Cloud Database Security Issues and Challenges: A Review

Aishah Alfarhan [1], Reem Alhussain[1], and Murad Rassam [1,2,*]

[1] Department of Information Technology, Colleg of Computer, Qassim University, Buraydah, Saudi Arabia

[2] Faculty of Engineering and Information Technology, Taiz University, Taiz, Yemen

ABSTRACT *Recently, cloud computing has been a heavily adopted technology by most businesses, simultaneously, the database has also shifted to the cloud computing environment. This paradigm called cloud database, and it can reduce data management costs and allow new business to focus on the delivered product. Moreover, cloud computing can be mean to solve scalability, flexibility, performance, availability and cost problems. However, security has been identified as a major threat to the cloud database, and it has played a critical role in cloud computing acceptance. Different aspects of security should be considered during the deployment of any cloud database management system. These aspects include abut are not limited to data confidentiality, data integrity, data availability, data privacy, data isolation, and the protection from insider attacks. In this paper, we address the state-of-the-art studies that considered such security challenges and issues facing the adoption of a cloud database. We also propose a conceptual model to summarize and provide a better understanding of these issues and their effect on cloud database. Furthermore, we investigate such issues according their relevant level and show two examples of vendors and the security feature that were practiced for the database on the cloud. Finally, we summarize the open cloud databases security issues and recommend some future directions.*

INDEX TERMS

Cloud Computing, Cloud Database Management System, Data Security, Database Security.

1. INTRODUCTIONS

Cloud computing can be defined as the delivered applications as services over the Internet, along with the hardware and system software resides in the data centers that provide those services [1]. Overall, the cloud computing model has three basic deployment models which are: Public cloud, Private clouds and Hybrid cloud [2]. The main categories of cloud computing services are Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS) [2]. Moreover, a new type called database-as-a-service (DBaaS) has been identified recently, and it could fall under any of these main types, based on its specifications [3].

The security issue has played a main role in cloud computing acceptance. Like the idea of putting your critical data, executing your software on someone else's hard disk using someone else's CPU can be terrifying to many. Security issues include data loss, phishing, and botnets, which cause damaging threats to an organization's data and software [2]. Furthermore, the multi-tenancy model and the shared computing resources in cloud computing has posed new security challenges (e.g. Botcloud Attack) which require novel techniques to deal with [2].

DBaaS or as called cloud database is a special database designed for virtualized computer environment (i.e. cloud environment), and it is mainly utilized for storing huge data on the cloud [4]. With the various utilization of different applications in the cloud, Database as a Service (DBaaS) becomes a promising way to provide cloud applications with trustworthy and flexible data storage services[5]. The cloud-based IT infrastructures act as a mean of solving scalability, performance, availability and cost problems [6]. However, cloud database is not as simple as deploying a relational database over a cloud server, it means adding more nodes when needed online, and improving the performance of the database. Leading examples of DBaaS include Apache Cassandra database, Amazon RDS and Microsoft SQL Azure [7].

Overall database in cloud computing can be either NoSQL database or relational database. NoSQL database stands for (Not Only SQL), but it is also useful for applications that deal with massive semi-structured and unstructured data, such as big data [8]. NoSQL database stores data in four main models which are Column-oriented, Key-value, Document-based,

*Corresponding Author: Murad A. Rassam (m.qasem@qu.edu.sa)

and Graph-based models [8]. Most NoSQL databases are designed to be scaled across several data centers and execute as distributed systems, which makes it a good choice for cloud computing infrastructure [9].

On the other hand, it is very tricky to keep distributed multiple copies of the database at various locations. Thus, the cloud database needs to be accessed and managed by a secured framework to access and manage cloud data [10]. Challenges that can face the adoption of cloud database include (1) efficient multi-tenancy, (2) elastic scalability, (3) and database security and privacy [7]. Furthermore, the tradeoff of data security for scalability and cost savings has led businesses to identify database security as the main issue in this sector [6].

Recently, 7.5 million customer records were exposed to Adobe Creative Cloud database and published online. Adobe Systems Inc. confirmed that the data exposure was a result of a vulnerability related to a misconfigured prototype environment. The exposed data were including email addresses, product subscriptions, payment statuses, login updates and other information, which can be later used in social engineering attacks, leading to account takeover and identity theft or so [11]. Moreover, the Cloud Security Alliance (CSA), which is a leading organization that defines best practices to ensure a secure cloud computing environment. In 2019, the company reported the topmost cloud computing security threats which are listed based on its significance [12]: data breaches, misconfiguration and inadequate change control , lack of cloud security architecture and strategy, insufficient identity, credential, access and key management, account hijacking, insider threat, insecure interfaces and APIs, weak control plane, megastructure and applistructure failures, limited cloud usage visibility and abuse and nefarious use of cloud services

In this paper, we address the security challenges and issues facing the adoption of a cloud database. The rest of the paper is structured as follows. Section.2 some related works and surveys in the same research field. Section 3 reviews the cloud database architecture. Section 4 addresses the cloud database security issues. Section 5 provides discussion and analysis, and Section 6 summarizes the open issues that can be researched in the future. Section 7 concludes this paper.

2. Related Works and Surveys

The related work in the cloud database sector can be classified into surveys that discussed general issues, and others which discussed special security issues in details such as auditing [13] and encryption [14] in cloud computing. Table.1 shows the differences and similarities between these studies including our survey.

A survey made by Deka et al. [8], addressed 15 popular cloud databases with providing an overview of each system and its storage platform, license type, and programming language. An example of a NoSQL database is a Cassandra database which stores data as a column-oriented database, and it is an open-source system written in Java. Another example is ClearDB which is a MySQL based database developed in C/C++ and it is also an open-source [8].

Han et al.[15] provided a background of the NoSQL database, the authors started by comparing the traditional database and NoSQL database. After that, they defined a NoSQL database features and data model along with its advantages and disadvantages. Each of the three data models (Key-value, Column-oriented, and Document) clearly defined by database examples and classification of these models based on the consistency, availability, and partition tolerance CAP theorem. Finally, the authors advise companies to check a list of options when deciding to use the NoSQL database which includes in (data model, CAP Support, multi-data center support, capacity, performance, query API, reliability, data persistence, rebalancing, and business support).

Researchers in [16] investigated the insider threat in the cloud relational database and how a cloud database structure can affect the security gaps, by enabling insiders to launch an attack. The proposed solution consisted of three mitigating models which include in (Peer-to-Peer, Centralized, and Mobile- Knowledgebases models), all three solutions were built based on the effect of the knowledge base of insiders, by controlling query execution after checking insider's knowledgebase (profiling insider's activities). The load balancing also was proposed to control the previously proposed models, to avoid launching an attack by a combination of data items that an insider can get from available data zones.

Researchers in [17] provided a comprehensive survey of cloud computing security. They covered in this work the security challenges and risks of each cloud model and service type, then they discussed the general threats of cloud computing that represent numbers of vulnerabilities such as data breach, denial of service (DoS), API browser vulnerabilities, malicious insider and more. Finally, the authors presented the countermeasures against the previously discussed threats. Countermeasures, which include end-to-end encryption, scanning for malicious activities (i.e. Firewall and Intrusion Detection Systems (IDS)), validation of cloud consumer, secure Interfaces and APIs, and business continuity plans.

Authors in[18] produced a work that aims to classify the cloud SaaS security patterns. Authors motivated in this work to present a new reference of official security best practices and security knowledge documentation to be used aa a guideline by the developers of cloud SaaS applications. They classified cloud SaaS security pattern into five categories which are firstly the compliance and regulatory that is related to laws governing the processing and usage of data in the

cloud. The second pattern is the identification, authentication, and authorization. The third pattern is the secure development, operation, and administration. The fourth pattern focused on privacy and confidentiality. Finally, the fifth pattern is a secure architecture. The authors concluded their study by providing a comparison of security solutions in AWS and Azure, which are the most famous cloud SaaS providers. Table 1 compares the existing surveys and shows the position of the proposed survey in this paper with respect to how existing surveys dealt with security issues and solutions of the cloud database environment.

TABLE 1. Related Surveys

Study Reference	Include Security solutions	Include Security threats& attacks	Study field		Include real examples of Cloud providers			
			Cloud Computing	Cloud DB	AWS	Azure	Oracle	Google
[8]	-	-	-	√	-	-	-	-
[15]	-	-	-	√	-	-	-	-
[16]	√	√	-	√	-	-	-	-
[13]	√	√	√	√		-	-	-
[14]	√	-	√	√		-	-	-
[17]	√	√	√	-	-	-	-	-
[18]	√	√	√	-	√	√		

3. Cloud Database Structure

Database environments in cloud computing can vary, for instance, some environments use a multi-instance model, while others use a multi-tenant model. The multi-instance provides a unique database management system (DBMS) running on a VM instance for each user, offering the user complete control for many security-related tasks. While the multi-tenant model provides a predefined environment for the cloud user with sharing it with other tenants, typically by tagging data with a unique user identifier. In the later, the cloud service provider is the one responsible to maintain a secured database environment [19].

Authors in [20] introduced a 5-layered architecture of a cloud database management system as shown in Fig 1. The 5 layers include the external layer that deals with the user followed by a conceptual middleware layer which hides the details of heterogeneity in the conceptual layer where different types of databases like DB2, SQL, and Oracle are used. The conceptual layer substitutes the logical structure of the entire database and concerns with the data processing. The physical middleware layer hides the details of heterogenous platforms such as Windows, macOS, Linux, among others, that are used. The last layer which is the physical layer concerns about the physical representation of data.

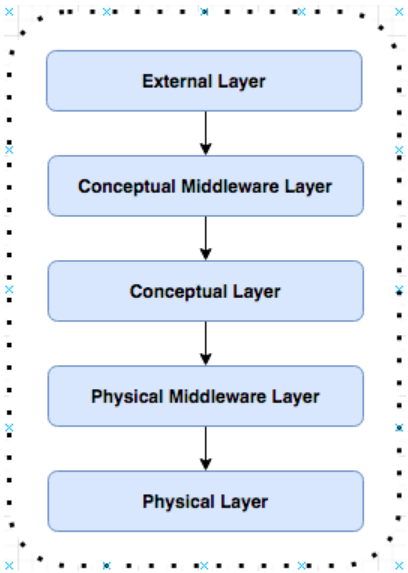

Figure 1. Cloud Database Management System [20]

In a cloud database, data are shared and distributed across several locations and may have a certain privilege and authentic information. Therefore, it's very critical to ensure data consistency, scalability and security. To deal with these

issues and others regarding data, a DBMS for cloud data is mandatory. Overall, in the cloud environment, there are two main DBMS architectures are used which are: shared-nothing and shared disk [10].

Firstly, shared-nothing is a distributed computing architecture where each node is self-sufficient and independent of any other node i.e. each node holds its memory and disk storage whiteout sharing them. Secondly, shared disk architecture is a computing architecture where the node has its memory but with a shared disk storage space. It segments the data as each database server processes and holds its piece of the database. Both shared nothing and shared disk architectures have limitations and issues, therefore, there are many efforts on the cloud database management system architecture field [10, 20].

4. Cloud Database Security

It was debated that DBaaS is a great option for companies with limited resources [14]. However, it can lead to numerous security issues, as the responsibility of database management and its underlying security is no longer managed by the data owner, but by a third party (i.e. the provider). Security has been recognized as a major threat to the data stored in cloud storage [14]. Therefore, in this section, we analyze the state-of-art security challenges in the cloud database, starting by the data-level security challenges, to the overall cloud database environment security issues.

4.1 Data Protection Challenges

In cloud computing, huge volumes of data are deployed and shared between many tenants; therefore, data protection is a critical aspect when storing them within the cloud database [10]. Mainly, data protection has four critical challenges which are data confidentiality, integrity, availability, isolation, and privacy [19, 21].

4.1.1 Data Confidentiality

Data confidentiality is a significant matter for users to store their private or confidential data in the cloud database. Authentication and access control techniques are used to guarantee data confidentiality. In cloud computing, data confidentiality, authentication, and access control issues can be solved by increasing cloud reliability and trustworthiness. Also, cryptography can guarantee data con confidentiality, but simple encryption cannot be the case as it will raise key management problems and it cannot support complex database requirements such as query, parallel modification, and fine-grained authorization. For example, when querying encrypted data, the process can be computationally very expensive, therefore, it is impossible to guarantee confidentiality by naively encrypting the private data within a cloud database, as traditional encryption hinders the execution of SQL queries through a DBMS engine. Therefore, there are methods to simplify the encryption technique to be used in cloud database [22].

i- Homomorphic Encryption

Encryption is normally used to ensure data confidentiality; the Homomorphic encryption was proposed by Rivest. The implementation of this encryption can solve data confidentiality and data operations in the cloud. It assures that the ciphertext result is consistent with the clear text results; besides, the process, after all, does not require the data to be decrypted. The fully homomorphic encryption method can complete any operation that can be performed in clear text without decrypting, which is a breakthrough in this type of encryption. However, the encryption operation does the very complicated calculation, and require high computing power and storage. After all, the fully homomorphic encryption is still far from real applications [22]. Several encryption algorithms were proposed for ensuring the security of user data in the cloud computing, such as Diffie-Hellman [23] and a hybrid technique that combines RSA, 3DES, and random number generator [24].

ii- Encrypted Search and Database

As the homomorphic encryption algorithm is inefficient in the cloud, limited homomorphic encryption algorithm was proposed, so Encrypted search is a common operation [22]. There are many propositions of this type including (1) The transposition, substitution, folding, and shifting (TSFS) algorithm, which is a lightweight technique for database encryption [25]. (2) In-Memory Database encryption technique to ensure privacy and security of sensitive data in the untrusted cloud environment. (3) Asymmetric encryption mechanism for databases in the cloud [26]. (4) A privacy-preserving multi-keyword ranked search approach over encrypted data in the cloud [27].

iii- Data Concealment

Data concealment can be used to ensure data confidentiality in the cloud. Delettre et al. [28] proposed a concealment concept for databases security. It combines real data with the visual fake data to falsify the real data's volume, with the availability for authorized users to differentiate the fake data from the real one, using the watermarking method. The goal of data concealment is to make private data secure from malicious users.

iv- Distributive Storage

To ensure the data integrity, we can store data in multiple clouds or cloud databases, this has become a promising approach in the cloud environment [22]. One way to do that was proposed by Ram et al.[29] by introducing a technique known as security as a service for securing cloud data. The technique was relaying on dividing the user's data into pieces to fulfil maximum security. These data chunks are then encrypted and stored within separated databases to form the concept of data distribution overcloud.

4.1.2 Data Integrity

Data integrity in cloud computing means that data should not be lost or modified by unauthorized access, and it is considered as the basis to provide cloud computing service, specially DBaaS. As the result of a large number of entities and access points in a cloud environment, authorization is a crucial aspect which means assuring that only authorized entities can interact with data, in which eventually can achieve greater trust in data integrity. Also, monitoring mechanisms can provide great visibility into determining who or what may have altered the data and affected its integrity. Finally, cloud computing environment normally offers data processing service, thus data integrity can be acquired by techniques such as RAID-like strategies and digital signature [22].

4.1.3 Data Availability

Database in the cloud must be highly available and reliable [10], and it is one of the critical security aspects that organizations need to consider when providing cloud database services [30], one known attack of data availability is Denial-of-Service (Dos/DDoS) attack. To accomplish that, cloud data storage must be stored redundant, using distributed storage technique and backups. Traditional relational database faces the problem of high scalability and availability, huge storage, and high performance, therefor, NoSQL database is made, and it is a better fit in cloud computing. Also, distributed database proxy can provide high availability, as the secondary disk database can achieve fast data recovery [25]. Finally, cloud database availability level, data backup options and disaster recovery techniques should be addressed fairly before moving to a cloud environment [30].

4.1.4 Data Isolation

In cloud computing, data can take many forms. For instance, in deployed applications, data can include contents created or used by the application, as well as the users' account information. Data encryption and access controls techniques are the means to keep data away from unauthorized access. Access controls are normally identity-based, which rise the importance of user's identity authentication and its issues in cloud computing. In the multi-tenant model, there are different types of arrangements for databases, each type of pools resources in a different form, offering various degrees of isolation and resource efficiency. For instance, data encryption is viable with arrangements that use separate rather than shared databases. After all, these types of tradeoffs need a careful evaluation of the suitability of the data management solution for the targeted data, with taking into account the field sensitivity in which the cloud is deployed (e.g. healthcare system) [19].

4.1.5 Data Privacy

A serious barrier to deploying databases in the cloud is the lack of privacy, which reduces users' trust in the system. Clients can utilize data encryption of all stored data within the DBaaS, to eliminate the privacy concerns. This drive the question of how can the DBaaS execute queries over the encrypted data? which leads to efficiently challenge [31]. Therefore, as aforementioned above, several approaches were proposed to solve the problem of encrypted data query. For example, a design architecture was proposed by [7] to utilize CryptDB into the relational cloud (i.e. transactional DBaaS) to solve data privacy problems. CryptDB is a system proposed by the researcher of MIT, that delivers practical and provable data confidentiality for applications that use SQL databases. It executes SQL queries over encrypted data using several efficient SQL-aware encryption schemes [31]. Also, data anonymization is a privacy-preserving technique, it makes the data identification, not an easy task for anybody except for the owners [26].

4.1.6 Data Sanitization

Sanitization process involves the efficient deleting of data from storage media by overwriting, degaussing, or destruction the media itself, to prohibit any unauthorized disclosure of data. In a public cloud environment, multiple customers' data are physically co-located together, that makes the sanitization process more complicated. Additionally, the data backups that are made to ensure high redundancy adds more complications[6]. Data sanitization issues are the result of the insufficient implementation of destruction policy, non-wiped, multi-tenant use of hard disk and irreversible resources[27].

The NIST published the DoD 5220.22-M ("National Industrial Security Program Operating Manual") and NIST 800-88 ("Guidelines for Media Sanitization"), as guidelines that contain general procedures to perform a data sanitization for customers. Overall, cloud providers have limited options for data sanitization, but with limitations, such as storage encryption within the cloud, as to ensure that if the storage media is not properly sanitized, the data is unreadable without the key.

4.2 Cloud Database Security Issues

In this section, we analyze the security challenges facing the database when working within the cloud environment.

4.2.1 Insecure Application Programming Interfaces (API)

To allow clients to manage and interact with cloud services, cloud computing providers offer a set of software interfaces for APIs, which allow providers to perform provisioning, management, orchestration, and monitoring using these interfaces. Both security and availability of cloud services are relays on the security of these APIs. Therefore, APIs must provide authentication and access control along with encryption and activity monitoring, Also, these interfaces must be resistance to either accidental or malicious attempts to revoke policies [32].

4.2.2 Authentication and Access Control (AAC) Issues

As we stated before, the cloud environment deal with multitenant that shared cloud resources. Therefore, there is a need for sufficient authentication and authorization control to guarantee isolation for each tenant and avoid privacy violations [33]. To grant user access and use cloud resources, authentication applied to confirm the user's identity, while authorization applied to control access based on predefined privileges. However, identity management and credentials are stored differently, based on the deployment models of the cloud database. In a private cloud, credentials are stored in the server, in the form of Active Directory (AD) or Lightweight Directory Access Protocol (LDAP). While public cloud providers use API to authenticate users. Therefore, authentication in a public cloud is more subject to vulnerability than a private cloud [34]. A broad consideration of authentication in the cloud, that we should consider authenticating the machines also, which enables automated actions like online backup, patching and updating systems and remote monitoring systems [34].

The most security concern in AAC is broken authentication and session control threat, that occurs due to misconfiguration of account management functions, for example, the attacker can gain benefit by an exposed user's session IDs that appear in the URL, resulting from compromised passwords, keys, and session tokens.

We can mitigate these issues by adopting strong authentication and session management controls, prevention of Cross-site Scripting (XSS), and using indirect object references for each user or session[4]. Also, to avoid security issues related to AAC, cloud providers develop and adopt different methods and standards, such as single-sign-on policy, Multi-factor authentication, and RSA cryptosystem. Besides, most of the cloud providers adopt open authentication protocols, which enable users to share their private resources using tokens-based API rather than passwords. The most used open authentication protocols by cloud providers according to [34]are Open Authorization (OAuth), and Security Assertion Markup Language (SAML).

4.2.3 Cloud Database Misconfigurations:

Some cloud providers are poor in offering features of auditing and monitoring to their customers. This may lead to failures and breaches due to cloud misconfiguration issues. Dependence on traditional configuration is no longer useful, because of the dynamic nature of the cloud database environment. Therefore, cloud providers must offer an auditing technique/tool, that produces full visibility into database activities, irrespective of database location [35].

A proper configuration and secure database implementation, which is based on meeting the criteria of a proper audit trail, is called an immutable database, that restricts access by authorized users only [33].

4.2.4 Multi-Tenancy Vulnerability

In a multi-tenant database system, one of the major security concerns is the data isolation issue. As the multi-tenant database contains many tenants (users/customers) accessing one database, so cloud providers should provide isolated accessing of databases among the different tenants. Ensure data isolation have a positive effect on user privacy and data protection. On the other hand, ignore the adopting of data isolation may lead to security breaches and data exposure [36].

Another security issue of the multi-tenant database is authorization and authentication within the system. To achieve proper prevention of these issues, first, we should apply strong access control along with authentication protocols to support the authentication process. Second, paying attention to the role of managing permissions and privileges to support authorization of the database. Successful authentication and authorization are affective against non-authorized access attack [36].

Cloud providers should examine basic factors before the adoption of a Multi-tenant database, such as the number of tenants, users per tenant, growth rate, and security of tenant database [36]. For example, attackers can leverage a cloud to establish botnet base (i.e. Botcloud attack), as the cloud can provide a reliable infrastructure at a relatively cheaper price for the attacker to launch an attack, this attack is a type of a cloud service abuse [2].

4.2.5 Data Loss or Leakage

The threat of data compromise raises in the cloud environment, mainly because of the number of and interactions between risks and challenges which are either unique to the cloud or riskier due to the architectural or operational characteristics of that environment. Data loss can be caused by the deletion or alteration of records without a proper backup. Poor linking of documents from larger records when lost or altered makes data unrecoverable. Also, losing the encoding key can result in real destruction. Finally, sensitive data must be prevented to access by any unauthorized parties. This risk can be mitigated using strong API access control and encryption. Also, efficient data storage, management and destruction process, with data protection analysis at design and run time and contractual specification of backup and retention procedures can be useful [32].

4.2.6 Account, Service and Traffic Hijacking

This threat includes numerous attacks such as phishing, fraud and exploitation of the software. When the attacker gains access to account's credentials, they can leverage an eavesdropping attack on activities and transactions, manipulate data, return false information, and redirect clients to malicious sites. To mitigate these attacks, it is essential to limit account sharing between a client and the services providers. Also, two-way authentication techniques and utilizing proactive monitoring measures to detect suspicious/unauthorized activities are crucial [15].

4.2.7 Malicious Injection Attack

This attack targets SQL servers with vulnerable database applications. When attackers exploit vulnerabilities of web servers, they inject a malicious script to bypass authentication and gain unauthorized access to backend databases. If successful, attackers can inject SQL scripts to manipulate database contents, gain confidential data, remotely execute system commands, or employ the web server for future use. Also, SQL injection attack can be delivered by a botnet, for instance, the Asprox botnet which controlled a thousand bots with equipped SQL injection kit to perform an SQL injection attack. This botnet attacked six million URLs of different153,000 web sites [37].

On the other hand, cross-site scripting (XSS) attacks are recognized as one of the most dangerous attacks to databases and web applications. Attackers can inject malicious code, such as JavaScript, VBScript, ActiveX, HTML, and Flash, into a vulnerable database or web page which will be executed on the victim's web browser. After that, the attacker can either steal the victims' session cookie used for authorization, get access to the victim's account, or manipulate the victim into clicking a malicious link. A research team in Germany have successfully demonstrated an XSS attack against Amazon AWS cloud platform[38]. They exploited a vulnerability in Amazon’s store which allowed them to hijack an AWS session and get access to all customer records, including authentication data, tokens, and plain text passwords [37].

4.2.8 Insider Threats

A malicious insider is a familiar threat within every business organization. This security threat becomes more visible when addressing cloud environment. As a result of the fusion of customers and services providers into one management sector, and the lack of transparency in the provision of process and procedures, which will eventually result in a security

gap. This issue can be eliminated by conducting an assessment on the supply chain management and ensure the enforcement of strict rules [32].

5. Discussion and Analysis

Based on our research, we can conclude that cloud database offers many benefits to companies, besides the efficient security solutions and management, as the database has many security requirements and issues, therefore choosing to outsource the database as a service of a cloud provider can be efficient solution to focus on the company's output. Table.2 summarizes a comparison between traditional and cloud database.

TABLE 2. Comparison between Traditional and Cloud Database

Criteria	Traditional Database	Cloud Database
Reliability	Reliable	Comparatively more reliable
Scalability	Limited scalability	Unlimited scalability
Cost	Setup cost very high	pay-per-use model
Security	Security under control	Security relay on the vendor
Availability	Limited availability	high availability

Moreover, we can admit haw security issues are a major threat to the cloud database. Overall, security challenges in this paradigm are a combination of inheriting the security issues of cloud computing and database. In this work, we propose a conceptual model to form the security challenges and issues that hinder the adoption of a cloud database, as shown in Fig 2.

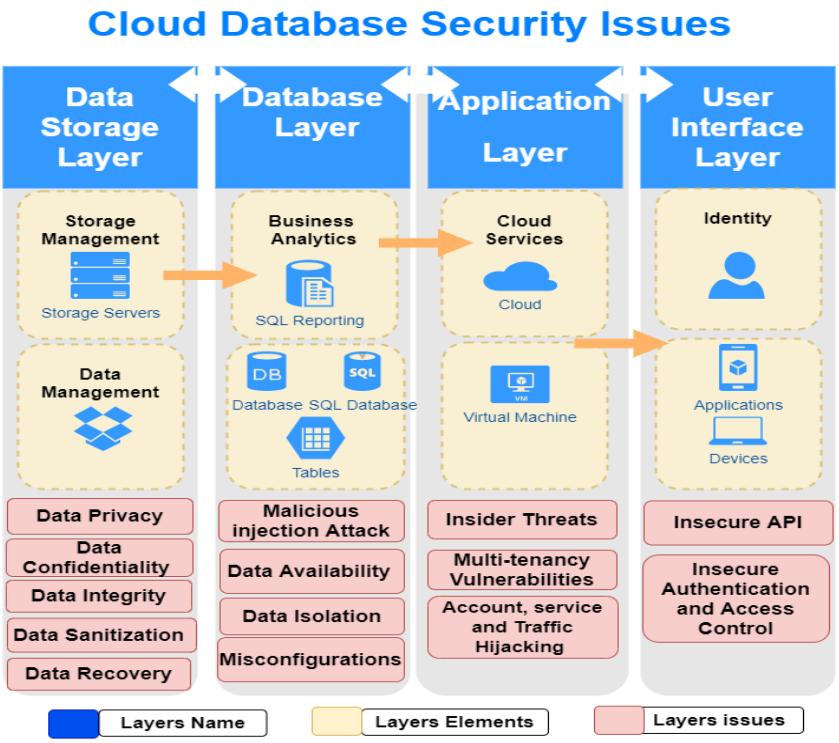

Figure 2. A Conceptual Model for Understanding the Cloud Database Security Issues

In the model, we classified the security issues into four levels: data-level security, Database-level security, and Cloud-level security. Data security constitutes an important part of the issues faced database on the cloud. All security issues that

are related to confidentiality, integrity, privacy among other data security issues such as data sanitization and data recovery are inherited from the traditional data processing systems into cloud systems.

In the database layer level, the important security issues include the malicious injection attack such as the well-known SQL injection attack. In this level, data availability is a concern as the database management systems should ensure the use of database elements such as table contents, queries, etc when needed. The issue of data isolation is also a matter of concern at this level. It requires that user's information in addition to other information added by the database management application should be isolated when some security operations such as encryption are applied. Avoiding the outcomes of misconfigurations should also be considered in the database management level. This is necessary because of the dynamicity of the cloud environment which requires more monitoring and auditing of the user's transactions over time.

The application layer also suffers from different types of security issues that include insider attacks that may occur due to untrusted applications. In addition, the multi-tenancy feature of cloud computing might be exploited to run numerous types of vulnerabilities especially in the environments that trust users. The traffic hijacking is also considered as a type of security issues in the application layer. This hijacking might happen on the level of a user application or any necessary service that should be run to allow the functionality of the application.

In the scope of the user interface layer, the insecure application programming interface (API) might be the weakest point that might be exploited by the attackers. Knowing the sockets of the interface may lead to different types of attacks such as DoS attack among others. Another important issue in this layer is the improper authentication process or the unsuitable access control privileges that result in an unauthorized login and a misuse of the database assets on the cloud.

To mitigate the previous security issues, companies can identify their security level needs. For example, if a company need a high available database it chose the vender that provide that feature. Therefore, companies can compare the security features of available cloud database vendors to choose the best fit for their needs. As an example on how customers prioritize their needs and focus on the features required in cloud database service, Table 3 summarized the security features of two cloud database vendors, which are Amazon AWS, Microsoft Azure and Oracle Cloud database.

TABLE 2. Security Features in Amazon AWS, Microsoft Azure and Oracle Cloud Database

Category	Security Pattern	Amazon AWS	Microsoft Azure	Oracle Cloud DB
AAC	Access token	Security token service	Azure Active directory (token service)	Available
	Single sign-on	AWS SSO	Azure AD SSO	Oracle SSO
	Multifactor Authentication	AWS Cognito	Azure Active Directory multi-factor	Oracle MFA
Data Privacy and Confidentiality	Computation on encrypted data	N/A	N/A	Available
	Encrypted at rest	Available	Available	Available
	Data Anonymization	AWS algorithms e.g. Lambda	Dynamic data masking on SQL DB	Oracle Data Masking
	Secured Socket Layer (SSL) Certification	AWS Certificate manager	App Service Certificate	Oracle Secure Socket Layer
Data Availability	Data Recovery	e.g. DynamoDB backup	e.g. Azure Backup	Oracle Recovery Manager
	DDoS Protection	AWS Shield	Azure DDoS Protection	Oracle Web App firewall
Secure Architecture	Secure Auditing	Available	Available	Available
	Data Monitoring	Cloud Watch	Azure Monitor	Application Performance monitoring

	Resource configuration	AWS Config	Azure portal (audit logs)	Oracle cloud governance services

Finally, we can conclude that security in the cloud database depends on the encryption methods and the storage locations of the data, as in which data is stored in the different locations in data centers.

6. Open Issues

Based on the discussion and analysis of the security issues of a cloud database, some open issues can be introduced for further future research and investigation.

Efficient Encryption: There is a great need for much strong encryption algorithms and at the same time applicable for cloud environments. The proposed algorithms should not add an additional burden to the cloud processes and hence reducing the latency. Proper encryption schemes can preserve the confidentiality and integrity.

Enhanced Data Privacy Schemes: Data privacy is a vital concern for all cloud services. More privacy-preserved schemes are needed. Such schemes should keep customer information safe and reduce any violation by service providers.

Enhanced Trust Schemes: Most of cloud customers concern about the level of trust in cloud providers. Therefore, a great need for increasing the level of trust by involving the service of a third party in a proper way is required.

Application-Level Protection Schemes: As we noticed in Fig 2, the weakness of the database management application may threaten the security of data, especially if such applications are exploited by insiders who are authorized. Furthermore, the protection from the hijacking of applications and services is a very important issue that should be addressed. Therefore, application-based protection frameworks for cloud database management systems are required.

7. CONCLUSIONS

For the last ten years, cloud computing has been heavily adopted, leading to the concept of DBaaS, which has drawn the interest of both the industry and research community. Moreover, many companies have started adopting cloud computing and accessing their data from a cloud database. On the other hand, security has been identified as the major threat to the cloud database, and it includes challenges facing the data protection and may lead to serious security issues, such as insecure API and multi-tenancy vulnerabilities. However, security solutions in the cloud database depend on cryptography and secure storage solutions. Moreover, combining encryption with SQL operations within the cloud database is a promising approach although it has many open issues. In this work, we addressed the state-of-the-art security challenges and issues that can hinder the adoption of a cloud database. Also, we proposed a conceptual model to summarize and provide a better understanding of these issues and their effect on a cloud database, to assists better choice of cloud database provider. Finally, we point out how companies compare cloud database providers based on their security needs.

We observe that researchers are taking interest in contributing to this field, by researches that support security to the cloud database. The future direction could cover encryption solutions (simplified encryption techniques), secure access control, privacy (anonymize and encrypt data), and data sanitization (still an open issue).

REFERENCES

[1] Armbrust, M., et al., A view of cloud computing. Communications of the ACM, 2010. 53(4): p. 50-58.

[2] Kuyoro, S., F. Ibikunle, and O. Awodele, Cloud computing security issues and challenges. International Journal of Computer Networks (IJCN), 2011. 3(5): p. 247-255.

[3] Weis, J. and J. Alves-Foss, Securing database as a service: Issues and compromises. IEEE Security & Privacy, 2011. 9(6): p. 49-55.

[4] Al Shehri, W., Cloud database database as a service. International Journal of Database Management Systems, 2013. 5(2): p. 1.

[5] Khan, S., et al., Bivariate, Cluster and Suitability Analysis of NoSQL Solutions for Different Application Areas. arXiv preprint arXiv:1911.11181, 2019.

[6] Sakhi, I., Database security in the cloud. 2012.

[7] Curino, C., et al., Relational cloud: A database-as-a-service for the cloud. 2011.

[8] Deka, G.C., A survey of cloud database systems. It Professional, 2013. 16(2): p. 50-57.

[9] Mongo, D., Nosql databases explained.

[10] Alam, M. and K.A. Shakil, Cloud database management system architecture. UACEE International Journal of Computer Science and its Applications, 2013. 3(1): p. 27-31.

[11] RILEY, D., "7.5M customer records exposed on Adobe Creative Cloud database in SiliconANGLE. 2019.

[12] CSA, CSA Releases New Research - Top Threats to Cloud Computing: Egregious Eleven. 2019, Cloud Security Allowance (CSA).

[13] Sawant, N., V. Pottigar, and N. Mane. A survey on auditing techniques used for preserving privacy of data stored on cloud. in 2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT). 2016. IEEE.

[14] Gong, S. and X.X. Huang. Study on database encryption-based protection mechanism under cloud computing environment. in 2016 2nd IEEE International Conference on Computer and Communications (ICCC). 2016. IEEE.

[15] Han, J., et al. Survey on NoSQL database. in 2011 6th international conference on pervasive computing and applications. 2011. IEEE.

[16] Yaseen, Q. and B. Panda. Tackling insider threat in cloud relational databases. in 2012 IEEE Fifth International Conference on Utility and Cloud Computing. 2012. IEEE.

[17] Ramachandra, G., M. Iftikhar, and F.A. Khan, A comprehensive survey on security in cloud computing. Procedia Computer Science, 2017. 110: p. 465-472.

[18] Rath, A., et al., Security Pattern for Cloud SaaS: From System and Data Security to Privacy Case Study in AWS and Azure. Computers, 2019. 8(2): p. 34.

[19] Sen, J., Security and privacy issues in cloud computing, in Cloud Technology: Concepts, Methodologies, Tools, and Applications. 2015, IGI Global. p. 1585-1630.

[20] Alam, B., et al., 5-layered architecture of cloud database management system. AASRI Procedia, 2013. 5: p. 194-199.

[21] Hussain, S.A., et al., Multilevel classification of security concerns in cloud computing. Applied Computing and Informatics, 2017. 13(1): p. 57-65.

[22] Sun, Y., et al., Data security and privacy in cloud computing. International Journal of Distributed Sensor Networks, 2014. 10(7): p. 190903.

[23] Boneh, D. The decision diffie-hellman problem. in International Algorithmic Number Theory Symposium. 1998. Springer.

[24] Kaur, A. and M. Bhardwaj, Hybrid encryption for cloud database security. Journal of Engineering Science Technology, 2012. 2: p. 737-741.

[25] Han, J., M. Song, and J. Song. A novel solution of distributed memory nosql database for cloud computing. in 2011 10th IEEE/ACIS International Conference on Computer and Information Science. 2011. IEEE.

[26] Sedayao, J. and I.I. Enterprise Architect, Enhancing cloud security using data anonymization. White Paper, Intel Coporation, 2012.

[27] Singh, S., Y.-S. Jeong, and J.H. Park, A survey on cloud computing security: Issues, threats, and solutions. Journal of Network and Computer Applications, 2016. 75: p. 200-222.

[28] Delettre, C., K. Boudaoud, and M. Riveill. Cloud computing, security and data concealment. in 2011 IEEE Symposium on Computers and Communications (ISCC). 2011. IEEE.

[29] Ram, C.P. and G. Sreenivaasan. Security as a service (sass): Securing user data by coprocessor and distributing the data. in Trendz in Information Sciences & Computing (TISC2010). 2010. IEEE.

[30] Bollavarapu, S. and K. Mistry, Secure Database as a Service-a Review. International Journal of Advanced Research in Computer and Communication Engineering Vol, 2015. 4: p. 425-429.

[31] Popa, R.A., et al. CryptDB: protecting confidentiality with encrypted query processing. in Proceedings of the Twenty-Third ACM Symposium on Operating Systems Principles. 2011.

[32] Izang, A., et al., Security and ethical issues to cloud database. Journal of Computer Science and Its Application, 2017. 24(2): p. 65-75.

[33] Malhotra, S., et al., Cloud Database Management System security challenges and solutions: an analysis. CSI transactions on ICT, 2016. 4(2-4): p. 199-207.

[34] Kumar, P.R., P.H. Raj, and P. Jelciana, Exploring data security issues and solutions in cloud computing. Procedia Computer Science, 2018. 125: p. 691-697.

[35] Mehak, F., et al., Security aspects of database-as-a-service (DBaaS) in cloud computing, in Cloud Computing. 2014, Springer. p. 297-324.

[36] Matthew, O., C. Dudley, and R. Moreton. A Review Of Multi-Tenant Database And Factors That Influence Its Adoption. in UKAIS. 2014.

[37] Deshpande, P., S. Sharma, and P.S. Kumar. Security threats in cloud computing. in International Conference on Computing, Communication & Automation. 2015. IEEE.

[38] 38.Constantin, L. Researchers demo cloud security issue with Amazon AWS attack. 2011 [cited 2020 20-07-2020].