INTERNATIONAL JOURNAL OF APPLIED RESEARCH AND TECHNOLOGY
ISSN 2519-5115
REVIEW ARTICLE

Security Risks in Online Distributed Database Systems

Dr. Govind Singh

FET, MGCGV, Chitrakoot
Satna(MP)

Corresponding author:
Dr.Govind Singh
eduinfoexpert@gmail.com

Received: December 17, 2016
Revised: December 25, 2016
Published: December 31, 2016

ABSTRACT

Maintaining data duality becomes an easier practice when using a DaaS because of the control provided by a single, managed interface to the data. The Data as a Service approach needs to be a consideration when analyzing the technical aspects of a Data Governance or Master Data Management program implementation. Business in these days of agile methodologies moves at a high velocity. Enterprises might not have the resources to fully manage the technical aspects of their data investment, like models and metadata. A DaaS interface can allow non-technical users to easily make minor structural changes to data or reports, quickly meeting business requirement changes

Keywords- Database System, Security and Cyber

INTRODUCTION

In recent years, the availability of databases and computer networks has promoted the development of a new field known as distributed databases. A distributed database is an integrated database which is built over a computer network instead of a single computer. The distributed databases offer several advantages to designers and users of databases. Among the most important is the transparency in accessing and locating information. However, the design and management of distributed databases faces major challenge that includes problems not found in centralized databases. There are two forces driving the evolution of database systems. On the one hand users as part of more complex organizations have demanded a number of capabilities that have been incorporated in database systems. An example of this is the need to integrate information from various sources. Technology has made it possible for some facilities initially imagined only in dreams come true. Online transaction that allows the current banking system would not have been possible without the development of communication equipment. Distributed computing systems are clear examples where organizational pressures combined with the availability of new technologies enable the realization of such applications.

In its simplest definition, distributed database systems pursue the integration of diverse and heterogeneous database systems. Its main goal is to provide the user with a global vision of the available information. This integration process does not involve the centralization of information, rather, with the help of computer networking technology available, the information is kept distributed and the systems of distributed databases allow access to it as if it were located in one place. The distribution of information allows, among other things, to have quick access to information, have copies of information for faster access and to have backup in case of failure.

Today's enterprises must support hundreds or even thousands of applications to meet growing business demands, but this growth is dramatically driving up the cost of running and managing the databases under those applications. The stress this puts on the IT budget makes it harder to provide databases to support new requirements such as Web 2.0 applications or other emerging collaboration solutions or even to support other uses such as increased application testing (Yuhanna, 2008).

Distributed Database as a Service

A new emerging option called database as a service (DaaS) hosts databases in the cloud and is a good alternative for some new applications. According to Forrester Research Study, some world known companies, such as Amazon, Google, IBM, Microsoft and Oracle are all targeting the DaaS market. Although most of today's DaaS solutions are very simple, in the next two to three years, more sophisticated offerings will evolve to support larger and more complex applications (Yuhanna, 2008).

Data outsourcing or database as a service has emerged as a new paradigm for distributed data management in which a third party service provider hosts a database and provides the associated software and hardware support.

The Database Service Provider

This new approach on distributed database technologies allows for the apparition of a new entity named "The Database Service Provider". Whose mission is to provide seamless mechanisms for organizations to create, store, and access their databases. Moreover, the entire responsibility of database management, i.e., database backup, administration, restoration, and database reorganization to reclaim space or to restore preferable arrangement of data, migration from one database version to the next without impacting availability will befall in such an organization. Users wishing to access data will now access it using the hardware and software at the service provider instead of their own organization's computing infrastructure. The application would not be impacted by outages due to software, hardware and networking changes or failures at the database service provider's site. This would alleviate the problem of purchasing, installing, maintaining and updating the software and administrating the system. Instead of doing these, the organization will only use the ready system maintained by the service provider for its database needs (Hakan, 2005).

The Database Service Provider provides data management for its customers, and thus obviates the need for the customer to purchase expensive hardware and software, deals with software upgrades, and hires professionals for administrative and maintenance tasks. However, as wonderful as it sounds, these new capabilities on distributed systems and data management technologies leads to the introduction of new challenges related to distributed database model. Among the most important:

1) Additional overhead of remote access to data,

2) Data privacy and security concerns, and

3) User interface design for such a service.

Security as a Main Concern

The distributed database has all of the security concerns of a single site database plus several additional problem areas. Some security threats involve: data tampering, eavesdropping and data theft, falsifying user identity, and administering too many passwords as well as others. Security can be provided for distributed databases by providing access control, user authentication, location transparency, and view transparency (Zubi, 2010).

With critical and sensitive amount of data being transferred across the network it is imperative that some form of security is implemented to secure the integrity and confidentiality of the system. General database security concerns must satisfy the following requirements: Physical integrity, which is the protection from data loss; Logical integrity, which is the protection of the logical structure of the database; Elemental integrity, which is ensuring accurate data; Easy Availability; Access control to some degree depending on the sensitivity of the data and user authentication to ensure that a user is who they say they are. The goal of these requirements is to guarantee that data stored in the distributed database system, is protected from unauthorized modification, and inaccurate updates (Coy, 2010).

Current Status of Cyber Attacks in India

According to the National Crime Records Bureau (NCRB), in 2013, 681 cybercrime related cases have been registered in Maharashtra, which has seen a 44.6 per cent rise in cybercrimes when compared to 2012. Andhra Pradesh with 635 cases registered in 2013 has also seen a 48 per cent rise when compared to 2012. Karnataka with 513 cases registered in 2013 has seen a 24.5 per cent rise when compared to 2012. Uttar Pradesh with 372 cases registered in 2013 is in the fourth place. It has seen a huge rise of 81.5 per cent in just one year. Kerala is in the 5th place with 349 cases registered in 2013. Among the bigger states Tamil Nadu and Bihar have very few cybercrime related cases. Just 54 cases have been registered in Tamil Nadu and just 23 cases have been registered in Bihar in 2013. Gujarat and Odisha have also registered just 61 and 63 cases respectively in 2013. Among the Union Territories, the national capital Delhi has registered 131 cybercrime related cases. It has seen a rise of 72.4 per cent when compared to 2012. As per the study, Andhra Pradesh, Karnataka and Maharashtra have occupied the top 3 positions when it comes to cybercrimes registered under the new IT Act in India. Interestingly, these three states together contribute more than 70 per cent to India's revenue from IT and IT related industries.

The ASSOCHAM report further said, mobile frauds are an area of concern for companies as well as 35-40% of financial transactions are done via mobile devices and this is expected and this is expected to grow to 55-60% by 2015, adds the study. Phishing attacks of online banking accounts or cloning of ATM/Debit cards are common occurrences. The increasing use of mobile/smartphones/tablets for online banking/financial transactions has also increased the vulnerabilities to a great extent. The maximum offenders came from the 18-30 age group, adds the report. These attacks have been observed to be originating from the cyber space of a number of countries including the US, Europe, Brazil, Turkey, china, Pakistan, Bangladesh, Algeria and the UAE, highlighted the ASSOCHAM-Mahindra SSG joint study.

Market Concerns: More Security, Optimization and Integrity

According to the National Science Foundation Project on DaaS, the following points are considered as a high priority on the subject:

1) The integration of data encryption with database systems to protect data against outside malicious attacks and to limit the liability of the service provider. However, encryption techniques have significant performance implications on query processing in databases.
2) The development of mathematical and statistical measures of Data Privacy for various privacy preserving schemes.
3) Development of techniques to protect the privacy of user data from the database service providers themselves. If the service providers themselves are not trusted, the protecting the privacy of users' data is much more challenging issue.

A service provider would need to implement sufficient security measures to guarantee data privacy. One key issue is how much privacy is enough. Any data privacy solution will have to utilize encryption which, as usual, comes with a certain cost in terms of database performance and additional hardware requirements. A fundamental question is whether encryption is too costly thus making the database service provider model infeasible (Mehtrotra, 2006).

Another approach regarding the security strength is the optimization of the

Query Process, which must able to perform efficiently over encrypted databases. New techniques changes the way we process queries over encrypted databases. Thus, optimization of these reformulated queries has to be carefully studied. The optimization process should ensure that the users of the system, the clients, can take full advantage of the capabilities promised by DaaS model (Hayes, 2008).

Other important element the demands attention is the database integrity. Once data encryption is employed as a solution to data privacy problem, it may generate integrity issues in this context. As a result of both malicious and non-malicious causes the integrity of the data may be compromised. When this happens, the client does not have any mechanism to detect the integrity of the original data. Therefore, new techniques have to be developed to provide clients mechanisms to check the integrity of their data hosted at the service provider side (Coy, 2010). An additional issue to address in the context of encrypted databases is key management. All encryption techniques rely on secure and efficient key management architectures. DaaS model puts additional complexity on key management architectures. Therefore, they demand new techniques for generation, registration, storage, and update of encryption keys (Reavies, 2010). Other emerging technologies that have evolved in some way from distributed databases are collaborative computing systems, distributed object management systems and the web. Much of the work on securing distributed databases can be applied to securing collaborative computing systems (Zubi, 2009).

A Market Survey for DaaS Adoption

In 2009, the Information Systems Audit and Control Association (ISACA) performed survey over 1,500 professionals across 50 countries, in order to measure the relative immaturity of DaaS over cloud computing usage and the uncertainty of the balance between risk and reward. This survey revealed that:

- 9.4% of respondents plan to use DaaS cloud computing for mission-critical IT services.
- 8.8 % will only use the cloud for low-risk, non-mission-critical IT services.
- 35.6% do not plan to use the cloud for any IT services.
- 28.2% were not aware of any plans for cloud computing.
- 12.1% would take large risks to maximize business return.
- 61% of reported that they believe the biggest risk to their organizations is failing to protect confidential data.

A similar study was appointed by Art Coviello, Executive Vice President of EMC Corporation. During a key note message of the RSA Conference 2010, he cited a recent survey conducted by CIO Magazine that stated 51% of IT chiefs in the USA, were unwilling to adopt DaaS or cloud computing because of security issues. The industry needs to deliver solutions that ensure levels of protection for databases in the cloud that would surpass what physical environments are providing today. Security needs to be embedded in the virtual layer and practitioners need to shift from safeguarding the enterprise architecture to adopting a posture of information-centric protection (Coviello, 2010).

Another survey conducted by IEEE/CSA in 2010, revealed that IT professionals are concerned and recognize the importance and urgency of DaaS security standards.

- 44% responded that are already involved in cloud computing projects but project that not involve corporative data stored in the cloud.
- 93% considered the need for cloud computing security standards as important.
- 82% percent said the need is urgent. Data privacy, security and encryption comprise the most urgent area of need for standards development.

Distribute databases on its DaaS flavor is still a young technology. It runs on the cloud and by consuming cloud services is important to recognize the dangers and potential risks facing us, as with any new or existing IT investment. The security concerns, questions about the maturity of the supplier in an industry in its infancy, reliability, and regulatory issues are topics that are of the concern of those professional making decisions regarding the adoption of this new technology. It's clear from the findings on the mentioned surveys that enterprises across sectors are eager to adopt database services over cloud computing, but security standards are needed both to accelerate cloud adoption on a wide scale and to respond to regulatory drivers (Smith, 2010). The absence of a security compliance environment is having impact on the adoption on database services over cloud computing. Distributed database systems are a reality, and more over are here to stay. Many organizations are now deploying distributed database systems. Therefore, we have no choice but to ensure that these systems operate in a secure environment. There is still a long road to travel; efforts are being done. The overall issue, aside from the database itself is to ensure that the databases, operating systems, applications, network, web technologies and clients are not only secure, but are also securely integrated (Zubi, 2010).

CONCLUSION

A wide variety of pricing models exist to support DaaS platform offerings for both private and commercially available data. These models are relevant whether a firm is a consumer of DaaS or one who provides data to others through a service. Tiered access to data appears to be a popular component for Data as a Service pricing models. The tiers fall in to two major categories: volume-based pricing and data type pricing. Volume-based pricing normally includes options for both pay by each instance of data access as well pay by the quantity of data consumed. A lower-tier pay by the instance option is generally a better choice for companies with smaller data needs. Pay by quantity allows for a certain volume of data per day, with overage charges coming into play if that daily limit is exceeded. Higher tiers with unlimited data options are also available. The data type pricing model features tiers essentially based on the number of fields returned in a query. DaaS offering would charge more for business data that included a company's location data, a list of officers and historical stock prices versus one that only provided the location data.

REFERENCES

Coy, .S. (2010) Implications of the Choice of Distributed Database Systems.In Proceedings IEEE Symposium on Research in Security and Privacy, pp. 260-272.

Reavies, J. (2010). Regulatory requirements demand security standards compliance. In Survey By IEEE and Cloud Security Alliance Details Importance And Urgency Of Cloud Computing Security

Standards.IEEE Press Release. IEEE Computer Society Press. pp. 29-30.

Zubi, S. (2010). On Distributed Database Security Aspects..ICMCS '09 International Conference on Multimedia Computing and Systems, 2009.

Coviello, A. (2010). Securing the Path to Virtualization and the Private Cloud from the Desktop to the Datacenter. In Proceedings of RSA 2010 Security Decoded Conference .International Conference on Computer Security. EMC-RSA, Inc. Boston, MA, 34-35.

Smith, B. (2010). Building Confidence in the Cloud. In A Proposal for Industry and Government Action for Europe to Reap the Benefits of Cloud Computing. International Conference on EU Digital Market. Microsoft Press. Seattle, WA, 11-20.

Hayes, B. (2008). The LDV Secure Relational DBMS Model. Communications of the ACM, pp. 9–11

Yuhanna, .N. (2008). Database-As-A-Service Explodes On The Scene. Forrester Research.

Hakan, .H. (2005).Providing Database as a Service.ACM Transactions on Database Systems. pp. 25-29.

Mehtrotra, .S. (2005).Encryption in relational database management systems.In Proc. Fourteenth Annual IFIP Working Conference on Databa Security. pp. 105-109