CLOUD QUERY PROCESSING ANALYSIS: ENCRYPTION AND DECRYPTION

Zainalabideen Ali
Faculty of Information Science and Technology, National University of Malaysia, Malaysia.
E-mail: gp06356@siswa.ukm.edu.my

Azana Hafizah Binti Mohd Aman
Faculty of Information Science and Technology, National University of Malaysia, Malaysia.
E-mail: azana@ukm.edu.my

Rosilah Hassan
Associate Professor, Faculty of Information Science and Technology, National University of Malaysia. Selangor, Malaysia.
E-mail: rosilah@ukm.edu.my

Recepción: 26/07/2019 **Aceptación:** 18/09/2019 **Publicación:** 06/11/2019

Citación sugerida:
Ali, Z., Aman, A.H.B.M. y Hassan, R. (2019). Cloud query processing analysis: encryption and decryption. *3C Tecnología. Glosas de innovación aplicadas a la pyme. Edición Especial, Noviembre 2019*, 65-75. doi: http://dx.doi.org/10.17993/3ctecno.2019.specialissue3.65-75

Suggested citation:
Ali, Z., Aman, A.H.B.M. & Hassan, R. (2019). Cloud query processing analysis: encryption and decryption. *3C Tecnología. Glosas de innovación aplicadas a la pyme. Special Issue, November 2019*, 65-75. doi: http://dx.doi.org/10.17993/3ctecno.2019.specialissue3.65-75

ABSTRACT

The usage of clouds to provide data query services is becoming an attractive solution to services that demand scalability and cost minimization. Despite the huge advantages, cloud consumers require their confidential or delicate data to be safe and secured, because violating their private data would be a great concern that is not tolerable. Therefore, corporations who use the cloud services especially the database-as-a-service have tended to encrypt sensitive data for security and confidentiality purpose. Encrypting data would facilitate protecting private information from any violation by the service provider. Several studies have proposed AES and RSA encryption methods. Yet, each encryption method provides a specific level of security which comes with an opposite level of efficiency. Therefore, this work will examine the performance for both encryption methods. The environment setup consists of Microsoft SQL Server as cloud database simulation, and a Visual Studio platform to simulate the local processing of queries. The performance evaluation parameters are time consumption for encryption and decryption. Overall, the results appeared are not significant as each method has its own benefits.

KEYWORDS

RSA, AES, Processing Time, Cloud Query Processing.

DOI: http://dx.doi.org/10.17993/3ctecno.2019.specialissue3.65-75

1. INTRODUCTION

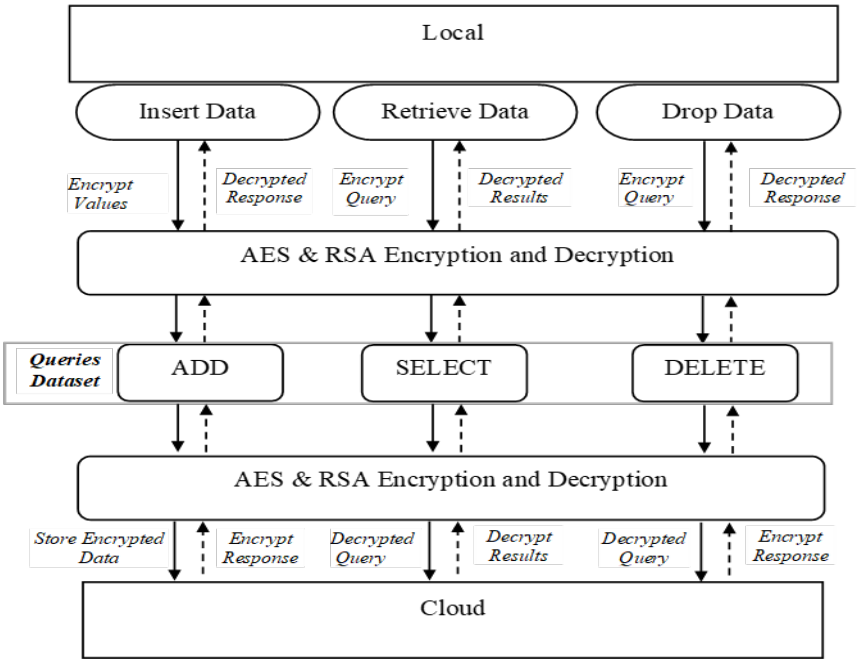
Cloud computing is a term that was introduced in 2006 after the introduction of Amazon's Elastic Compute Cloud (EC2) (Singh, 2015) defined a cloud computing model as a model that facilitates easy and on-demand network access to a shared pool of configurable computing services and resources. These resources include networks (Aman, 2019), servers, storage, apps, and services. Modak, Chaudhary, Paygude, and Ldate (2018) noted that there are three components of cloud computing, which are data centers, the client computer, and distributed servers. A company that intends to create a database would prefer to rent an existing one provided by the cloud rather than initiating it from scratch, where there is a third party that can manage and controls these services (i.e. a virtual world) (Singh, Rishiwal, & Kumar, 2018).

Despite cloud computing has huge advantages. Cloud consumers do not wish to place their confidential or delicate data, such as health records (Ibrahim, 2019), emails, and govern-mental important files; because violating their private data would be a great concern that is not tolerable. Encrypting data would facilitate protecting private information from any violation by the service provider (Vurukonda & Rao, 2016). The daily usage of query processing over an encrypted data would require a long time where the query needs to be encrypted, and the retrieved data will be decrypted to be shown for the employees. Apparently, the efficiency would be significantly impacted. Recent efforts in the cloud query processing have shown some attempts to improve the efficiency of processing encrypted queries (Amini, 2018). However, there are still some concerns regarding the privacy in which the encryption type would be examined (Albadri & Sulaiman, 2016; Ghaleb, Shukur, Sulaiman, & Mobidin, 2018).

This paper consists of four (4) sections. Section I introduces an overview of cloud computing, Section II methods of evaluation. Section III presents the results and discussion. Lastly, section V concludes the paper with a summary of the findings and recommended future work.

2. RESEARCH METHODOLOGY

The aim objective of this paper is to analyze the performance of two encryption methods namely: RSA and AES. SQL Server is used as a cloud database simulation and have been simulated the local processing of queries by using a Visual Studio platform. As shown in Graphic 1, the architecture of the proposed method contains three key components namely the local side, Encryption and Decryption methods (AES and RSA), and the cloud side. The queries include three types which are Insert data, retrieve data, and drop data.



Graphic 1. Model of The Proposed Method.

The dataset is stored in Microsoft SQL Server Management Studio, for the experiments, a set of queries is prepared. This set contains three types of queries including 'Add', 'Delete' and 'Select'. Each type of query gives different results from where security and time consumption for each method. Each type of query is run 50 times with different data. The database name is Student with two tables represents

DOI: http://dx.doi.org/10.17993/3ctecno.2019.specialissue3.65-75

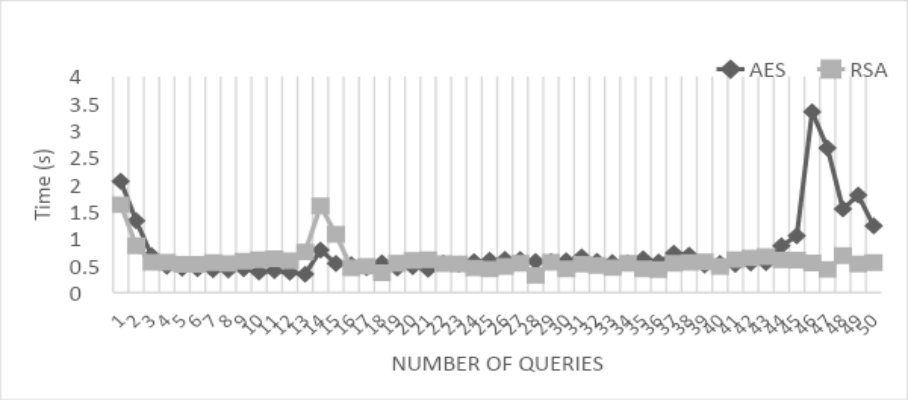
RSA and AES table. The data type is using the non-variable character (nvarchar), since using nvarchar rather than varchar, avoid encoding conversions which consume time every time it reads from or writes to the database. Conversions take time and are prone to errors. The nvarchar size is depending on the key length for each method, 200 for AES and 2000 for RSA.

The computer which has been utilized having intel core i7-7500U CPU @2.70GHz 2.90GHz processor with 8GB RAM, system type 64-bit, Windows 10 Pro and computer type is LENOVO Ideapad 310. The AES has been implemented using a C# library called AesManaged, while the RSA has been implemented a C# library called RSACryptoServiceProvider. The interface of the proposed method enables the user to type a query from the predefined ones. Then, either by using AES or RSA encryption methods the interface will encrypt the query and attempt to execute it, meanwhile, decrypt the retrieved results to present it to the user. With regards the encryption and decryption, for RSA, the asymmetric key was 2048-bit key, while for AES, symmetric key generation using the 128-bit key.

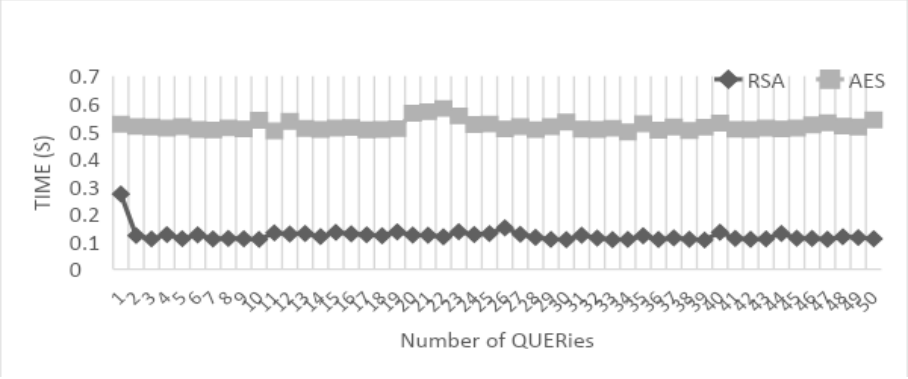
3. RESULTS AND DISCUSSION

The results of applying the encryption time including AES encryption method, and RSA encryption method. Graphic 2, Graphic 3 and Graphic 4 shows the encryption is being performed for 'Add', 'Select', and 'Delete' queries respectively.

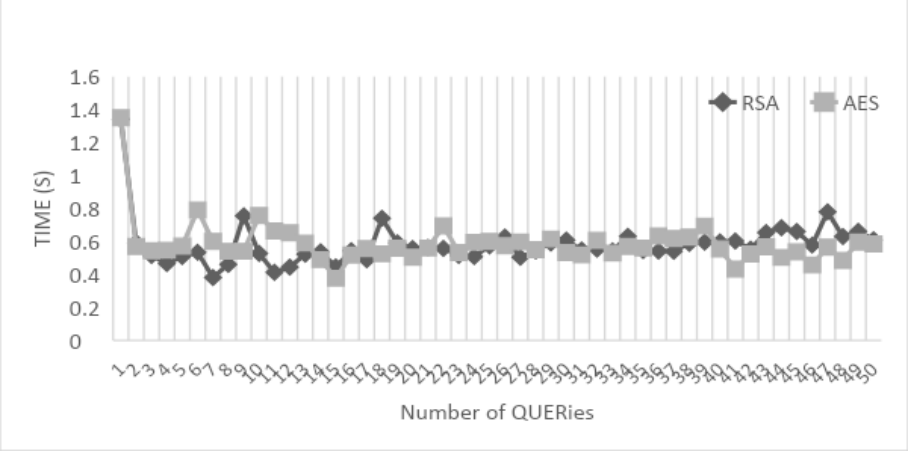
While the results of applying the dencryption time for AES and RSA method is shown in Graphic 5, Graphic 6 and Graphic 7 being performed for 'Add', 'Select', and 'Delete' queries respectively.



Graphic 2. Encryption Time for Add.

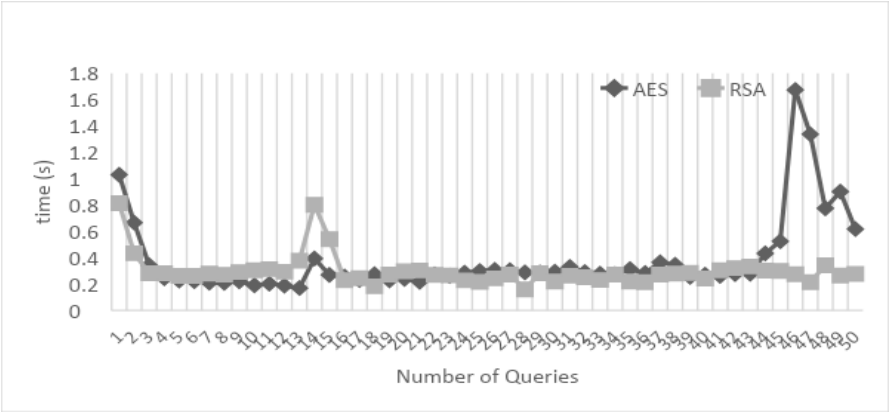


Graphic 3. Encryption Time for Select.

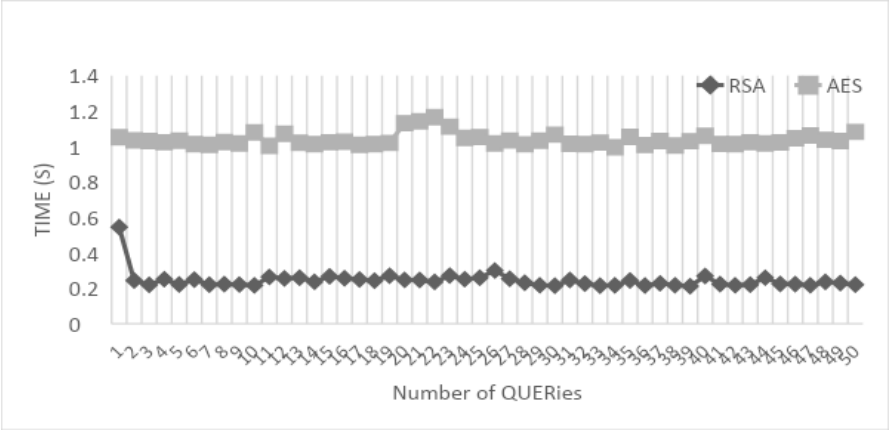


Graphic 4. Encryption Time for Delete.

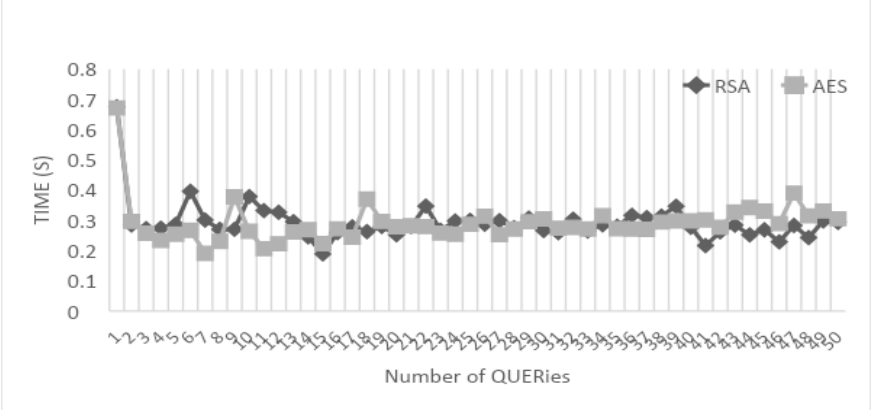
DOI: http://dx.doi.org/10.17993/3ctecno.2019.specialissue3.65-75



Graphic 5. Decryption Time for Add.



Graphic 6. Decryption Time for Select.



Graphic 7. Decryption Time for Delete.

Obviously, the "Add" queries have taken the longest time to complete, given that Add process requires inserting new records which consume more time, compared to displaying existing record as in the "Select" query, or deleting existing record as in the "Delete" query. In general, the performance of the proposed study tends to be competitive between AES and RSA in terms of efficiency.

The results are not significant, as the percentage of improvement for each query types are calculated. It has appeared 23% for Add command, 2% for Select command, and 2% for Delete command between the two encryption methods. The RSA with 2048 key length has given slightly better results in terms of the processing time: "Add", "Select", and "Delete" when the data is set to nvarchar 2000. This might be because of the selection of key size; data type and data size play an important metric criterion in choosing the encryption methods. However, it is recommended, methods should be chosen based on types of cloud applications and services, as well as possible attacks and threats.

4. ACKNOWLEDGEMENT

The authors are grateful to Faculty of Information Science and Technology, National University of Malaysia. This research is also funded by research grant DIP-2018-040.

5. CONCLUSIONS

The potential enhancement that could be used in future studies are using another encryption method may improve encryption time and encryption security, suggest a combination of multiple encryption methods in order to enhance a part of the encryption time and enhance the security of some part, and using real-time dataset could provide some advantage regarding the tactical issue.

DOI: http://dx.doi.org/10.17993/3ctecno.2019.specialissue3.65-75

REFERENCES

Albadri, H., & Sulaiman, R. (2016). A Classification Method for Identifying Confidential Data to Enhance Efficiency of Query Processing over Cloud. *Journal of Theoretical and Applied Information Technology, 93* (2), 412-20.

Aman, A.H.M., Hassan, R., Hashim, A.H.A., and Ramli, H.A.M. (2019). Investigation of Internet of Things Handover Process for Information Centric Networking and Proxy Mobile Internet Protocol. In *3rd International Multi-Topic Conference on Engineering and Science 2019.*

Amini, R., Sulaiman, R. & Abd Rahman Kurais, A. H. (2018). CryptoROS: A secure communication architecture for ROS-based applications. *International Journal of Advanced Computer Science and Applications, 9*(10), 189-194.

Ibrahim, R., Aman, A. H. M., Nur, A. M., & Aljunid, S. M. (2019). Cost Centric Data Mining for Radiology Procedures at Teaching Hospital in Malaysia. In *3rd International Multi-Topic Conference on Engineering and Science 2019.*

Ghaleb, H. S. M., Shukur, Z., Sulaiman, R. & Mobidin, H. S. (2018). Implementation of AES algorithm in QGIS software. *Proceedings of the 2017 6th International Conference on Electrical Engineering and Informatics: Sustainable Society Through Digital Innovation, ICEEI 2017. Institute of Electrical and Electronics Engineers Inc., Vol. 2017-November,* 1-6.

Gupta, P., Verma, D. K. & Singh, A. K. (2018). Improving RSA Algorithm Using Multi-Threading Model for Outsourced Data Security in Cloud Storage. *Proceedings of the 8th International Conference Confluence 2018 on Cloud Computing, Data Science and Engineering, Confluence 2018*, 163-69.

Modak, A., Chaudhary, S.D., Paygude, P.S., & Ldate, S.R. (2018). Techniques to Secure Data on Cloud: Docker Swarm or Kubernetes? *2018 Second International Conference on Inventive Communication and Computational Technologies (ICICCT)*, 7-12.

Singh, K. P., Rishiwal, V., & Kumar, P. (2018). Classification of Data to Enhance Data Security in Cloud Computing. *Proceedings-2018 3rd International Conference On Internet of Things: Smart Innovation and Usages, IoT-SIU 2018*, 1-5. doi: https://doi.org/10.1109/IoT-SIU.2018.8519934

Singh, M. (2015). Study on Cloud Computing and Cloud Database. *International Conference on Computing, Communication and Automation, ICCCA 2015*, 708-13.

Vurukonda, N., & Rao, B. T. (2016). A Study on Data Storage Security Issues in Cloud Computing. *Procedia Computer Science, 92,* 128-35. doi: https://doi.org/10.1016/j.procs.2016.07.335

Edición Especial Special Issue Noviembre 2019
DOI: http://dx.doi.org/10.17993/3ctecno.2019.specialissue3.65-75