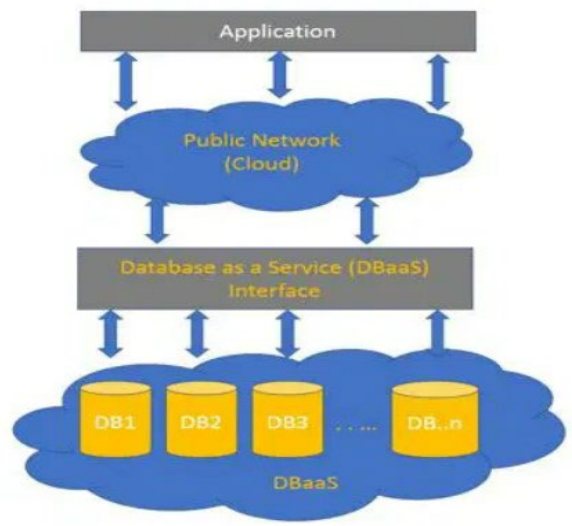

Fig. 1 Components of DBaaS

3. *Database Server:* The database server is the computer on which the DBMS is installed and operates. In the DBaaS model, the service provider manages and maintains the server, while customers access the database through a web-based interface.

4. *API (Application Programming Interface):* The API offers a standardized interface for customers to interact with the database. It allows users to perform operations such as creating, reading, updating, and deleting data using programming languages like Python, Java, or PHP.

III. REVIEW OF LITERATURE

DBaaS has emerged as a popular service model in cloud computing, offering significant benefits such as cost savings, scalability, and flexibility. However, the associated security issues have become a major concern. This literature review explores the security challenges and the policies and mechanisms designed to address them in the context of DBaaS.

A. Security Issues in DBaaS

Several studies have identified security issues associated with DBaaS. Mehak *et al.,* [6] and Ferrari [7] highlight that data confidentiality is a critical concern, as sensitive data may be stored in cloud databases. Internal and external malware attacks, including sniffing, spoofing, and Denial of Service (DoS) attacks, threaten data confidentiality [8]. The lack of robust access control mechanisms, especially in outsourced data management scenarios, further exacerbates the risks [9]. Poor data isolation may lead to unauthorized access and breaches, as service provider employees could exploit their privileges to access sensitive client data [10].

Data integrity is another significant challenge, as data can be intentionally or unintentionally modified or deleted by authorized or unauthorized users, leading to corruption or loss [4]. Additionally, data privacy concerns arise when cloud providers fail to ensure that users' data is not accessed or used without consent [4], [5].

Zheng [9] identifies various shortcomings in DBaaS, including insufficient transparency in security practices and the potential for data theft, deletion, or tampering if hackers gain access. Furthermore, hosting multiple clients on a single platform raises concerns about data isolation and security [9].

Data availability is also critical in DBaaS. Providers must ensure continuous access to data, implement disaster recovery and business continuity policies, and safeguard data from tampering during transmission or storage. Januzaj et al. [8] emphasize the risks of downtime and data loss due to cloud infrastructure issues. Additionally, network latency and limited control over database infrastructure can hinder customization for specific business needs. DBaaS providers must also comply with regulatory requirements, including data protection and privacy laws. Failure to meet these obligations can result in legal penalties and reputational damage [9].

B. Policies and Mechanisms for Addressing Security Issues in DBaaS

Various security policies and mechanisms have been proposed to address these challenges. Customers should implement data encryption at rest and in transit, adopt access controls, and employ auditing and monitoring tools [12]. Secure communication protocols, such as Secure Sockets Layer (SSL) or Transport Layer Security (TLS), firewalls, strong passwords, two-factor authentication, and role-based access control mechanisms, enhance database security. Kumar *et al.,* [13] propose a multi-layered security model for cloud database services.

1. *Physical Security Layer:* Focuses on securing the data center with access controls, surveillance, and environmental safeguards.
2. *Network Security Layer:* Secures the network infrastructure using encryption, access controls, and intrusion detection systems.
3. *Data Security Layer:* Protects stored data through encryption, access controls, and backup procedures.
4. *Application Security Layer:* Mitigates application vulnerabilities through authentication, access controls, and input validation.

5. *Compliance and Governance Layer:* Ensures adherence to laws, regulations, and governance practices.

Mehak *et al.,* [6] advocate for multi-layered security approaches encompassing the application, database, and infrastructure layers, supported by encryption, access control mechanisms, and monitoring tools. Service Level Agreements (SLAs) between providers and customers are crucial to ensure security compliance. Ferrari [7] emphasizes shared responsibility between providers and customers for DBaaS security.

Encryption of sensitive data, access controls, authentication mechanisms, auditing, and monitoring are highlighted as key measures. Frameworks such as ISO 27001 and SOC 2 ensure adherence to best practices. Customers are advised to supplement provider measures with their own, such as firewalls and intrusion detection systems.

IV. SECURITY ISSUES IN DBaaS IN CLOUD COMPUTING

When considering quality of service as the primary emphasis, data security becomes a critical issue. Cloud computing introduces new security challenges for various reasons. Traditional cryptosystems cannot be employed directly because users may be denied access to data stored in a cloud computing environment. To ensure proper data storage in the cloud, a checksum must be performed independently of the entire database or dataset [14].

When working in the cloud, reliance on the deployment model is crucial as it governs the data. In older architectural designs, trust is considered an essential component of the security strategy. In a public cloud, the infrastructure owner has control over the underlying resources and is expected to implement appropriate security measures to mitigate risks. Trusting the security processes and implementations provided by the infrastructure owner is deemed essential.

However, deployment models vary, and private cloud infrastructures, owned by private organizations, retain the same degree of trust. Thus, private clouds do not require additional security standards [15]. The Cloud Security Alliance (CSA) has identified various risks associated with cloud computing over the past year. The research reflects current challenges discussed by IT experts, highlighting specific security issues inherent to cloud computing services [16].

A. Breach of Data

Data breaches pose a significant risk, affecting approximately 110 million users by compromising personal and credit data. The cloud computing industry faces new attack vectors. CSA identifies such breaches as a primary concern. Although no definitive study has confirmed the complete security of hypervisor and virtual machine (VM) activities, theoretical assumptions and isolated evidence suggest potential vulnerabilities. For example, cloud users might detect encryption key activity on separate VMs hosted on the same node [17].

B. Loss of Information

Data loss occurs when the disk drive fails, and no backup exists, or when encryption keys necessary for decoding data are lost. Instances of data loss have also resulted from human operator errors [18]. Furthermore, malicious attacks can lead to significant data loss.

C. Interfaces and APIs That Are Not Secure

Low-security interfaces or APIs increase the risk of attacks. Robust interfaces should incorporate user authentication, data encryption, and access control measures. A high-quality API architecture is necessary to mitigate these risks [19].

D. Denial-of-Service (DoS) Attacks

DoS attacks, traditional methods of disrupting online activities, remain a threat [20]. Attackers attempt to overwhelm users by launching rapid and dispersed attacks, preventing the processing of legitimate requests. Attackers may also exploit users' services without entirely disabling them, causing users to incur costs for resources consumed during the attack. Continuous DoS attacks can render cloud services infeasible to operate [21].

E. Malicious Insiders

Malicious insiders present significant security risks. Attackers leveraging extensive cloud services may exploit internal vulnerabilities. Cloud service consumers are responsible for securing encryption keys. If keys are exposed and consumers fail to retain copies, insider attacks become feasible. Relying solely on cloud providers for data protection puts consumers at risk [7].

F. Cloud Abuse

Cloud computing's scalability and flexible service options can be exploited by attackers. While breaking encryption keys using traditional hardware may take years, attackers leveraging cloud resources could achieve this in minutes. Additionally, hackers can use cloud services for activities such as Distributed Denial of Service (DDoS) attacks, malware propagation, or pirated software distribution [22]. Service providers are responsible for monitoring cloud services, while customers must maintain records of services received.

G. Insufficient Investigation

Many organizations migrate operations to the cloud without fully understanding the scope and rules of the undertaking. Customers who lack awareness of security policies, encryption implementation, and incident response measures

face challenges in managing expectations from cloud providers. Consequently, these organizations operate at a heightened risk level [23].

H. Common Technology Vulnerabilities

In shared cloud environments, security breaches can result from misconfigured applications or operating systems. Vulnerabilities in processor caches, shared services, or databases can expose sensitive information. If the underlying infrastructure is compromised, customer data may be at risk [8].

I. Insufficient Visibility

DBaaS resources hosted on external servers lack visibility in some organizations. Many traditional network monitoring solutions are ineffective in the cloud, complicating efforts to monitor and protect resources. This lack of cloud-specific security solutions increases the difficulty of safeguarding cloud-based assets [24].

V. SECURITY POLICIES IN DBaaS IN CLOUD COMPUTING

Cloud service providers are emphasizing multi-layered security measures. This focus aims to fulfill their commitment to delivering standardized security solutions to consumers. The widespread adoption of cloud computing has created a fertile ground for hackers and other malicious actors. Discussions around cloud security have centered on critical aspects, including maintaining the confidentiality, availability, and integrity of data and applications.

A. Security Assessment

Cloud service consumers need to perform a comprehensive security assessment as the final step in their process. The ability to identify potential hazards is crucial to ensuring the safety of cloud infrastructure [25], [26]. Such assessments are valuable for validating that cloud workloads are secure and free of risks. In some cases, additional protections may be required. Security assurance measures and policies aligned with a company's risk assessment goals can enhance the security of cloud environments and benefit customers.

B. Securing Your Information

Data stored in the cloud, whether on public or hybrid cloud architectures, often resides on shared infrastructure and integrates scattered data from nodes in different geographic locations. Organizations using public cloud architectures must secure data by restricting access and ensuring secure storage [27], [28].

This data includes user profiles and transaction details, which attackers can exploit. Cloud applications typically include not only programmed functionalities but also configurations, scripts, and users' account information. Access to such resources should be restricted based on user identification, as demonstrated in [29].

C. Identity and Access Management

The increasing adoption of cloud services by enterprises has heightened the complexity of managing identities. In some cases, organizations may lose control over the services they provide. A robust policy is essential to establish provisions for access based on user identification. It is necessary to grant users the permissions required to complete their tasks and access the information they need [30].

VI. CONCLUSION

This research highlights the security risks associated with DBaaS and outlines potential solutions to mitigate these risks. As businesses increasingly adopt cloud-based services, DBaaS has gained popularity. However, the security risks connected with DBaaS cannot be overlooked. The study identifies several security challenges under four major categories: data confidentiality and integrity, privacy, availability, and compliance. Additionally, it discusses various security measures, including technological and management strategies, that can help reduce risks associated with DBaaS.

VII. LIMITATIONS AND FUTURE DIRECTION

The solutions presented in this paper may not be universally applicable, as each organization has unique security requirements and challenges. Furthermore, the findings may not be generalizable across all types of DBaaS. Security risks and solutions can differ depending on the type of DBaaS, such as relational or NoSQL databases, or the specific provider used. Future research could examine these differences in greater detail. Another limitation of this paper is that it is based on the current state of technology and security practices. As these evolve, the solutions presented here may become outdated or insufficient. Future research should focus on developing new security solutions tailored to DBaaS. As technology advances, new threats and vulnerabilities will emerge, necessitating innovative approaches to security. Additionally, research could explore the cost-benefit analysis of DBaaS security solutions. Organizations may be hesitant to invest in additional security measures; such research could help quantify the benefits of these investments and encourage the adoption of robust security practices.

Declaration of Conflicting Interests
The authors declare no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding
The authors received no financial support for the research, authorship, and/or publication of this article.

Use of Artificial Intelligence (AI)-Assisted Technology for Manuscript Preparation
The authors confirm that no AI-assisted technologies were used in the preparation or writing of the manuscript, and no images were altered using AI.

REFERENCES

[1] M. N. Al-Refai, A. Haya, H. Fawareh, and H. H. Khafajeh, "Database as a Service (DBaaS) Challenges and Solutions," in *Proc. 22nd Int. Arab Conf. Inf. Technol. (ACIT)*, Muscat, Oman, 2021, pp. 1-6, doi: 10.1109/ACIT53391.2021.9677127.

[2] K. K. Hingwe and S. M. S. Bhanu, "Sensitive Data Protection of DBaaS Using OPE and FPE," in *Proc. 4th Int. Conf. Emerg. Appl. Inf. Technol.*, Kolkata, India, 2014, pp. 320-327.

[3] I. Astrova, A. Koschel, C. Eickemeyer, J. Kersten, and N. Offel, "DBaaS comparison: Amazon vs. Microsoft," in *Proc. Int. Conf. Inf. Soc. (i-Society)*, Dublin, Ireland, 2017, pp. 15-21.

[4] Gartner, "Top security and risk management trends for 2021," 2021. [Online]. Available: https://www.gartner.com/smarterwithgartner/top-security-and-risk-management-trends-for-2021

[5] W. Shehri, "Cloud Database Sheri as a Service," *Int. J. Database Manag. Syst.*, vol. 5, no. 2, pp. 1-12, 2013.

[6] F. Mehak, R. Masood, Y. Ghazi, and M. A. Shibli, "Security aspects of database-as-a-service (DBaaS) in cloud computing," in *Proc. 11th Int. Bhurban Conf. Appl. Sci. Technol. (IBCAST)*, Islamabad, Pakistan, 2014, pp. 23-28.

[7] E. Ferrari, "Database as a Service: Challenges and solutions for privacy and security," in *Proc. 1st Int. Conf. Cloud Comput. (CLOUD'09)*, Beijing, China, 2009, pp. 517-520.

[8] Y. Januzaj, J. Ajdari, and B. Selimi, "DBMS as a Cloud service: Advantages and disadvantages," *Int. J. Adv. Comput. Sci. Appl.*, vol. 8, no. 11, pp. 225-230, 2017.

[9] X. Zheng, "Database as a service-current issues and its future," *J. Softw. Eng. Appl.*, vol. 5, no. 11, pp. 1079-1086, 2012.

[10] J. Weis and J. Alves-Foss, "Securing database as a service: Issues and compromises," *J. Comput. Sci. Coll.*, vol. 28, no. 6, pp. 72-78, 2012.

[11] K. Munir, "Security model for cloud database as a service (DBaaS)," *J. Inf. Secur.*, vol. 6, no. 1, pp. 13-20, 2015.

[12] A. Behl, "Emerging Security Challenges in Cloud Computing-An insight to Cloud security challenges and their mitigation," in *Proc. World Congr. Inf. Commun. Technol. (WICT)*, Mumbai, India, 2011, pp. 217-222.

[13] A. Kumar, H. Lee, and R. P. Singh, "Efficient and Secure Cloud Storage for Handling Big Data," in *Proc. 6th Int. Conf. New Trends Inf. Sci. Serv. Sci. Data Min. (ISSDM)*, Seoul, South Korea, 2012, pp. 162-166.

[14] M. Rassam, A. Alfarhan, and R. Alhussain, "Cloud Database Security Issues and Challenges: A Review," *J. Innov. Inf. Commun. Technol.*, vol. 1, no. 1, pp. 21-31, Nov. 2021.

[15] K. Munir, "Security model for mobile cloud database as a service (DBaaS)," in *Cloud Security: Concepts, Methodologies, Tools, and Applications*, IGI Global, 2019, pp. 760-769.

[16] M. S. Cholke and S. B. Natikar, "New Secure Concurrency Management Approach for Distributed and Concurrent Access of Encrypted Cloud Databases Using DBaaS," *Int. J. Innov. Eng. Res. Technol.*, vol. 1, pp. 1-4, 2019.

[17] S. Bauskar, "Navigating Database Security in Cloud Computing: Challenges and Solutions," *Int. J. Comput. Appl.*, vol. 975, pp. 88-87, 2019.

[18] S. Banothu, G. Janardhan, G. Sirisha, S. Shepuri, M. Karnam, and B. Allam, "A Secure Data Storage Approach for Online Examination Platform using Cloud DBaaS Service," *Scalable Comput. Pract. Exp.*, vol. 25, no. 5, pp. 3715-3724, Aug. 2024.

[19] M. Battula, "A Systematic Review on a Multi-tenant Database Management System in Cloud Computing," in *Proc. Int. Conf. Cogn. Robot. Intell. Syst. (ICC-ROBINS)*, Sydney, Australia, 2024, pp. 890-897.

[20] H. Liu, R. Li, Z. Zhang, and B. Tang, "Tao: Improving Resource Utilization while Guaranteeing SLO in Multi-tenant Relational Database-as-a-Service," *Proc. ACM Manag. Data*, vol. 2, no. 4, pp. 1-26, Sep. 2024.

[21] E. M. Shiriaev, A. S. Nazarov, N. N. Kucherov, and M. G. Babenko, "Analytical review of confidential artificial intelligence: Methods and algorithms for deployment in cloud computing," *Program. Comput. Softw.*, vol. 50, no. 4, pp. 304-314, Aug. 2024.

[22] D. E. Wolf, L. Louw, and D. Palm, "An analysis of blockchain versus relational databases for digitalising information flows in global supply chains using the analytic network process," *Int. J. Prod. Res.*, vol. 62, no. 14, pp. 5016-5035, Jul. 2024.

[23] S. C. Misra and K. Doneria, "Application of cloud computing in financial services: An agent-oriented modelling approach," *J. Model. Manag.*, vol. 13, no. 4, pp. 994-1006, Nov. 2018.

[24] E. A. Shammar and A. T. Zahary, "The Internet of Things (IoT): A survey of techniques, operating systems, and trends," *Library Hi Tech*, vol. 38, no. 1, pp. 5-66, Apr. 2020.

[25] H. Alabool, A. Kamil, N. Arshad, and D. Alarabiat, "Cloud service evaluation method-based Multi-Criteria Decision-Making: A systematic literature review," *J. Syst. Softw.*, vol. 139, pp. 161-188, May 2018.

[26] P. Elango, K. Kuppusamy, and N. Prabhu, "Data Replication Using Data Mining Techniques," *Asian Journal of Computer Science and Technology*, vol. 8, no. S1, pp. 107-109, Feb. 2019.

[27] S. De and J. Mishra, "A New Approach of Functional Dependency in a Neutrosophic Relational Database Model," *Asian Journal of Computer Science and Technology*, vol. 8, no. 2, pp. 44-48, Apr. 2019.

[28] S. Mamatha and T. Sudha, "A Survey on Big Data Analytics Using HADOOP," *Asian Journal of Computer Science and Technology*, vol. 8, no. S3, pp. 35-40, Apr. 2019.

[29] B. Kotte and T. S. Madhuri, "Providing Security to Ensure Biometric Identification System in Cloud," *Asian Journal of Computer Science and Technology*, vol. 8, no. 3, pp. 1-5, Jul. 2019.

[30] G. Thangarasu, P. Dominic, M. C. Johnwiselin, and S. P. P. Kumar, "Fashions in Data Mining and Hidden Knowledge Innovation from Clinical Database," *Asian Journal of Computer Science and Technology*, vol. 1, no. 2, pp. 36-39, Nov. 2012.