


Chapter 33

An Efficient, Secure, and Queryable Encryption for NoSQL-Based Databases Hosted on Untrusted Cloud Environments

Mamdouh Alenezi

 <https://orcid.org/0000-0001-6852-1206>
Prince Sultan University, Riyadh, Saudi Arabia

Muhammad Usama

Bahria University, Karachi, Pakistan

Khaled Almustafa

Prince Sultan University, Riyadh, Saudi Arabia

Waheed Iqbal

University of the Punjab, Lahore, Pakistan

Muhammad Ali Raza

University of the Punjab, Lahore, Pakistan

Tanveer Khan

COMSATS University, Islamabad, Pakistan

ABSTRACT

NoSQL-based databases are attractive to store and manage big data mainly due to high scalability and data modeling flexibility. However, security in NoSQL-based databases is weak which raises concerns for users. Specifically, security of data at rest is a high concern for the users deployed their NoSQL-based solutions on the cloud because unauthorized access to the servers will expose the data easily. There have been some efforts to enable encryption for data at rest for NoSQL databases. However, existing solutions do not support secure query processing, and data communication over the Internet and performance of the proposed solutions are also not good. In this article, the authors address NoSQL data at rest security concern by introducing a system which is capable to dynamically encrypt/decrypt data, support secure query processing, and seamlessly integrate with any NoSQL-based database. The proposed solution is based on a combination of chaotic encryption and Order Preserving Encryption (OPE). The experimental evaluation showed excellent results when integrated the solution with MongoDB and compared with the state-of-the-art existing work.

DOI: 10.4018/978-1-7998-7705-9.ch033

1. INTRODUCTION

Nowadays, NoSQL databases are widely used to store and process Big Data mainly due to high performance, scalability, and flexibility features (Schram & Anderson, 2012; Tudorica & Bucur, 2011; Pokorny, 2013). These benefits became possible mainly due to ease of data distribution and shredding in the NoSQL systems. Relational Database Management Systems (RDBMS) are famous for providing the surety of ACID properties, however, performance and scalability of RDBMS are poor after database size start growing dramatically. There are many applications which may not require all ACID properties. For example, social network applications can tolerate relaxation in strict consistency. Moreover, NoSQL databases do not need a strict schema which provides flexibility to the users to update data easily (Okman, Gal-Oz, Gonen, Gudes, & Abramov, 2011). NoSql databases support availability, partition tolerance, and high performance. However, it relaxes data consistency as compared to RDBMS, though most of the NoSQL database support eventual consistency which is feasible and can be neglected in the most of cases because any change in the data will propagate to all the node within few milliseconds and makes the data consistent quickly. Therefore, NoSQL databases are attractive and used in many large-scale applications.

One of the major disadvantages of the NoSQL database is a weak security support which raises concerns for users. Specifically, NoSQL databases store data in flat files which increases security concerns of data at rest. This concern severely increases when NoSQL-bases solutions are deployed on untrusted servers specifically on the cloud because any unauthorized access beaches data confidentiality easily. Some of the NoSQL-based databases provide data encryption methods to ensure data security and confidentiality (Nafi, Kar, Hoque, & Hashem, 2013), (Meyer & Schwenk, 2013). However, the data-at-rest and data-at-transit remain vulnerable as these systems do not provide query processing on encrypted data. Commonly, DES (Data Encryption Standard), AES (Advanced Encryption Standard), Hashing (MD5, SHA) techniques etc. are implemented for data-at-rest encryption but data needs to be decrypted before querying the database. Additionally, these systems require transport layer security protocols and method e.g., SSL, IPSec, TLS and SSH to ensure security during data-at-transit. These techniques increase processing and communication time overhead to ensure security for server-to-server and server-to-client communication. Moreover, plain data exists in memory as query processing over encrypted data is not supported.

Primarily, NoSQL databases were designed and developed without focusing on data security. Thus, third-party tools and services were employed to secure NoSQL databases (Okman, Gal-Oz, Gonen, Gudes, & Abramov, 2011). Moreover, distributed architecture of NoSQL databases exposes to various security vulnerabilities e.g. accidental modifications, illegal use or unauthorized access, administrative or logical decontrols, insecure communication channel, etc. (Zahid, Masood, & Shibli, 2014; Baccam, 2010). This brings new challenges to protect sensitive and critical data from unauthorized access and illegal usage in NoSQL databases. Classic cryptographic techniques can be employed to protect against various security vulnerabilities, and preserve data security during data storage and communication. However, original data remains vulnerable during query processing in the NoSQL database, especially while processing personal information related to healthcare and personal financial transaction (Lin, Tsai, & Lin, 2014). Moreover, NoSQL databases are deployed on public clouds to leverage the benefits of adaptive resource provisioning (Iqbal W., Dailey, Carrera, & Janecek, 2011) and pay-as-you-go features. Which makes the data of NoSQL vulnerable and easy to access by unintended users.

17 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:
www.igi-global.com/chapter/an-efficient-secure-and-queryable-encryption-for-nosql-based-databases-hosted-on-untrusted-cloud-environments/270623

Related Content

Intelligent Personalized Abnormality Detection for Remote Health Monitoring

Poorani Marimuthu, Varalakshmi Perumaland Vaidehi Vijayakumar (2020). *International Journal of Intelligent Information Technologies* (pp. 87-109).

www.irma-international.org/article/intelligent-personalized-abnormality-detection-for-remote-health-monitoring/250282

Agile Workflow Technology and Case-Based Change Reuse for Long-Term Processes

Mirjam Minor, Alexander Tartakovskii and Daniel Schmalen (2008). *International Journal of Intelligent Information Technologies* (pp. 80-98).

www.irma-international.org/article/agile-workflow-technology-case-based/2431

Artificial Intelligence in Innovation Labs: Map of Cases for the Public Sector

Rodrigo Sandoval-Almazan and Adrián Osiel Millán-Vargas (2023). *Handbook of Research on Applied Artificial Intelligence and Robotics for Government Processes* (pp. 115-132).

www.irma-international.org/chapter/artificial-intelligence-in-innovation-labs/312624

On Multi-Fuzzy Rough Sets, Relations, and Topology

Gayathri Varma and Sunil Jacob John (2019). *International Journal of Fuzzy System Applications* (pp. 101-119).

www.irma-international.org/article/on-multi-fuzzy-rough-sets-relations-and-topology/214942

Integrating Modified Delphi with Fuzzy AHP for Concrete Production Facility Location Selection

Golam Kabir and Razia Sultana Sumi (2013). *International Journal of Fuzzy System Applications* (pp. 68-81).

www.irma-international.org/article/integrating-modified-delphi-with-fuzzy-ahp-for-concrete-production-facility-location-selection/94620