WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Exploring NoSQL Databases and Cloud Computing Security Implementations

Shahida B[a]

[a]*CSE department, PDIT, Hospet, India*

DOI: https://doi.org/10.55248/gengpi.2022.3.9.25

A B S T R A C T

It is commonly known that cloud computing, with its prospective benefits, has completely changed the enterprise IT sector. Due to the advantages of worry-free hardware maintenance, many businesses and sectors are transitioning to the cloud computing era. Large businesses are still not migrating to the cloud, which is reducing the market share of cloud computing. From the standpoint of the consumer, the biggest obstacles to using the cloud for data storage are security and privacy concerns. This paper outlines the numerous restrictions relating to data security and privacy protection issues and provides a few technologies, such as Trend Micro's SecureCloudTM, which enables users to function in the cloud safely and securely. Additionally, employing NoSQL databases, personal data security on the cloud. SecureCloud, FIPS 140-2, NoSQL databases, NSA, IAM rules, Accumulo Apache, Amazon DynamoDB, MarkLogic are some of the terms in the index.As a result, cloud users can benefit from the services provided by the cloud while still having total control over their data thanks to encryption keys. The SecureCloudTM uses VM-level encryption to encrypt data in working storage, enabling the use of distinct encryption keys for each user's particular data. This lessens the possibility of recycled disk blocks being sent to other users or of a configuration error causing data privacy violations. The third is commonplace encryption. Data is encrypted using Industry Standard AES by SecureCloudTM, making it inaccessible to anybody missing the encryption keys. The ability of SecureCloudTM to encrypt data gives users advantages when switching users or terminating storage.

Keywords:NoSQL database, Cloud Computing Security, Accumulo Apache, Amazon DynamoDB, MarkLogic, Big Data, Big Data Analytics

1. Introduction

The client-server model was created as a result of the introduction of less expensive RAM and processors, which in turn allowed a large number of users to share the same computing resources on distributed servers. Additionally, bandwidth for these interconnected networks that make up the Internet got faster and less expensive. Additionally, the hardware became so inexpensive that cloud providers could support the development of cloud technology through their datacenters [7] [8] [9]. In order to deliver quick provisioning, efficiency, and cost savings, more and more businesses are turning to cloud computing. Although the suppliers of cloud computing services make claims about the dependability and security of their services, the reality is different. The introduction of these new functionalities brings with it threats to privacy and security. Twice in 2009, between February and July, Amazon S3 services were disrupted. Numerous network-based websites had to be paused as a result of this disaster. Due to security flaws, Google Docs put its customers' private information at risk in March 2009. For roughly 4 hours, even Gmail from Google had issues. Cloud computing uses comparable security procedures as traditional IT. However, because cloud computing is multitenant, it confronts a number of additional dangers and difficulties. Although the extension of enterprise boundaries to the cloud prevents the use of conventional measures. Due to its anonymous multi-tenant nature, deploying confidential information on the cloud attracts numerous risks and threats [1][4][6]. Applications and storage resources continue to be present in the virtual environment, which increases the risk of theft, unauthorized information exposure, and malicious assaults. Additionally, customers cannot be certain that their storage volumes will be cleaned after use. Even after the user has left their cloud volumes, they are still at risk because of this leftover data. If data confidentiality is compromised or regulated data is transported across borders, government legislation and rules for data privacy also give

* *Corresponding author.* Tel.: +0-000-000-0000 ; fax: +0-000-000-0000.
E-mail address: shahida@pdit.ac.in

cloud providers cause for concern. Here, we first briefly go through a number of data security-related challenges before introducing Trend Micro's SecureCloudTM as one of the tools that helps cloud customers securely store their data. The advantages of SecureCloudTM are then brought up to close.

2. Review of Literature

Issues Identified for Cloud Computing Security

Businesses typically erect protocols and safeguards around their datacenters to protect their servers. The physical confinement of servers and hardware resources made it simple to manage the security and safety of their datacenters [2][3][5]. With contrast, the same strategy cannot be applied in cloud computing. Since the consumers' data are kept in distant datacenters and they aren't aware of where they are, Furthermore, numerous users can remotely access the same datacenter that houses the user's data, endangering both the user's data and the actual hardware because it is out of the user's line of sight. Multiple Tenancy Through multi-layer software virtualization, cloud computing users can share the same physical hardware resources. As a result, users are unaware of the virtual machine next to them that is running and whether it has nefarious intentions or just wants to test the hypervisor. The consumer has no idea who or what its neighbor is trying to accomplish.

According to an Amazon Web Service security alert, the Zeus Botnet was able to successfully install and run the command and control infrastructure in the cloud setting. B. Data Control and Mobility Consumers transfer their data from stationary physical servers to distant virtual servers, which makes it dynamic and mobile and enables storage of the data at any virtual datacenter. Additionally, for the sake of maintaining high availability and data upkeep, cloud service providers create duplicate copies of the data. Many legal issues arise as a result. According to laws like the EU Privacy Act, which restricts the transfer of home data to foreign data centers. Therefore, the providers must make sure that such data is not sent outside of authorized areas. C. Remanence of Data even while recycling data is crucial Once a customer leaves the cloud, there are no established standard clear procedures being developed to clear the datacenters. In order to maintain high availability and reliability, providers replicate the customer's data at many locations, yet frequently vacant hardware is assigned to new users without performing the appropriate recycling. D. Data Privacy The open nature of the cloud presents a significant risk to the privacy and confidentiality of data. Since the users' data is stored in a remote virtual location, there is always a chance of a data breach, for which the guilty corporation must pay hefty fines. If private medical records are revealed, it can also have an influence on business and personal levels of loss.

3. Analysis

Cloud Computing Security

With encryption, policy-based key management, and unique server validation, Trend Micro's SecureCloudTM [1] gives cloud and virtual environments the distinguishing feature of data protection and security. It enables the company to function safely with sensitive data in the public cloud using service providers like VMware vCloud, Amazon EC2, Dell, Eucalyptus, and NTT America. The following are some of the SecureCloudTM's primary features: 1) Modern security methods featuring Federal Information Processing Standard (FIPS) 140-2 [2] certification and Advanced Encryption Standard (AES) encryption that has been authorized by FIPS [3]. Real-time encryption and decryption ensure that data at rest remains secure at all times.Encrypts the entire volume to safeguard all data, metadata, and related structures while maintaining application functionality.2) Controls for access and authentication (a) Role-based management is used to achieve proper job separation. b) either automates virtual machine permission and key release for faster operations or requires manual approval for increased security.c) Allows cloud providers to rotate their credentials.Principle-based Key Management a) enforces policies based on identity and integrity to guarantee that only authorized virtual machines have access to secure volumes and keys. b) integrates with Deep Security Manager to more thoroughly verify the security posture of the environment. c) makes it possible to establish policies to control how and when information is accessible. Strengthened Auditing, Reporting, and Alerting Actions in the management console are logged for audit purposes (a). b) Provides extensive reporting and alerting capabilities, as well as incident-based and periodic notifications.Users of Trend Micro's SecureCloudTM have access to the following features, which help to secure their cloud-based data: A Simple Deployment Through kernel-level encryption and the installation of a straightforward agent in the virtual image, SecureCloudTM guarantees that the data stored in the cloud is secure. Since the communication between this agent and the SecureCloudTM is safe, all man-in-the-middle attacks to obtain access to the encryption keys are avoided. Consumers in SecureCloudTM have exclusive access to the encryption keys and, as a result, complete control over their data.Consumers or Trend Micro are responsible for managing encryption keys; cloud providers are not.

This enables cloud users to take advantage of the services offered by the cloud while also maintaining complete control over their data through encryption keys. Data in working storage is encrypted thanks to the SecureCloudTM's use of VM-level encryption, which allows for separate encryption keys to be utilized for each user's unique data. This reduces the chance that recycled disk blocks will be distributed to other users or that a configuration error will violate data privacy. Industry-standard encryption is a third. SecureCloudTM encrypts data using Industry Standard AES, rendering it unusable by anybody lacking the encryption keys. SecureCloudTM's characteristic of encrypting the data allows the consumers to have benefits when changing users or ending storage. The storage is secure for the users because any encrypted data that is still present is useless and unrecognisable. As a result, there are fewer chances of data theft, exposure to outsiders, etc. D. Granular Control: The user can precisely track which server has access to its encrypted data thanks to SecureCloudTM's innovative policy-based key management and safe data access features.TheSecureCloudTM key server must first be verified by virtual servers using credentials that have been encrypted in the virtual machine's kernel. The SecureCloudTM key server verifies the data in

accordance with the established policies and releases the key to the server when it is determined that the virtual environment is safe. Additionally, it gives administrators role-based access with a range of permissions, including audit logging, key access, and full access. E.Users are given access to the control data necessary to isolate the physical key storage from the company that provides the cloud infrastructure. This prevents the infrastructure provider from having access to the keys and gives consumers complete control so they can switch vendors without experiencing a vendor lock-in issue. Its on-premises solution offers more features by enabling the keys to be kept in the custody of SecureCloudTM at all times. Viewing the system configuration settings is made possible by SecureCloudTM thanks to the management server's audit trail of significant approvals. It also enables the thorough logging and reporting of all activities taken in connection with important approvals. All changes made by the administrator or the system itself are also kept track of and recorded.

As cloud users, we cannot guarantee the security of sensitive data. Since there is no way for the cloud provider to completely ensure security, NoSQL databases [4] have become a popular option when dealing with massive data sets in such circumstances. Now, big data administrators may take advantage of NoSQL's advantages while still exerting some control over who has access to particular cloud data subsets. There are three methods for protecting NoSQL data stores: Cell-based access controls for Accumulo [5][19] Amazon DynamoDB [6] [18] and AWS Identity and Access Management (IAM) [7][17] are used.policies [8] [10] [11]: The compartment controls and execution privileges of MarkLogic are described. The Accumulo Data Store, developed by the NSA and released in 2011, is the first Big Table-based distributed, key-value data storage system.Accumulo is a Hadoop-based Apache project that offers extra functionality not included in Big Table, such as cell-based access controls. A visibility attribute on Accumulo keys specifies security designations like admin, finance, or management. The set of rows that a user can query, or change is constrained by key-based access controls since each key is linked to a single value, which corresponds to a row in a relational table. Then, permissions are granted to users, specifying particular security labels that can be coupled in logical expressions to build access controls as required. A manager in the finance division, for instance, would be given the "manager" and "finance" identities. B. Amazon DynamoDB [18] Key-value data storage serviceDynamoDB offers both provided IOPS and managed scaling. For programmers and application administrators who prefer a hosted service to managing their own NoSQL database [18], Amazon DynamoDB is an excellent choice. Administrators must include conditions in an IAM policy to ensure fine-grained access control in Amazon DynamoDB. Conditions determine whether certain objects and attributes in the key-value data store are accessible or not. This paradigm restricts access to certain values or rows, such as data linked to a specific customer account, allowing customers to see just their own data [13][14][15][16][20][21]. C. MarkLogic Document-based NoSQL databases, like MarkLogic, provide the ability to expand role-based access controls by compartmentalizing roles and documents. Additionally, MarkLogic offers access control for when operations are carried out. In the database, there is a set of predefined execute privileges for data management, security, and other administrative tasks.

4. Summary

Despite the many options offered by cloud computing, questions about data security and safety often come up. To reduce this risk, some cloud service providers employ encryption, key management, and other strategies. Through its encryption and unique key management, Trend Micro's SecureCloudTM enables users to move their data in a virtualized environment without worrying about data security. It safeguards and maintains the user's data, giving them the freedom to move across cloud users, have complete control over their data, and choose who gets access. It offers a comprehensive solution for protecting data in both private clouds and public infrastructure-as-a-service. NoSQL database policies are used by some businesses and cloud IT administrators to safeguard data in the cloud and limit access by using the right queries, rights, and table partitions. For instance, the compartment control in MarkLogic, Amazon DynamoDB, and Accumulo's cell-based access controls.As a result, users of the cloud can benefit from those services while still having total control over their data thanks to encryption keys. The SecureCloudTM uses VM-level encryption, which enables distinct encryption keys to be used for each user's particular data, to encrypt data in working storage. The likelihood that recycled disk blocks will be given to other users or that a setup error will compromise data privacy is decreased as a result. The third type of encryption used in business. Data is encrypted by SecureCloudTM utilizing Industry Standard AES, making it inaccessible to anybody missing the encryption keys. Data encryption is a feature of SecureCloudTM that gives users advantages while switching users or terminating storage.

REFERENCES

[1] Abramova, V., & Bernardino, J. (2013, July). NoSQL databases: MongoDB vs Cassandra. In Proceedings of the international C* conference on computer science and software engineering (pp. 14-22).

[2] Ali, W., Shafique, M. U., Majeed, M. A., & Raza, A. (2019). Comparison between SQL and NoSQL Databases and Their Relationship with Big Data Analytics. Asian Journal of Research in Computer Science, 4(2), 1-10

[3] Becker, M. Y., & Sewell, P. (2004, June). Cassandra: Flexible trust management, applied to electronic health records. In Proceedings. 17th IEEE Computer Security Foundations Workshop, 2004. (pp. 139-154). IEEE.

[4] Berg, K. L., Seymour, T., & Goel, R. (2013). History of databases. International Journal of Management & Information Systems (IJMIS), 17(1), 29-36.

[5] Bjeladinovic, S., Marjanovic, Z., & Babarogic, S. (2020). A proposal of architecture for integration and uniform use of hybrid SQL/NoSQL database components. Journal of Systems and Software, 168, 110633.

[6] Chandra, D. G. (2015). BASE analysis of NoSQL database. Future Generation Computer Systems, 52, 13-21.

[7] Chen, J. K., & Lee, W. Z. (2019). An introduction of NoSQL databases based on their categories and application industries. Algorithms, 12(5), 106.

[8] Cuzzocrea, A., & Shahriar, H. (2017, December). Data masking techniques for NoSQL database security: A systematic review. In 2017 IEEE International Conference on Big Data (Big Data) (pp. 4467-4473). IEEE.

[9] de Oliveira, V. F., Pessoa, M. A. D. O., Junqueira, F., & Miyagi, P. E. (2021). SQL and NoSQL Databases in the Context of Industry 4.0. Machines, 10(1), 20.

[10] Deka, G. C. (2013). A survey of cloud database systems. It Professional, 16(2), 50-57. IEEE.

[11] Di Martino, S., Fiadone, L., Peron, A., Riccabone, A., & Vitale, V. N. (2019, June). Industrial Internet of Things: Persistence for Time Series with NoSQL Databases. In 2019 IEEE 28th International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE) (pp. 340-345). IEEE.

[12] dos Santos Ferreira, G., Calil, A., & dos Santos Mello, R. (2013, December). On providing DDL support for a relational layer over a document NoSQL database. In Proceedings of International Conference on Information Integration and Web-based Applications & Services (pp. 125-132).

[13] Gessert, F., Wingerath, W., Friedrich, S., & Ritter, N. (2017). NoSQL database systems: a survey and decision guidance. Computer Science-Research and Development, 32(3), 353-365.

[14] Guimaraes, V., Hondo, F., Almeida, R., Vera, H., Holanda, M., Araujo, A., ... & Lifschitz, S. (2015, November). A study of genomic data provenance in NoSQL document-oriented database systems. In 2015 IEEE International Conference on Bioinformatics and Biomedicine (BIBM) (pp. 1525-1531). IEEE.

[15] Rodriguez, K. M., Reddy, R. S., Barreiros, A. Q., & Zehtab, M. (2012, June). Optimizing Program Operations: Creating a Web-Based Application to Assign and Monitor Patient Outcomes, Educator Productivity and Service Reimbursement. In DIABETES (Vol. 61, pp. A631-A631). 1701 N BEAUREGARD ST, ALEXANDRIA, VA 22311-1717 USA: AMER DIABETES ASSOC.

[16] Kwon, D., Reddy, R., & Reis, I. M. (2021). ABCMETAapp: R shiny application for simulation-based estimation of mean and standard deviation for meta-analysis via approximate Bayesian computation. Research synthesis methods, 12(6), 842–848. https://doi.org/10.1002/jrsm.1505

[17] Reddy, H. B. S., Reddy, R. R. S., Jonnalagadda, R., Singh, P., & Gogineni, A. (2022). Usability Evaluation of an Unpopular Restaurant Recommender Web Application Zomato. Asian Journal of Research in Computer Science, 13(4), 12-33.

[18] Reddy, H. B. S., Reddy, R. R. S., Jonnalagadda, R., Singh, P., & Gogineni, A. (2022). Analysis of the Unexplored Security Issues Common to All Types of NoSQL Databases. Asian Journal of Research in Computer Science, 14(1), 1-12.

[19] Singh, P., Williams, K., Jonnalagadda, R., Gogineni, A., &; Reddy, R. R. (2022). International students: What's missing and what matters. Open Journal of Social Sciences, 10(02),

[20] Jonnalagadda, R., Singh, P., Gogineni, A., Reddy, R. R., & Reddy, H. B. (2022). Developing, implementing and evaluating training for online graduate teaching assistants based on Addie Model. Asian Journal of Education and Social Studies, 1-10.

[21] Sarmiento, J. M., Gogineni, A., Bernstein, J. N., Lee, C., Lineen, E. B., Pust, G. D., & Byers, P. M. (2020).Alcohol/illicit substance use in fatal motorcycle crashes. Journal of surgical research, 256, 243-250.

[22] Brown, M. E., Rizzuto, T., & Singh, P. (2019). Strategic compatibility, collaboration and collective impact for community change. Leadership & Organization Development Journal.

[23] Sprague-Jones, J., Singh, P., Rousseau, M., Counts, J., & Firman, C. (2020). The Protective Factors Survey: Establishing validity and reliability of a self-report measure of protective factors against child maltreatment. Children and Youth Services Review, 111, 104868