Rushi Samirbhai Patel rs397441@dal.ca
B00886157

Assignment 3 - Problem 1

Summary on "Security and Privacy Solutions associated with NoSQL Data Stores" conducted by G. Vonitsanos, E. Dritsas, A. Kanavos, P. Mylonas and S. Sioutas.

Central Idea:

This research paper addresses the security issues involved with storing a large amount of data. It primarily focuses on the main security risks with non-relational databases, also known as NoSQL databases. NoSQL databases are being used by an increasing number of businesses [1]. NoSQL solutions surpass RDBMS, especially when dealing with large amounts of data and parallel processing, and especially when relational modelling isn't required [1]. The research demonstrates that there are security concerns involved with NoSQL databases which are severe in nature since critical data is stored daily here.

The study was conducted since there were significant improvements in cloud computing and distributed applications which led to the adoption of NoSQL databases. Some of the most serious security vulnerabilities in NoSQL databases include the lack of encryption capabilities and insufficient authentication between servers and clients [1]. The research sheds light on how important it is to have a better database that won't have the limitations of all the traditional databases. Modern businesses deal with non-relational data, which necessitates more sophisticated databases than traditional businesses, which face scalability and availability issues due to data volume [1]. There are however some NoSQL databases that are managed by Big Data which use authorization models created with structure, speed, and a large amount of data in mind. Furthermore, the information is stored and retrieved using a unique key for each entry, allowing for a quick search [2].

The research is segregated into multiple sections where the study mentions information on existing related studies on strategies for dealing with security issues along with an overview of a comparison of relational and non-relational databases. Finally after discussing these sections, the researchers propose their mechanism for ensuring security and privacy.

The proposed mechanisms illustrated in the paper act as solutions to security and privacy for NoSQL data stores are - 'Pseudonyms-based Communication Network' and

'Monitoring, Filtering and Blocking'. The former states that a user can enter their credentials just once and use multiple services to ensure user protection while the later states that anomaly detection is implemented in real time, and security analytics can be recorded and updated on a regular basis.

Scope of improvement:

Although this research paper tried to cover all the major security issues of NoSQL databases, I believe a key aspect was left to address by the researchers in this study. I believe that the security of shared NoSQL databases is a major security issue which needs to be addressed as well. There could have been more research on NoSQL sharding mechanisms and analyze the risks associated with such sharded databases. This not only aids in the further research of those places in sharded databases that are lacking in security, but it also allows NoSQL providers and customers to improve the security mechanisms that are already in place [3].

Reference:

[1] G. Vonitsanos, E. Dritsas, A. Kanavos, P. Mylonas and S. Sioutas, "Security and Privacy Solutions associated with NoSQL Data Stores," *2020 15th International Workshop on Semantic and Social Media Adaptation and Personalization (SMA*, 2020, pp. 1-5, doi: 10.1109/SMAP49528.2020.9248442.

[2] P. Colombo and E. Ferrari, "Fine-grained access control within nosql document-oriented data stores", *Data Science and Engineering*, vol. 1, no. 3, pp. 127-138, 2016.

[3] A. Zahid, R. Masood and M. A. Shibli, "Security of sharded NoSQL databases: A comparative analysis," *2014 Conference on Information Assurance and Cyber Security (CIACS)*, 2014, pp. 1-8, doi: 10.1109/CIACS.2014.6861323.