Security Policies for Securing Cloud Databases

Ingrid A. Buckley
Department of Computer Science
Tuskegee University
Tuskegee, Alabama, USA

Fan Wu
Department of Computer Science
Tuskegee University
Tuskegee, Alabama, USA

***Abstract*—Databases are an important and almost mandatory means for storing information for later use. Databases require effective security to protect the information stored within them. In particular access control measures are especially important for cloud databases, because they can be accessed from anywhere in the world at any time via the Internet. The internet has provided a plethora of advantages by increasing accessibility to various services, education, information and communication. The internet also presents challenges and disadvantages, which include securing services, information and communication. Naturally, the internet is being used for good but also to carry out malicious attacks on cloud databases. In this paper we discuss approaches and techniques to protect cloud databases, including security policies which can realized as security patterns.**

Keywords—relational database; cloud; security; threats; hackers, security patterns; cloud database

I. Introduction

Technology has changed the way businesses conduct their daily tasks and processes. Most businesses have evolved in how they utilize data, most times they have to collect, query, manipulate and store data rapidly in order to provide services to their consumers. Databases are one of the most common resources used for business. Today, Relational Database Management System (RDBMS) is a staple resource in businesses of all types. In particular, cloud databases provide increased accessibility to valuable information that is stored to carry out business functions. The main advantages of the cloud are increased availability, scalability, elasticity and performance of databases.

The Internet, since its inception, has been continuously evolving, creating both problems and solutions. The cloud lives in the internet and has inherited the benefits, challenges and problems associated with the Internet. The cloud is still a relatively new approach in how technology and resources are shared through a network: the Internet. Cloud computing is by nature a dynamic and fast changing environment which is designed to provide services to various clients. The goals of these clients vary, from business owners, employees, customers to attackers. An attacker can take any form; this makes the job of security more complex and challenging. Since the introduction of cloud Databases, there has been sustained and increased attacks against web services and databases [1] which are primary aspects of the cloud. The goal of an attackers is to attack exploit the fundamental components of the cloud.

The paper is organized as follows. Section 2 presents background information on database security breaches. Section 3 provides an overview of cloud relational databases.

Section 4 presents some approaches to protect cloud databases. Section 5 discusses security patterns. Section 6 presents some related work. The paper concludes in section 7.

II. Security Breaches

On November 2013 the Target store databases were attacked, the personal and credit card information of 40 million customers was compromised [1]. In April 2010, hackers gained access to approximately 77 million PlayStation Network accounts. In this attack unencrypted credit card numbers, personal information and purchase history was compromised [2]. RSA servers were compromised my hackers which is the security division of EMC which is a huge storage company used by many financial institutions. EMC stores close 40 million authentication tokens used by employees to access corporate and government networks, the hackers were able to gain access to these tokens. Since this incident EMC has spent over 60 million to monitor the information of concerned clients. Similarly in August 2007 hackers attacked Monster.com and stole resume information of 1.3 million dollar job seekers [2]. These incidents are common and hackers continue to strengthen their efforts in attacking corporate, e-commerce and government systems. The problem associated with security breaches are far reaching and affect other aspect such as privacy and reliability. Security patterns can be used in software engineering/development solutions to solve security problems [3].

III. Cloud Relational Database Management System (RDBMS)

Database Management Systems (DBMS) provide an organized way to utilize data. They also secure information against system failure or tampering and permit data to be shared among multiple users. A Relational Database Management System (RDBMS) stores a collection of interrelated data that allows programs to access the data. A relational database allows the definition of data structures, storage, retrieval operations and integrity constraints. The data and relations between them are organized in tables. A table is a collection of records and each record in a table contains the same fields.

Fig. 1 illustrates a simplified example of the cloud architecture. Clients or users connect to the internet through their respective internet providers. Once the client is connected to the cloud, they have access to variety of infrastructure, services, and platforms. We are interested in The Relational

Database Management System (RDBMS) as shown in red below. The architecture of the cloud consists of virtual machines and hardware which consists of storage, servers and networks.

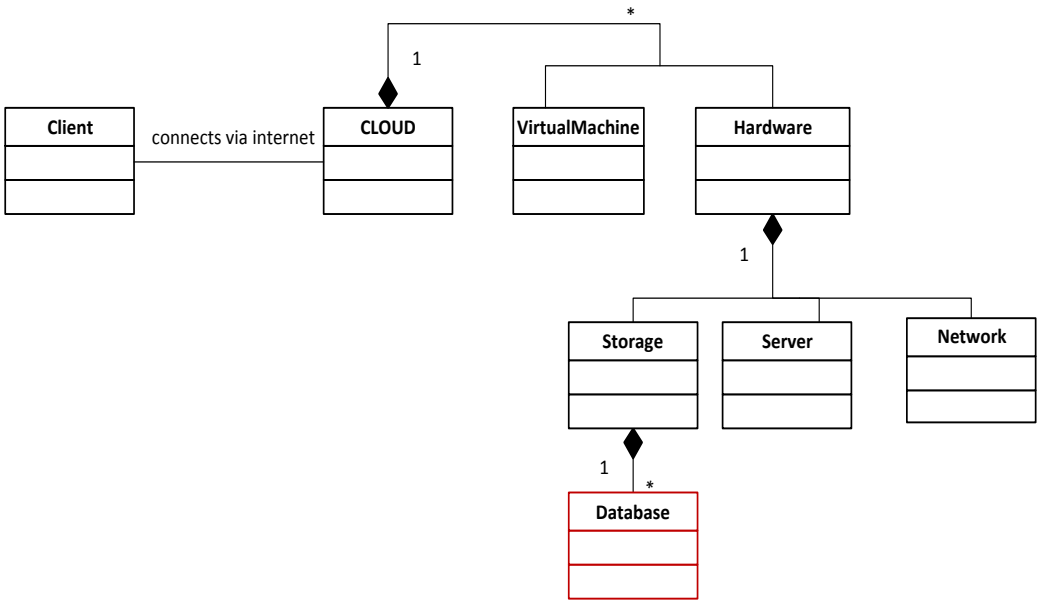

Fig. 1. Cloud Architecture

IV. Approaches and Techniques to Secure Cloud Databases

Security provides protection against unauthorized data disclosure, data modification, data destruction and denial of service. The database system is a fundamental aspect for security because it stores the persistent information, which constitutes most of the information assets for an institution. A private cloud is concerned with the internal needs of an organization. A public cloud sells resources to the general public. A hybrid cloud gathers resources from different clouds; it is a combination of public and private clouds. Due to the nature of the cloud environment, and the need to have active reliable security mechanisms, we enumerate here some common security and reliability policies which are used to protect cloud databases [8, 10]:

A. *Equations Security Policies:*

- **Least Privilege -** Limits access to resources by allowing only the minimal level of access, while still allowing an application to function normally.
- **Separation of Privileges** - Separates critical functions that can affect the security of the database into portions that is performed by different people or systems.
- **Authorization And Authentication -** Authorization defines permitted access to resources. Authentication verifies the identity of an entity requesting access to a resource [14].
- **Defense in Depth -** ensures that security controls are implemented at all levels of the information architecture including the database, network, sever, and operating system. This policy can be implemented using *Cloud Pools* [8].
    - A cloud pool is common set of resources that is shared by multiple tenants.
- **Logging and Auditing -** Tracks all activities by keeping a log of actions that may be relevant for security.
- **Information Hiding -** Conceals sensitive information with the use of cryptography and hashing functions.

B. *Reliability Policies:*

- **Redundancy** [13, 14] - The replication of critical components in a system or of a complete system with the intention of increasing the reliability of the system.
    - Additionally scheduling frequent backups of the DMBS is essential to restore corrupt/lost data if required.
- **Monitoring** [13, 14] - The constant checking of the state of a system to ensure that specifications are being met. This is a fundamental step because a security breach cannot be addressed if it is not detected.

Most databases do not implement all of the policies mentioned above; because this is not practical, due to the fact that increased security can result in a reduction in throughput and robustness. In particular, cloud databases have to respond quickly to requests in order to maintain their effectiveness. Many of these policies are described in pattern format to help developer's better implement security in cloud databases and environments.

Different security approaches and techniques have been proposed to secure databases that live in the internet or the cloud [10]. However despite the advances, hackers are still

finding ways to exploit vulnerabilities that go under the radar during development, testing and deployment. Access control is a very fundamental and critical security concern for databases that live online.

There are different types of users that interact with a database novice users, database administrators, programmers etc. Each of these requires a certain degree of leeway to perform their activities; as a result an authorized user can easily misuse their rights to compromise a database. Access control is generally achieved through one or more of the security policies discussed earlier.

V. Security Patterns

Patterns [3] embody the experience and knowledge of many designers and when properly catalogued, they provide a repository of solutions for useful problems. Initially used for improving code, patterns are becoming a staple tool to build secure systems [7, 9, 12]. The POSA [7] template defines a systematic way to describe patterns. It consist of approximately eleven units, each describes one aspect of a pattern. This template is designed to capture the experience and knowledge of professionals that have solved common problems. Patterns support best practices. Each unit of the POSA Template is described below:

a) ***Name*** - the name of the pattern should correspond to the generic name given to the specific type of attack in standard attack repositories such as CERT [11].

b) ***Intent or thumbnail description*** - A short summary of the intended purpose of the pattern, including which problem it solves

a. **Example** of a specific problem.

b. **Context** -this section describes where the pattern applies, including prerequisites and the general environment.

c. **Problem** - describe the forces which affect the solution, attacks.

d. **Solution** - describes the general idea of solving the problem, it includes UML models (static and dynamic), formalization.

e. **Implementation** – provides recommendations and hints for implementers

f. **Example resolved** - describes how the pattern solved the specific problem

g. **Known uses** - provides at least three examples of use in real systems

h. **Consequences** – provides advantages and disadvantages of the pattern's solution.

i. **Related patterns** - presents complementary or alternative patterns.

Security patterns describe mechanisms that control threats. Security patterns join the extensive knowledge accumulated about security with the structure provided by patterns to provide guidelines for secure system construction and evaluation. Security has had a long trajectory, resulting in a variety of approaches to analyze security problems and to design security mechanisms. It is helpful to capture this expertise in the form of patterns [7]. There are several books [10, 13] on security patterns and academic institutions that write and share security patterns. An attacker can attack a system from all levels. If a hacker does not find vulnerability in level n, then level n+1 or n-1 may have vulnerabilities that can be exploited. It is important to identify attacks at every level or stage in software development. Security patterns provide the following advantages:

- Security patterns embody experience and good design practices.
- They help to prevent errors, and save time.
- Can be reused.
- Provide guidelines to solve security problems.
- Provide best case solutions to common problems.

VI. Related Work

Google Cloud SQL [4] uses two level of access control before access is granted to the database. It first authorizes access to an instance using the host application ID or IP address. Second it authorizes the user or application to access the database. EDB Cloud database [5] provides role permission management, authentication of object permissions, auditing of user and application using logs and SQL injection protection. Oracle Database [6] provides label based access control to provide multi-level security and restricting access to data based on data classification and user security clearance. It also provides data encryption, data masking, blocks SQL injection attacks, and auditing of user and application activities.

VII. Conclusion

Database need effective access control security mechanisms to protect the data stored. In particular, cloud databases present a difficult problem because they can be accessed at anything through the Internet, therefore effective security mechanisms are necessary to protect them without affecting normal business operations. Not only is it important that a database as security controls but in addition, a wide variety of security policies are required at varying levels of a systems architecture to sufficiently protect it.

Acknowledgment

The This work has been supported in part by US. NSF grant # DUE-1241670 and US Department of Homeland Security Scientific Leadership Award grant # 2012-ST-062-000055.

References

[1] CNN Money. (2013, December 19).Target: 40 million credit cards compromised. Retrieved from: http://money.cnn.com/2013/12/18/news/companies/target-credit-card/ Last Accessed: 1/30/2014.

[2] CNN Money. (2011, April). 9 of the worst security breaches ever. Retrieved from: http://money.cnn.com/galleries/2012/technology/1206/gallery.9-worst-security-breaches.fortune/2.html. Last Accessed: 1/30/2014.

[3] Ingrid. A. Buckley and Eduardo. B Fernandez. (2009).Three patterns for fault Tolerance. Proceedings of the OOPSLA MiniPLoP.

[4] Google Cloud.(2012, October). Levels of access control. Retrieved from: https://developers.google.com/cloud-sql/docs/access-control. Last Accessed: 2/28/2014.

[5] EDB Cloud database. (2005, May). Postgres Plus Advanced Server: Better protection for your critical data. Retrieved from: http://www.enterprisedb.com/docs/en/9.3/conncloud/Tutorial_Connecting_to_a_Cloud_Database_Cluster.htm. Last Accessed: 2/28/2014.

[6] Oracle Database 12^{c}. (2012, July). Security and Compliance. Retrieved from: http://www.oracle.com/technetwork/database/security/index.html. Last Accessed: 2/28/2014.

[7] M. Schumacher, E.B. Fernandez, D. Hybertson, F. Bushmann and P. Sommerland. (2006). Security Patterns: Integrating security and system engineering. West Sussex, England:Wiley.

[8] Google Cloud.(2012, October). Levels of access control. Retrieved from: https://developers.google.com/cloud-sql/docs/access-control. Last Accessed: 2/28/2014.

[9] F. Buschmann, R. Meunier, H. Rohnert, P. Sommerlad, M. Stal. (1996). *Pattern-Oriented Software Architecture: A System of Patterns*, vol. 1, Wiley.

[10] Oracle Corporation. (2012). Security in Private Database Clouds. Oracle White Paper. Retrieved from: http://www.oracle.com/technetwork/database/database-cloud/security-in-private-db-clouds-1733933.pdf

[11] CERT.(1988). Cybersecurity Engineering. Retrieved from: https://www.cert.org/about/.

[12] E. B. Fernandez.(2013). Security patterns in practice: Building secure architectures using software patterns., Wiley Series on Software Design Patterns.

[13] Ingrid. A. Buckley and Eduardo.B. Fernandez.(2011). Enumerating Software Failures to Build Dependable Distributed Applications. High-Assurance Systems Engineering (HASE), 2011 IEEE 13th International Symposium. 120 - 123. doi:10.1109/HASE.2011.35.

[14] I. Buckley and E.B.Fernandez, "Patterns Combing Reliability and Security", Procs. of the Third International Conferences on Pervasive Patterns and Applications, September 25-30, 2011, Rome, Italy.