Paper Summary

Title: Security and Privacy Solutions associated with NoSQL Data Stores

Overview

The article focuses on security and privacy concerns in NoSQL (non-relational) databases, which have become more and more popular due to their better performance and capacity to manage enormous amounts of semi-structured and unstructured data when compared to conventional relational databases. Despite its benefits, NoSQL databases have a number of security flaws, dangers, and threats, including insufficient authentication, lack of role-based access control (RBAC), vulnerability to injections, and susceptibility to denial of service attacks.

The CAP theorem—which claims that no shared data system can deliver consistency, availability, and partition tolerance all at once—is covered in this work. The evolution of distributed database systems like Amazon's Dynamo and Google's Bigtable may be affected by this theory.

The article also discusses how non-relational data handling is a must for modern businesses, which conventional databases find challenging owing to scalability and availability issues. Several authorisation methods, such as key-value, broad column, and document-oriented authorization, are used by NoSQL databases and are intended for large volumes of data, speed, and structure.

Related Work

The purpose of the article is to outline security and privacy concerns with NoSQL databases and to provide effective security measures and privacy remedies.

The writers go over a number of early works that analyse the similarities and differences between relational and NoSQL databases, as well as their advantages and dislikes of NoSQL. They point out that, NoSQL databases like Cassandra can enhance system performance and network scalability using low - cost commodity hardware.

The article covers privacy and security issues with NoSQL databases and offers workable solutions. The authors go over earlier studies comparing relational and NoSQL databases, emphasising the benefits of NoSQL in terms of performance and scalability utilising inexpensive hardware. Although acknowledging NoSQL's applicability for expansive, content-focused applications, they also recognise the ongoing usage of relational databases for commercial applications. In addition, the paper provides a thorough overview of security concerns with NoSQL databases like Cassandra and MongoDB and discusses various methods to improve privacy preservation, such as Arx, the BigSecret system, a method utilising searchable encryption algorithms with the Redis database, and SafeRegions for secure NoSQL queries on HBase clusters.Role of NoSQL databases in Big Data management

The authors talk on the use of NoSQL databases for managing Big Data, highlighting how well suited they are for distributed node high-speed data storage and retrieval. NoSQL databases may manage structured, unstructured, or semi-structured data and make use of multi-core GPU systems. Scalability is a major concern for relational databases, which prioritize precision and employ tables, rows, and columns to store data. Relational databases collect information from many sources, which causes big data issues including performance deterioration when utilising OLAP, statistical methods, or data mining. Nevertheless, NoSQL databases were not created with data warehouse applications in mind;

instead, they place a strong emphasis on scalability, availability, and fast performance.Whereas NoSQL databases rely on replication for crash recovery, relational databases have a recovery manager that uses log files and the ARIES algorithm.

Security and Privacy solutions for NoSQL data stores

With the help of RSA and Diffie Hellman protocols, a centralised Identity Provider (IP), Service Providers (SPs), a Verifier (V), and a Credential Authority, the proposed pseudonyms-based communication network provides privacy and security by enabling users to log into multiple services with a single login while remaining anonymous (CA). Nevertheless, the ability to recognise and halt hazardous activities and queries is still restricted for NoSQL databases. Because current real-time security processes in big data technologies are only effective at the API level, the authors propose an initial authentication using Kerberos and a second level of authentication for accessing MapReduce in order to increase security.

Conclusions

This article discusses the main security issues in NoSQL databases, with a focus on access control and data protection. It investigates issues such user data privacy, distributed environments, authentication, granular authorization and access control, data integrity, and protection of data in transit and at rest that may be the cause of security problems in different NoSQL databases. Data in NoSQL databases is grouped by security level for fine-grained authorisation and is authenticated using Kerberos. MongoDB administrators must enact rules to guarantee correct data access, whereas Cassandra employs the TDE approach to protect data while it is at rest. The article discusses several methods for preventing attacks and suggests security and privacy solutions for NoSQL databases in an effort to clarify these issues and advance the creation of trustworthy and secure systems.

The study provides helpful insights into the problems with and solutions for NoSQL database security, although there is still space for improvement in several areas:

Compared with other databases: A more comprehensive examination of NoSQL's security advantages and disadvantages against those of other database formats, such as NewSQL databases, would be possible.

Comprehensive case studies: Case examples from the actual world would assist illustrate the applicability and constraints of the suggested approaches.

Metrics for evaluating suggested solutions: The use of particular criteria will enable more unbiased comparisons and the identification of areas requiring additional study.

Emerging technologies: It would be helpful to investigate how edge computing, serverless architectures, and quantum computing affect the security and privacy of NoSQL.

concentrating on certain NoSQL types: Addressing specific security requirements and vulnerabilities would benefit from analysing security concerns and solutions for each type of NoSQL database (key-value, document, column-family, and graph).

References

[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, Zakynthos, Greece, 2020, pp. 1-5, doi: 10.1109/SMAP49528.2020.9248442.