Journal of Informatics Education and Research
ISSN: 1526-4726
https://doi.org/10.52783/jier.v3i2.274
Vol 3 Issue 2 (2023)

Enhancing Security of Relational Databases in Cloud Computing through Blockchain Integration

[1]Dr. Reda Salama, [2]Wajdi Alghamdi, [3]Dr. Ujjwal Agarwal, [4]Prof (Dr.) Harikumar Pallathadka, [5]Dr. Dolpriya Devi Manoharmayum, [6]Dayakar Babu Kancherla

[1]Department of Information Technology, Faculty of Computing and Information Technology, King Abdulaziz University, Jeddah, Saudi Arabia

[2]Department of Information Technology, Faculty of Computing and Information Technology, King Abdulaziz University, Jeddah, Saudi Arabia

[3]Lecturer (Information Technology), College of Computing & Information Sciences, University of Technology and Applied Sciences, Salalah, Oman

[4]Professor and Director, Manipur International University, Imphal, Manipur

[5]Assistant Professor, KL College of Agriculture, Koneru Lakshmaiah Education Foundation -KLEF (Deemed To Be University), Guntur, Andhra Pradesh, India

[6]Sr Technology Leader, Health and Wellness , Pharmacy, Albertsons Companies, Plano, Tx, USA

Abstract

Using legacy technology and technique is very harmful in IT. Change is only constant in IT for upgrading technology. Running on older architecture is huge risk to IT systems. Current IT is era of cloud edge technology. Cloud is simpler, rapid and low-cost solution to customers. Trending approaches is pay-as-use services, because infra is huge cost to projects. Hence every project is migrating to cloud. Truth is technology itself godship and enemy. So, challenges are security to data. Every application demands security and privacy of customer data. In past seen many incident of security issues into cloud infrastructure. However, organisations move on cloud is smarter choice but also see an increase the huge risk of data security. Today our work focus is about enlighten on issue about security, privacy and authenticity of data into cloud services. Storage to sensible data on cloud to across glob is huge chance of attack, stolen and manipulation. One of the most innovative and trustful solution of cloud security is blockchain. It works for all phase of data security, privacy, encryptions and authenticity. Blockchain as self-proven, life-saver solution for security on cloud computing. Blockchain effectively works for controls on encryption, authentication and validation of data. Blockchain has solve constant issue and prove it by cryptocurrency, smart contacts, smart grid and safe from assaults like brute force. In distributed RDBMS services has many challenges from internal and external attacks. Finally, our work is investigating the blockchain and try for RDBMS services on cloud.

Keywords – Blockchain, Coud Computing, Confidentiality, Integrity, Privacy, Relational Database.

I. INTRODUCTION

Among the most important issues with digital advertising using blockchain today are worries about sphere fraud, bot business, a lack of transparency, and extended payment methods. Blockchain can address these problems since the technology will only allow the right businesses to succeed. By fewer negative actors in the force chain, fraud and other problems will be reduced.

Blockchain is utilised in cyber security. Data breaking and verification will be aided by the innovative cryptography point of the blockchain technology. This reduces the likelihood that the data will be compromised or altered without authorization.

Blockchain is helpful while vaticinating. Blockchain technology is expected to change the way that research, counselling, analysis, and soothsaying are all done. Vaticination requests are made using a sizable fraction of the distributed online portals used throughout the world.

II. RELATED WORK

Authors present PRADA, a new approach to account for compliance with data handling requirements in key-value based cloud storage systems. To achieve this goal, PRADA introduces a transparent data handling layer, which empowers clients to request specific data handling requirements and enables operators of cloud storage systems to comply with them. Authors implement PRADA on top of the distributed database Cassandra and show in our evaluation that complying with data handling requirements in cloud storage systems [1].

In this paper, author introduce PRADA, a practical approach to enforce data compliance in key-value based cloud storage systems. To this end, PRADA introduces a transparent data handling layer which enables clients to specify data handling requirements and provides operators with the technical means to adhere to them [2].

The contributions of this paper are in detailing how an IFC (Information Flow Control) system can best be designed and engineered to meet such concerns. The IFC mechanism provider, e.g. a cloud PaaS provider where IFC is enforced at OS level, can be expected to provide a correct enforcement mechanism, but cannot take responsibility for the correct definition of application policies [3].

Author present a dynamic and extensible system for the management of storage resources in multitenant cloud applications. In the presented approach, tenants are hierarchically clustered based on multiple scenario-specific characteristics, and allocated to storage resources using a hierarchical bin packing algorithm (static allocation). As the load changes over time, the system corresponds to these changes by reallocating storage resources when required (dynamic reallocation) [4].

Author propose the Swift Analytics object storage system to address them: (I) it uses locality-aware writes to control an object's location and eliminate unnecessary I/O related to renames during job completion, speeding up analytics jobs by up to 5.1×; (ii) it transparently chunks objects into smaller sized parts to improve data-locality, leading to up to 3.4× faster reads [5].

Author present an approach for service owners to influence placement of their service components by explicitly specifying service structure, component relationships, and placement constraints between components. Author show how the structure and constraints can be expressed and subsequently formulated as constraints that can be used in placement of virtual machines in the cloud [6].

Author introduce IFC, Information Flow Control (IFC) potentially offers data-centric, system-wide data access control. It has been shown that IFC can be provided at operating system level as part of a PaaS offering, with an acceptable overhead. In this paper authors consider how IFC can be integrated with application-specific access control, transparently from application developers, while building from simple IFC primitives, access control policies that align with the data management obligations of cloud providers and tenants [7].

In this article, authors present a dynamic and extensible system for the management of storage resources in multitenant cloud applications. In the presented approach, tenants are hierarchically clustered based on multiple scenario-specific characteristics, and allocated to storage resources using a hierarchical bin packing algorithm (static allocation). As the load changes over time, the system corresponds to these changes by reallocating storage resources when required (dynamic reallocation). Authors evaluate both the static and dynamic behaviour of our system [8].

Authors identify the two most severe performance problems when running data-parallel frameworks on the OpenStack Swift object storage system in comparison to the HDFS distributed filesystem:(I) the fixed mapping of object names to storage nodes prevents local writes and adds delay when objects are renamed; (ii) the coarser granularity of objects compared to blocks reduces data locality during reads. We propose the Swift Analytics object storage system to address them: (I) it uses locality-aware writes to control an object's location and eliminate unnecessary I/O related to renames

Journal of Informatics Education and Research
ISSN: 1526-4726
https://doi.org/10.52783/jier.v3i2.274
Vol 3 Issue 2 (2023)

during job completion, speeding up analytics jobs by up to 5.1×; (ii) it transparently chunks objects into smaller sized parts to improve data-locality, leading to up to 3.4× faster reads [9].

Authors present an approach for service owners to influence placement of their service components by explicitly specifying service structure, component relationships, and placement constraints between components. Authors show how the structure and constraints can be expressed and subsequently formulated as constraints that can be used in placement of virtual machines in the cloud. Authors use an integer linear programming scheduling approach to illustrate the approach, show the corresponding mathematical formulation of the model, and evaluate it using a large set of simulated input [10].

III. OPEN ISSUE

The data must be stored in RDBMS, and there is a possibility that a third party with access credentials could compromise the data's integrity. Therefore, the data that was saved in the cloud lacked security. To solve this issue, we built a project that requires three steps for anyone wishing to access the data.

- Security: Ensure that the customer has the right to know whether and how their data is refined.
- Data discretion: Prevents the release of customer information to unauthorised parties.
- Data Consistency: New processing procedures maintain data consistency throughout the life cycle, are not random, and satisfy client requirements.

IV. PROPOSED SYSTEM

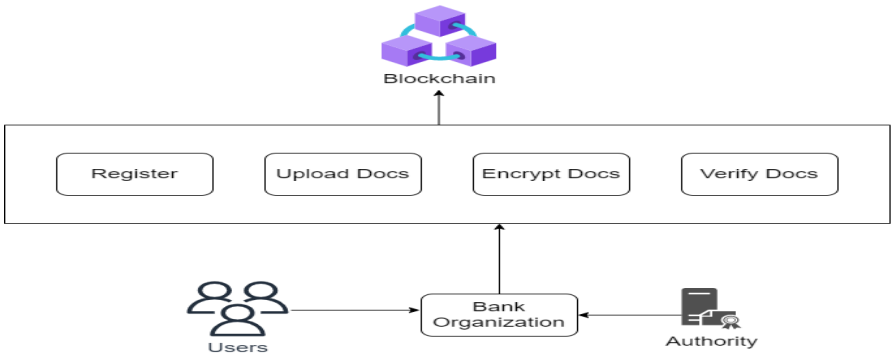

Figure 1. System Architecture

- In proposed system, we implement a block chain Based system, in which each customer uploads a data files and encrypts these data with corresponding key.
- To implement both security preservation and relevant searches, we propose an effective search scheme.
- In this framework, the server is permitted to viably combine various encrypted records, and safely play out the pursuit without uncovering the user sensitive data, neither information documents nor the questions.

Algorithm Details

AES Algorithm for Encryption.

- AES (advanced encryption standard). It is symmetric algorithm. It used to convert plain text into cipher text. The need for coming with this alga is weakness in DES. The 56-bit key of des is no longer safe against attacks based on exhaustive key searches and 64-bit block also consider awakes was to be used128-bit block with128-bit keys.
- Rivendell was founder. In this drop we are using it to encrypt the data owner file.
- Input:
- 128_bit /192 bit/256-bit input (0, 1)

Journal of Informatics Education and Research
ISSN: 1526-4726
https://doi.org/10.52783/jier.v3i2.274
Vol 3 Issue 2 (2023)

- Secret key (128_bit) +plain text (128_bit).
- Process:
- 10/12/14-rounds for-128_bit /192 bit/256-bit input
- Xor state block (i/p)
- Final round:10,12,14
- Each round consists: sub byte, shift byte, mix columns, add round key.
- Output:
- cipher text (128 bit)

MD5(Message-Digest Algorithm)

- The MD5 message-digest algorithm is a widely used cryptographic hash function producing a 128-bit (16-byte) hash value, typically expressed in text format as a 32-digit hexadecimal number. MD5 has been utilized in a wide variety of cryptographic applications, and is also commonly used to verify data integrity.
- Steps:
- A message digest algorithm is a hash function that takes a bit sequence of any length and produces a bit sequence of a fixed small length.
- The output of a message digest is considered as a digital signature of the input data.
- MD5 is a message digest algorithm producing 128 bits of data.
- It uses constants derived to trigonometric Sine function.
- It loops through the original message in blocks of 512 bits, with 4 rounds of operations for each block, and 16 operations in each round.
- Most modern programming languages provides MD5 algorithm as built-in functions

Result and Discussion:

Experiments are done by a personal computer with a configuration: Intel (R) Core (TM) i3-2120 CPU @ 3.30GHz, 4GB memory, Windows 7, MySQL 5.1 backend database and Jdk 1.8. The application is web application used tool for design code in Eclipse and execute on Tomcat server.

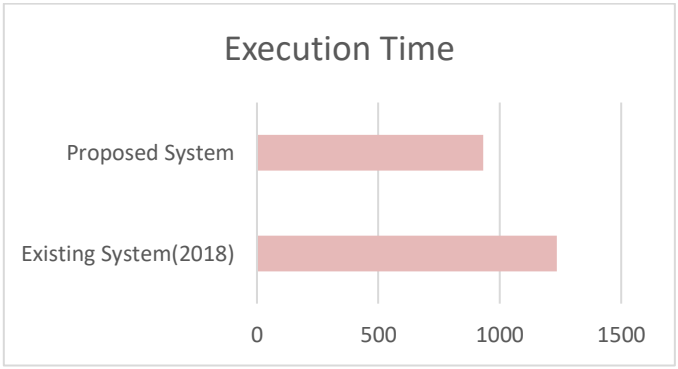

Figure 2: overall system execution graph

Existing System (2018)	Proposed System
1236	932

Table 1: overall system execution table

Conclusion

The paper aims to fortify database security in cloud computing. Its title is "Enhancing Relational Database Security Using Blockchain". The approach uses a three-tier authentication process. This involves encryption and decryption techniques.

As a result, data access by unauthorized third parties is hindered. Blockchain technology is at the core of this enhancement. Its implementation ensures heightened security measures. In essence, this project blends blockchain and cloud computing. This fusion promises a more secure database environment. The outcomes can be revolutionary for data protection in the cloud.

Reference

[1] Martin Henze, Roman Matzutt, Jens Hiller, Erik M¨uhmer, Jan HenrikZiegeldorf, Johannes van der Giet, and Klaus Wehrle" Complying with Data Handling Requirements in Cloud Storage Systems" IEEE 2020
[2] M. Henze et al., "Practical Data Compliance for Cloud Storage," in IEEE IC2E, 2017.
[3] T. Pasquier et al., "Data-centric access control for cloud computing," in ACM SACMAT, 2016.
[4] P.-J. Maenhaut et al., "A Dynamic Tenant-Defined Storage System for Efficient Resource Management in Cloud Applications," Journal of Network and Computer Applications, 2017.
[5] L. Rupprecht et al., "SwiftAnalytics: Optimizing Object Storage for Big Data Analytics," in IEEE IC2E, 2017.
[6] D. Espling et al., "Modeling and Placement of Cloud Services with Internal Structure," IEEE Transactions on Cloud Computing, vol. 4, no. 4, 2014.
[7] T. Pasquier et al., "Data-centric access control for cloud computing," in ACM SACMAT, 2016.
[8] P.-J. Maenhaut et al., "A Dynamic Tenant-Defined Storage System for Efficient Resource Management in Cloud Applications," Journal of Network and Computer Applications, 2017.
[9] L. Rupprecht et al., "SwiftAnalytics: Optimizing Object Storage for Big Data Analytics," in IEEE IC2E, 2017.
[10] D. Espling et al., "Modeling and Placement of Cloud Services with Internal Structure," IEEE Transactions on Cloud Computing, vol. 4, no. 4, 2014.
[11] Sobia Wassan, Chen Xi, Tian Shen, Kamal Gulati, Kinza Ibraheem, Rana M. Amir Latif Rajpoot, "The Impact of Online Learning System on Students Affected with Stroke Disease", Behavioural Neurology, vol. 2022, Article ID 4847066, 14 pages, 2022. https://doi.org/10.1155/2022/4847066
[12] Sobia Wassan, Tian Shen, Chen Xi, Kamal Gulati, Danish Vasan, Beenish Suhail, "Customer Experience towards the Product during a Coronavirus Outbreak", Behavioural Neurology, vol. 2022, Article ID 4279346, 18 pages, 2022. https://doi.org/10.1155/2022/4279346
[13] Dhiman, G.; Juneja, S.; Viriyasitavat, W.; Mohafez, H.; Hadizadeh, M.; Islam, M.A.; El Bayoumy, I.; Gulati, K. A Novel Machine-Learning-Based Hybrid CNN Model for Tumor Identification in Medical Image Processing. Sustainability 2022, 14, 1447. https://doi.org/10.3390/su14031447
[14] Akanksha, E., Sharma, N., & Gulati, K. (2021, January). OPNN: Optimized Probabilistic Neural Network based Automatic Detection of Maize Plant Disease Detection. In 2021 6th International Conference on Inventive Computation Technologies (ICICT) (pp. 1322-1328). IEEE.
[15] Gulati, K., Boddu, R. S. K., Kapila, D., Bangare, S. L., Chandnani, N., & Saravanan, G. (2021). A review paper on wireless sensor network techniques in Internet of Things (IoT). Materials Today: Proceedings.
[16] Gulati, K., Kumar, S. S., Boddu, R. S. K., Sarvakar, K., Sharma, D. K., & Nomani, M. Z. M. (2021). Comparative analysis of machine learning-based classification models using sentiment classification of tweets related to COVID-19 pandemic. Materials Today: Proceedings.
[17] Wisetsri, W., R.T.S., Julie Aarthy, C.C., Thakur, V., Pandey. D. and Gulati K. (2021), Systematic Analysis and Future Research Directions in Artificial Intelligence for Marketing. Turkish Journal of Computer and Mathematics Education (TURCOMAT), 12(11), 43-55.
[18] Akanksha, E., Sharma, N., & Gulati, K. (2021, April). Review on Reinforcement Learning, Research Evolution and Scope of Application. In 2021 5th International Conference on Computing Methodologies and Communication (ICCMC) (pp. 1416-1423). IEEE.
[19] Singh, U. S., Singh, N., Gulati, K., Bhasin, N. K., & Sreejith, P. M. (2021). A study on the revolution of consumer relationships as a combination of human interactions and digital transformations. Materials Today: Proceedings.
[20] Gulati, K., Boddu, R. S. K., Kapila, D., Bangare, S. L., Chandnani, N., & Saravanan, G. (2021). A review paper on wireless sensor network techniques in Internet of Things (IoT). Materials Today: Proceedings.

[21] SANGEETHA, D. M., PRIYA, D. R., ELIAS, J., MAMGAIN, D. P., WASSAN, S., & GULATI, D. K. (2021). Techniques Using Artificial Intelligence to Solve Stock Market Forecast, Sales Estimating and Market Division Issues. Journal of Contemporary Issues in Business and Government, 27(3), 209-215.

[22] Dovhan, O.D., Yurchenko, O.M., Naidon, J.O., Peliukh, O.S., Tkachuk, N.I. and Gulati, K. (2021), "Formation of the counter intelligence strategy of Ukraine: national and legal dimension", World Journal of Engineering, Vol. ahead-of-print No. ahead-of-print. https://doi.org/10.1108/WJE-06-2021-0358

[23] Billewar, S.R., Jadhav, K., Sriram, V.P., Arun, D.A., Mohd Abdul, S., Gulati, K. and Bhasin, D.N.K.K. (2021), "The rise of 3D E-Commerce: the online shopping gets real with virtual reality and augmented reality during COVID-19", World Journal of Engineering, Vol. ahead-of-print No. ahead-of-print. https://doi.org/10.1108/WJE-06-2021-0338

[24] Sanil, H.S., Singh, D., Raj, K.B., Choubey, S., Bhasin, N.K.K., Yadav, R. and Gulati, K. (2021), "Role of machine learning in changing social and business eco-system – a qualitative study to explore the factors contributing to competitive advantage during COVID pandemic", World Journal of Engineering, Vol. ahead-of-print No. ahead-of-print. https://doi.org/10.1108/WJE-06-2021-0357

[25] L. M. I. L. Joseph, P. Goel, A. Jain, K. Rajyalakshmi, K. Gulati and P. Singh, "A Novel Hybrid Deep Learning Algorithm for Smart City Traffic Congestion Predictions," 2021 6th International Conference on Signal Processing, Computing and Control (ISPCC), 2021, pp. 561-565, doi: 10.1109/ISPCC53510.2021.9609467.

[26] S. L. Bangare, S. Prakash, K. Gulati, B. Veeru, G. Dhiman and S. Jaiswal, "The Architecture, Classification, and Unsolved Research Issues of Big Data extraction as well as decomposing the Internet of Vehicles (IoV)," 2021 6th International Conference on Signal Processing, Computing and Control (ISPCC), 2021, pp. 566-571, doi: 10.1109/ISPCC53510.2021.9609451.

[27] V. P. Sriram, K. B. Raj, K. Srinivas, H. Pallathadka, G. S. Sajja and K. Gulati, "An Extensive Systematic Review of RFID Technology Role in Supply Chain Management (SCM)," 2021 6th International Conference on Signal Processing, Computing and Control (ISPCC), 2021, pp. 789-794, doi: 10.1109/ISPCC53510.2021.9609414.