Jurnal Teknologi

Full paper

Privacy Issues and Protection in Secure Data Outsourcing

Touraj Khodadadi*, A. K. M. Muzahidul Islam, Sabariah Baharun, Shozo Komaki

Malaysia-Japan International Institute of Technology (MJIIT), Universiti Teknologi Malaysia, 54100, Kuala Lumpur, Malaysia

*Corresponding author: ktouraj2@live.utm.my

Article history

Received :1 January 2014
Received in revised form :
15 February 2014
Accepted :18 March 2014

Abstract

Utilizing database encryption to safeguard data in several conditions where access control is not sufficient is unavoidable. Database encryption offers an extra layer of security to traditional access control methods. It stops users that are unauthorized, such as hackers breaking into a system, and observing private data. Consequently, data is safe even when the database is stolen or attacked. Nevertheless, the process of data decryption and encryption causes degradation in the database performance. In conditions where the entire information is kept in an encrypted format, it is not possible to choose the database content any longer. The data must be first decrypted, and as such, the unwilling and forced tradeoff occurs between the function and the security. The suitable methods to improve the function are techniques that directly deal with the data that is encrypted without having to decrypt them first. In this study, we determined privacy protection and issues that each organization should consider when it decides to outsource own data.

Keywords: Data owner; privacy; DbaaS; database security; encrypted database

1.0 INTRODUCTION

In today's business world, client's information is one of the most crucial resources for companies. The present marketing database contains information that is vital for all parts of the organization such as sales, marketing, customer support, product development and finance[1]. Even though this information is important for organizations, most of them choose to outsource the maintenance process of this crucial resource. Companies outsource data maintenance to other external providers for several valid reasons, which include taking advantage of the provider's expertise and experience, move the technical risk complexity to the provider, and so that, they are free from other disruptions and would be able to pay attention to their primary proficiency, that is marketing [2].

The present network based information control solutions make it more critical to identify and prevent defective actions. In fact, new data control solutions should provide guaranteed solutions without any harmful activities. This is important especially when customers leave information control with specialized service agency [3]. With today's use of cloud computing, all sources and programs are provided as a support over the Internet [1]. In this case since the data is the most essential situation in a business resource, data management support is an essential part.

Nevertheless, a new growing option in this area is shown by Database as a Service or the DbaaS framework. According to this model, information owner handles the DBMS and responses to a person's questions straight, rather than using the conventional client-server structure. One of the most serious challenges to the frequent utilization of DbaaS is associated to protection problems [4]. However, in this new model, protection concepts like privacy, authenticity, integrity, and confidentiality can be ensured. This study tries to point out the main security problems for protected data outsourcing model and particularly concentrates on several critical information and privacy security specifications.

2.0 DATABASE AS A SERVICE PARADIGM

The DbaaS design information and application are saved together in the exterior server that takes full liability of their control. In this model, however, service accessibility may enhance using the exterior server, but data ownership control of the information decreases. Actually, in data outsourcing model, several new security problems such as privacy are prevalent [5].

In this data outsourcing model, users and information owners trust that the exterior server is reliable and maintains outsourced information reliability. In fact, this server warrantees that the accessibility to outsourced information is available to the clients whenever they asked for it. Nevertheless, privacy of the data source content is a problem. While outsourced information may be made of vital information, that information owner wants to safeguard them against illegal parties. Therefore, preventing exterior servers from making illegal accesses to the contracted information is an important requirement in DbaaS model.

3.0 SECURITY PRINCIPLES

Data security can be basically categorized into three main ideas: privacy which implies preventing details from frequent accessibility (reading, knowing about, and browsing) by

unapproved parties; reliability, which implies, preventing details about illegal or non-suitable access (writing, modifying, removing, and modifying status), and accessibility, which implies, safeguarding details from illegally accessed or even, recovery of details from any errors that may cause them to be available [6].

To cope with these critical features, many of the DBMSs contain tools that offer private security services. Access control is software that controls the overall security service including all accessibility requests according to several mentioned functions that give rise to three positions namely partial, total, and denied accessibility. Thus, the accessibility management's major objective is to provide confidentiality and integrity. The accessibility management process demonstrated the resources and accessibility modes given to each user.

■4.0 PRIVACY

Various resources demonstrate a variety of definitions on the matter of privacy. Some of the definitions refer to privacy to having confidentially and others point out the differences between these two terms. In fact, privacy is linked to the rights of an individual to the level of personal information, how and when it can be revealed to others [7]. In addition, privacy refers to having authority (storage, communication, access, collection, constitution, and manipulation) over one's data. This goes to show that privacy is in fact a wider concept compared to confidentiality. Therefore, in the prevention of privacy is built upon having access management tools that guarantee privacy, several matters like the reason for utilizing the data should be highlighted. For the user, in fact the data should only be used for the purpose of authorization that it was initially indicated for.

4.1 Privacy Issues

There are several concerns when it comes to privacy where all companies considers when deciding to outsource their own data. Each company should qualify these matters when selecting the data owner.

Firstly, the method and reason for collection of data must be controlled by the data owner. However, data should not be collected unless it is for an authorized reason that is related directly to the activity of the data owner, and the data collection is a main requirement for or directly related to that reason. A data owner must not conduct data collection through unfair or illegal methods.

Secondly, data should be requested from the concerned individual. In general, when the data owner solicits data from the concerned individual, it should be ensured that the individual concerned is aware of the data collection purpose.

Thirdly, the data owner should be ensured that the data are collected for the authorized purpose. For instance, it must be ensured that data collection is current and associated to the original purpose. The data owner must also ensure that the collection of data does not impose on any unacceptable level of the individual's private concerns.

Fourthly, the data owner should ensure that the data is kept safe with several security measures against unauthorized accessibility, use, loss, disclosure or modification, and any other misuse. If required, the data should be made available to the individual and reasonable measures are taken to ensure authorized use only, and disclosures are made only to the authorized person.

Fifthly, the data under the control of the data owner, can be accessed for authorized reasons even to the individual and the individual can be denied access is necessary. These scope should be defined under the security policy.

Sixthly, the data owner should ensure several tools are available to make suitable changes to make sure that the data is accurate. In addition, the purpose the data was collected should be considered and ensure that the data is utilized accordingly. Seventhly, the data owner should be careful about using the data for the specified reason and consent of the individual is required if it is used any other purposes.

Lastly, the data owner is not allowed to share the data with a third party unless person has been granted and the individual is aware of this arrangement. A note should be added in the disclosure policy if the data owner would release data if required by law or by enforcement agencies for criminal investigations. The third party in this instance should also ensure that the data is not shared with any other agency, or person.

■5.0 PRIVACY PROTECTION of DbaaS

Database management systems are a core area in data management and have a critical function in web communications and day-to-day operations of companies. Nowadays, with the extended usage of applications and web functions, the risk of online attacks and misuses are much more prevalent. It is a fundamental requirement of a company to store and ensure secure data both in external and internal communications. Attacks and data destruction does not only affect one individual or application but will have a drastic effect on the entire company [8].

Access control tools and backup are utilized to safeguard the database systems. Backups safeguard the data against natural disasters like earthquakes, floods, disk failures, fire, and database access control tools safeguard against access that is unauthorized. Different strategies and frameworks have been suggested in terms of database access control [9, 10]. Nevertheless, access control is only possible when the attacker tries to enter the database using the key interfaces. Access control does not stop unusual data access. For instance, when the media that have the databases are stolen or when the database managers want to access the sensitive data, access control will not stop disclosure of the sensitive data. In these instances, other techniques must be utilized for safety measures.

This case, the data encryption method can be used to prevent disclosure of information in the database. This method is in fact, complementary to the access control method. Given these situations, techniques should be utilized in databases to keep and offer secure accessibility to information in databases. It is impossible to disclose encrypted data, even when the database servers are at risk. With stored encrypted data on the server, the attacker can only have access to raw data and not thee information kept in it. In addition, encryption allows the database managers to conduct administrative works without causing danger to the user's data [10, 11].

Utilizing cryptography for this reason causes new challenges. One of the challenges is executing user query on the encrypted data. Database management system cannot query the encrypted databases like how it is done with raw plaintext database. This problem is managed in two ways: the first option would be to decode all the data when executing the queries. However, to decode the data for each query will reduce the speed and performance of the total system. Techniques are suggested for lowering the number of decryptions and then improve the query execution speed, but in several applications, data encryption is carried out because there is insufficient confidence in the database server. Therefore, putting the decryption key in the database server would mean to neglect the main objective, which is encryption. In these types of applications, the server cannot decrypt the data. The other solution is to search the encrypted data

without having to decode it. This technique can lower the costs required for encryption and decryption and enhance the efficiency of the system [12, 13].

When it comes to developing a technique for looking for the encrypted data, an essential objective that should be taken into consideration is to reduce the computation required on the user's end (a decoding key holder) and lowering the communication expenses. The techniques must be developed so that a large amount of processes can be conducted on the servers[14]. The organizations and individuals need techniques to find on the encrypted data of similar quality with the decrypted version. It suggests that if possible the search records should have a specific value, with a logarithmic level of the size of database. Furthermore, it is possible for the data to be inclusive of decrypted and encrypted data. The access performance of decrypted data should not be lowered due to the encrypted data [8]. Providing these techniques is difficult. Offering this feature may put the information security at risk.

There exist some techniques for finding the encrypted data without having to decrypt them. Nevertheless, these techniques cannot be applied in the database that is encrypted. Most of them are used for finding a word in the encrypted files. Techniques that are provided for the database that is encrypted should offer the requirement of this environment for operations and searching.

The search techniques for encrypted database based on the applicable data types can be categorized into two classifications: procedures and techniques that are applicable to the numerical and string data [4, 7, 15].

The situations that require the data string, are normally applied to equality (=) and pattern matching (LIKE) and these situations in the numerical data are range matching and equality (<. >, =). Therefore, it appears logical that various techniques are used for each one.

Many present techniques used for searching the encrypted database are only able to run based on equality of encrypted numeric and string data. A secure and effective method for searching for patterns that are arbitrary in the encrypted string data and search range matching in the encrypted numeric data is yet to be implemented.

6.0 CONCLUSION

Database outsourcing is highly regarded because of reducing organization costs in data management and also introducing data management and maintenance services. The problem is providing security issues for outsourced data. Actually, outsourcing gives data control to the unreliable server. One way for providing security in data outsourcing paradigm is use of encryption, which has its own problems such as how to run the query on encrypted data. There are several methods for performing queries on the encrypted data that all of them are not able to fully meet the requirements of this environment.

Acknowledgement

This work is partially supported by MJIIT Research Grant, with Vote No. 4J044 of Universiti Teknologi Malaysia (UTM) Year 2012-2014, under Ministry of Higher Education (MoHE).

References

[1] M. Alizadeh, W. H. Hassan, N. Behboodian, and S. Karamizadeh. 2013. A Brief Review of Mobile Cloud Computing Opportunities. *Research Notes in Information Science (RNIS)*. 12: 155–160.

[2] S. De Capitani di Vimercati, S. Foresti, S. Jajodia, S. Paraboschi, G. Pelosi, and P. Samarati. 2008. Preserving Confidentiality of Security Policies in Data Outsourcing. In *Proceedings of the 7th ACM workshop on Privacy in the electronic society*. 75–84.

[3] E. Bertino and R. Sandhu. 2005. Database Security-concepts, Approaches, and Challenges. *Dependable and Secure Computing, IEEE Transactions on*. 2: 2–19.

[4] B. T Ograph and Y. R. Morgens. 2008. Cloud Computing. *Communications of the ACM*. 51.

[5] S. D. C. Di Vimercati, S. Foresti, S. Jajodia, S. Paraboschi, and P. Samarati. 2007. A Data Outsourcing Architecture Combining Cryptography and Access Control. In *Proceedings of the 2007 ACM workshop on Computer Security Architecture*. 63–69.

[6] S. Castano, M. G. Fugini, G. Martella, and P. Samarati. 1995. *Database Security*. ACM Press Books, Wokingham, England: Addison-Wesley,| c1995. 1.

[7] C. Wang, Q. Wang, K. Ren, and W. Lou. 2010. Privacy-preserving Public Auditing For Data Storage Security In Cloud Computing. In *INFOCOM, 2010 Proceedings IEEE*. 1–9.

[8] J. He and M. Wang. 2001. Cryptography and Relational Database Management Systems. In *Database Engineering and Applications, 2001 International Symposium on*. 273–284.

[9] S. Abolfazli, Z. Sanaei, M. Alizadeh, A. Gani, and F. Xia. 2014. An Experimental Analysis on Cloud-based Mobile Augmentation in Mobile Cloud Computing. *IEEE Transactions on Consumer Electronics*. 60.

[10] M. Alizadeh, W. H. Hassan, M. Zamani, S. Karamizadeh, and E. Ghazizadeh. 2013. Implementation and Evaluation of Lightweight Encryption Algorithms Suitable for RFID. *Journal of Next Generation Information Technology*. 4: 65–77.

[11] M. Alizadeh, W. H. Hassan, M. Zamani, and T. Khodadadi. 2013. A Prospective Study of Mobile Cloud Computing. *International Journal of Advancements in Computing Technology (IJACT)*. 5: 198–209.

[12] M. Alizadeh and W. H. Hassan. 2013. Challenges and Opportunities of Mobile Cloud Computing. In *Wireless Communications and Mobile Computing Conference (IWCMC), 2013 9th International*. 660–666.

[13] M. Alizadeh, M. Salleh, M. Zamani, S. Jafar, and K. Sasan. Security and Performance Evaluation of Lightweight Cryptographic Algorithms in RFID. Kos Island, Greece.

[14] J. Brodkin, 2008. Gartner: Seven Cloud-Computing Security Risks. *Infoworld*. 1–3.

[15] E. Ghazizadeh, M. Zamani, J.-l. Ab Manan, and M. Alizadeh. 2014. Trusted Computing Strengthens Cloud Authentication. *The Scientific World Journal*. 17.