Volume 4, Issue 6, June 2014 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Approach to Secure Data across Different Networks

Simran Syal*
CSE & CGC Group of Colleges
India

Dr. Mandeep Singh
CSE & Chandigarh University
India

Abstract- With data becoming an increasingly bulky as well as valuable, today's IT organizations need the efficient tools to store, manage, and move the information in most reliable and cost-efficient manner where security is also a key concern. An algorithm is proposed to secure data across different networks.

Keywords- Data security, Data migration, Information security, Server Attack, Data Repository.

I. INTRODUCTION

With the advancement and development of information technology, old system has been replaced or updated by more powerful system. During the process of updating [1], data migration is significant issue. Data security is also considered to be an important issue. In recent years, [2] data security research has been actively conducted through access control or data loss protection, etc. Data security and access control has a lot in common with information security. The information security has become more difficult due to largely increasing data volume that is why cost of GB has decreased but security investment for data has increased.

II. DATA MIGRATION SECURITY CHALLENGE

Some security concerns related to data migration are:

- Sometimes computing resources are shared with other organizations those have no knowledge and control about where to run the resources which may cause the loss of security.
- Sometimes the user may move data to the storage service which is incompatible and this may also result in the loss of security.
- Sometimes it becomes complicated to preserve the consistency of security because of the dynamic nature of the virtual machines.

For secure data access and transfer, confidentiality must be achieved. And it can be achieved by using cryptographic protocols. There is a need for securing [3] data migration process because if data migration is not done properly and systematically, it can give rise to problems concerning security of company's assets that primarily comprise of data.

III. MIGRATION TECHNIQUES

Various migration techniques known are:

A. Stop and Copy:

This is the simplest approach for migrating data from source to destination. One limitation of this approach is it results in long downtimes and the other is high post migration overhead. Though being a safe migration technique, it is not a suitable technique for migration due to the disruption caused in service during migration.

B. On demand migration:

In this technique, data is not migrated immediately, but on demand due to which it results in reducing service irruption and thus becomes an effective technique. This technique has high post migration overhead and it also requires expensive synchronization between source and destination servers.

IV. FACTORS EFFECTING THE COST OF MIGRATION

Data migration should be inexpensive and cost effective. The ultimate goal should not only depend on the throughput and latency of operations but also on optimizing the operating cost.

A. Service Interruption during migration:

Service interruption or downtime is one factor that contributes to the cost of migration. The overall system unavailability is referred as downtime whereas the aborted transaction of user whose data is being migrated is referred as service interruption.

B. Migration Overhead:

Data Migration should have low overhead in order to minimize the effect of migration. In order to facilitate migration, the additional work done and the corresponding impact is referred as overhead. Overhead can be before

migration or after migration as well as during migration. To facilitate migration, the overhead occurred during normal operation is overhead before migration. The overhead occurred on the system while the data is being migrated is overhead during migration. The overhead on execution after the migration of data has been completed is overhead after migration.

V. RELATED WORK

An influential tool is designed that enables high performance data migration in a broad variety of storage environments. This migration tool will facilitate migration of data from MS Access to SQLServer and Oracle. The existing database will be taken by the system from the user that is in one format which is converted to a database which is in the other format that is specified by the user. Here data migration is the process of transforming, cleaning and loading the data into the new system. Usually, a Database Migration Suite is developed for organizations and consumers to save time for converting to a new database. But this tool provides flexibility to client, without any manual interference, to migrate his existing database into different database. [1]

The security hardening methodology is projected in which attributes relation graph is used. An effective security method is more vital than the entire security method for big data because big data have large size and it needs too much security investment. Due to large amount of data, management of data and its security is more difficult than the current information. So the aim is to protect the significance through the analysis of the data rather than the data itself. [2] As clients seem to shift their data and applications to the cloud, security is the question most constantly raised. An approach associated to the security is carried out in migration process of legacy systems with the aim to find the concerns, requirements, aspects and benefits of the security. Privacy and security concerns still remain a main obstacle to common acceptance, although industry leaders and consumers have extensive hope for cloud computing. [3]

The continuous accessibility of services is a key concern for Internet-based service providers. To deal with outages, a context-aware approach is used for data center migration across WANs. To facilitate the replication and migration of server functions, server virtualization technology is used. The designs make use of the existing server virtualization technologies and propose network and storage mechanisms to facilitate migration across WAN. A migration management system, manages the migration across subsystems involved, such as the server platforms, the wide area network and the disk storage system. The design of a framework that will allow the immigration of all subsystems across a WAN is the main involvement. [4]

A migration technique is designed for the cloud in a database system is proposed. The various database multitenancy models are evaluated and proposed a proficient technique with least downtime and impact on performance for live migration of tenant's database. Multitenancy [5] is a method to combine multiple customer applications in one operational system. It is often used to prevent the need for different systems for each tenant. Multitenant DBMS serves thousands of tenants by collocating multiple tenant databases at identical machine. Database multitenancy allows effective resource sharing for customer applications that have small but varying resource requirements [7][8].

A database migration scheduling method is proposed which is suitable for heterogeneous WANs. Dynamic database relocation using DB-Migration can be used for several purposes, including transaction processing [9][10]. Every database is fixed in a conventional distributed database and through a number of operation request messages a distinctive database operation is performed. The way to resolve an agenda of DB-migration for a given access sequence is shown, which gives small communication time for database operations. For every database, an agenda should be independently determined due to the characteristics of WAN which make it hard to manage DB-migrations in the granularity of the transactions [6].

VI. METHODOLOGY

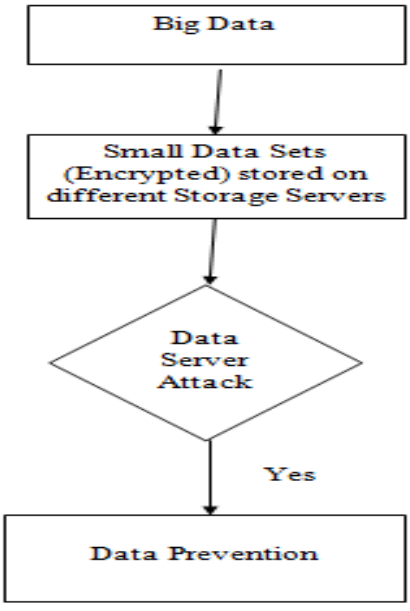

Fig. 1 Flow chart of method to secure data.

A. *Large Data:*

Large amount of data in the order of petabyte coming out from one or more source.

B. *Small Data Sets:*

Data is manipulated from large data and it is then segregated into smaller data sets which can be later on encrypted and stored on different servers linked together to form some meaningful source. It can be represented as below.

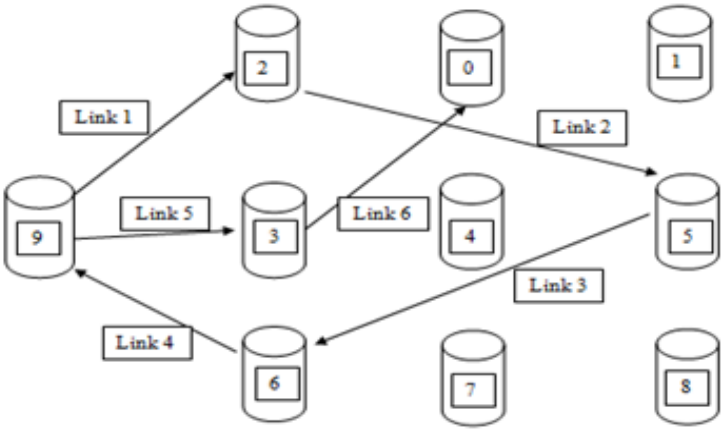

Fig. 2 Linking of data on different servers to form a meaningful Dataset.

C. *Data Server Attack:*

Possibility is there when hackers can hack into some organization's data server to sneak into some of their important data resources. We must prevent this from happening.

D. *Data Prevention:*

Idea is to implement an algorithm which can detect any malicious activity going on with the server's login and hence upon detection, it will replicate its data to some other server on some other place and delete all the data from itself. In this way, important data will be held private by the firm. Moreover, the data can be brought back when triggered by the authenticated administrator after required interval of time set by company policy (a feature provided by the algorithm developed).

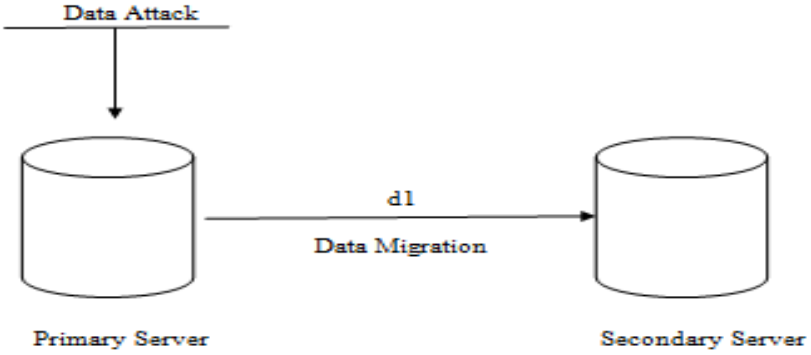

Fig. 3 Pictorial representation of data migration.

VII. ALGORITHMIC PERSPECTIVE

To implement an efficient algorithm to secure large scale data stored across different networks (storage servers) is the basic concern.

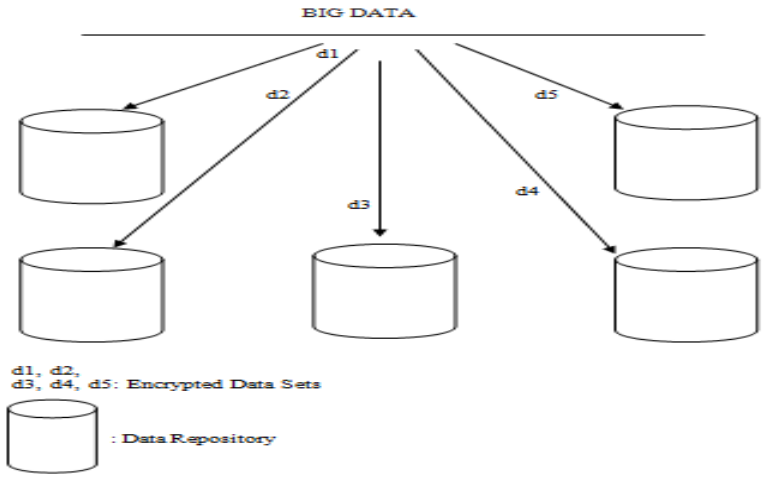

Fig. 4 Distribution of Big Data across various networks.

By chunking the large data across different networks after filtering out the raw data makes it possible for us to enhance our storage capability and hence the data reachability by storing it to servers where it is most needed. However, there is significant chance that our important data might be sniffed in by unwanted people which we don't want to. We come across such situations when we come to know that many social sites are hacked. Many profiles contain private data which could prove to be heinous if hacked. Consider the situation of facebook profiles hacked. We would not want it to happen but we come across such situations when we hear that many facebook profiles were hacked or consider in case of NetBanking each of which deals with large data everyday.

Our objective is to reduce such kinds of activities so that we can protect ourselves from cybercrime and retain our valuable data.

VIII. CONCLUSION

Data Prevention has become to be of utmost concern for the IT industry, therefore this approach of securing risky data would be much feasible and more secure. Many of the financial firms and other social sites actively use various encryption algorithms but then also the data is hacked by unwanted sources. In the approach presented in the paper, first of all, even if the hacker breaks into the server and gets the data, encrypts it, then also the data would be vague for him/her since the associated meaningful data set is distributed across many servers in encrypted format. By the time even if the hacker figures out the distribution of data set, the data would have already migrated to some other server and the server will hold a lock file and could not be accessed by any operator other than administrator who reboots it manually at the physical site.

REFERENCES

[1] Shinde Anita Vitthal, Thite Vaishali Baban, Roshni Warade, and Krupali Chaudhari, "Data Migration System in Heterogeneous Database," *IJESIT*, vol. 2, pp. 88-92, March 2013.

[2] Sung-Hwan Kim, Jung-Ho Eom, and Tai-Myoung Chung, "Big data Security Hardening Methodology using Attributes Relationship," *IEEE*, Aug. 2013.

[3] Virendra Singh Kushwah, and Aradhana Saxena, "A Security Approach for Data Migration in Cloud Computing," *IJSRP*, vol. 3, pp. 1-8, May 2013.

[4] K.K. Ramakrishnan, Prashant Shenoy, and Jacobus Van der Merwe, "Live Data Center Migration across WANs: A Robust Cooperative Context Aware Approach," AT & T Labs-Research, University of Massachusetts.

[5] Sudipto Das, Shoji Nishimura, Divyakant Agrawal, and Amr El Abbadi, "Live Database Migration for Elasticity in a Multitenant Database for Cloud Platforms," University of California, NEC Corporation, UCSB Computer Science Tech. Rep. 1-14, 2010.

[6] Takahiro Hara, Masahiko Tsukamoto, and Shojiro Nishio, "A Scheduling Method of Database Migration for WAN Environments," Research work, Osaka University, Japan.

[7] S. Aulbach, T. Grust, D. Jacobs, A. Kemper, and J. Rittinger, "Mulyi-tenant Databases for Software as a Service," *SIGMOD*, pp. 1195-1206, 2008.

[8] D. Jacobs, and S. Aulbach, "Ruminations on Multi-tenant Databases," *BTW*, pp. 514-521, 2007.

[9] T. Hara, K. Harumoto, M. Tsukamoto, and S. Nishio, "Database Migration: A New Architecture for Transaction Processing in Broadband Networks," *IEEE Transactions on Knowledge and Data Engineering*, vol. 10, pp. 839-854, Oct. 1998.

[10] T. Hara, K. Harumoto, M. Tsukamoto, and S. Nishio, "DB-MAN: A Distributed Database System Based on Database Migration in ATM Networks," in *Proc. ICDE'98*, 1998, p. 522-531.

