BioGecko

Vol 12 Issue 03 2023
ISSN NO: 2230-5807

Cloud Computing And Secure Keyword-Based Search: A Review

1st Dr.Arulprakash A
Department of Computer Science and Engineering
Bharath Institute of Higher Education and Research
Chennai, India
Prakash875@gmail.com

4th Rohith.G
Department of Computer Science and Engineering
Bharath Institute of Higher Education and Research
Chennai, India
rohithg302002@gmail.com

2nd Karthikeyan.K
Department of Computer Science and Engineering
Bharath Institute of Higher Education and Research
Chennai, India
karthicthalapathy0@gmail.com

5th Sai Vignesh
Department of Computer Science and Engineering
Bharath Institute of Higher Education and Research
Chennai, India
saivignesh2203@gmail.com

3rd Kasam Shree Veera Hanuman Reddy
Department of Computer Science and Engineering
Bharath Institute of Higher Education and Research
Chennai, India
kasamhanuman2001@gmail.com

ABSTRACT:

A system that combines Block chain technology is used for secure distributed data storage and a keyword search service. Users can upload encrypted files, the system distributes them across cloud nodes, and it makes use of cryptographic techniques to ensure data availability. The cloud server is also regarded as trustworthy. We first highlight the significance of maintaining the data in a public chain before providing a block chain-based solution for secure distributed data storage with keyword search functionality. We suggest a solution that combines block chain technology-based keyword search with secure distributed data storage. The technology makes it possible for users to upload data in an encrypted format, distributes it across cloud nodes, and guarantees data availability. Takes Exam offers server-side verifiability, preventing and it is imperative that dishonest data owners refrain from using dishonest cloud servers as props throughout the storage phase of the data lifecycle. Additionally, without the use of third parties, block chain technologies and hash functions enabled equitable payment of search fees. Regardless of TKSE is sufficiently secure and efficient to be used for cloud computing according to our security and performance analysis. This system possesses the main objective of being secure and efficient, additionally; our performance assessment and security research show that it may be employed in cloud computing systems.

Keywords: *searchable symmetric encryption schemes (SSE), block chain technology, trusted third party (TTP), ECDSA stands for Elliptic Curve Digital Signature Algorithm.TKSE, cloud computing.*

1. INTRODUCTION:

Cloud computing technologies have advanced quickly in recent years, and a number of research has been done on cloud computing security challenges, specifically access control and privacy protection [1]. Cloud storage requires both search functionality and data security as a typical cloud computing service. User-side verifiability takes harmful cloud server potential into serious consideration, which means it might purposefully produce inaccurate results or just return a portion of the search results [2]. The first topic covered in is user-side verifiability. However, without a reliable third party, these two systems are unable to offer server-side verifiability and fair remuneration. Server-side verifiability also considers the possibility of unscrupulous data owners, who can purposefully outsource inaccurate data during the data storage phase and then falsely seek recompense afterwards [3]. This issue has not been addressed, and even in the literature, it has not gotten much attention. Not least among other things, the majority of the earlier programmers rely on banks. In particular either the usual traditional payment system is utilized or it is necessary to install a reputable bank is an example of a trusted third party (TTP).to ensure payment fairness because The payment issue is not considered [4]. Fair payment procedures can motivate cloud servers and users to behave honestly [5]. Whatever the cloud server (or data owner) performs, if a detrimental behavior is identified [6]. If malicious activity is found based on user-side verifiability, the data owner (i.e. cloud server) will be notified immediately.) Will be adequately reimbursed (resp. server-side verifiability). This makes SSE's responsibility to make fair payments without the help of a third party a big and challenging one. We our performance review demonstrates the efficacy of TKSE and demonstrates its security. The following ideal characteristics best describe TKSE in particular. Searching for Keywords in Encrypted Data [8]. The Elliptic Curve Digital Signature Algorithm (ECDSA)-based encrypted data index enables users to browse through the encrypted material that has been outsourced. Verifiable by the user [9] In TKSE, a data owner can add search criteria to a joint transaction's output script in order to ensure that, and only in the event that, the script evaluates to true base on their turned search result, the data owner will receive the joint transaction's results. The cloud server may redeem the transaction. TKSE is used to achieve user-side verifiability as a result, and the data owner is able to fend against adversarial cloud servers [10]. On the server side, verifiable, similar to user-side verifiability, verifiability on the server is accomplished by the cloud server by recognizing fraudulent data owners. Just Compensation and No TTP block can be used without adding any TTP. Chain allow for a fair payment system in TKSE. Prior to outsourcing cloud computing, data must be encrypted because cloud servers are unreliable and users' data privacy must be protected [12]. Users are able to upload encrypted data, distribute it among cloud nodes, and employ cryptographic techniques to ensure data availability. Additionally The project's use of cloud computing and analysis based on search and data sharing to provide security is novel [13]. According to Our performance evaluation and security analysis show that TKSE is appropriate for cloud computing since it is both secure and effective. [14]. we provide a solution for Utilizing block chain technology, Through the implementation of server-side verifiability, TKSE safeguards trustworthy preventing malicious data owners from using cloud servers as props throughout the data storage phase. The system's social impact is to ensure data security and protect user privacy. The technology also decreases the expense of data management [15]. It offers message authentication, ensuring the security of data exchange. It also resolves the issue of integrity protection.

2. METHODOLOGY:

2.1. MODULES

- Login
- Registration
- Create Secrete Key
- Authentication Scheme
- Two-Side Verification

2.1.2. Login

Several websites, computer programs, and mobile applications demand a login. Security measures are put in place to guard against unauthorized access to confidential data. Access is denied to the user in the event that a login attempt is unsuccessful (i.e., the entered username and password do not correspond to an existent user account). Many systems stop users from even attempting to log in when they repeatedly fail.

2.1.3 Registration

A registered user is someone who has signed up for an account on a website, piece of software, or other platform in the past. The procedure through which signed-up users provide the system with credentials (such as a username, email address, and password to confirm their identity) is known as logging in. The majority of systems designed for public use enable any user to sign up by simply choosing a register or sign up function and entering these credentials for the first time. Additional rights may be granted to registered users over those given to unregistered users.

2.1.3. Create Secrete Key

Through the application of cryptography, secure communication in the presence of third parties is practiced and explored. The primary goal of cryptography in the past was encryption. When information is encrypted, it is converted from plain text to cypher text. Decryption is carried out backwards. By utilizing encryption, information can be kept secret from all parties except the intended recipients. Encryption and decryption are made possible by the cypher algorithm pair. The algorithm and the key determine how the cypher functions. The secret that communicators know is the solution.

2.1.4. Authentication scheme

It is used to address the difficulty of examining the person's keys (let's say "person B") that someone else ("person A") engages in conversation with or makes an effort to do so. To put it another way, it is the procedure used to ensure that the key held by "person B" belongs to "person A" and vice versa. Although other algorithms disclose the keys at the time of authentication as well, this is often done after the keys have been transferred between the two sides over some secure channel. The easiest way to solve this issue On the other hand, in systems with a sizable user base or in this is not practicable for situations where the users do not directly know one another (like online purchasing). To address this issue, a variety of symmetric key and asymmetric public key techniques are available.

2.1.5. Two-Side Verification

In this module, as shown in below figure 1:

In order to confirm that the person or entity requesting access is who or what they claim to be, two authentication methods must be used sequentially. This procedure is known as two-side verification.

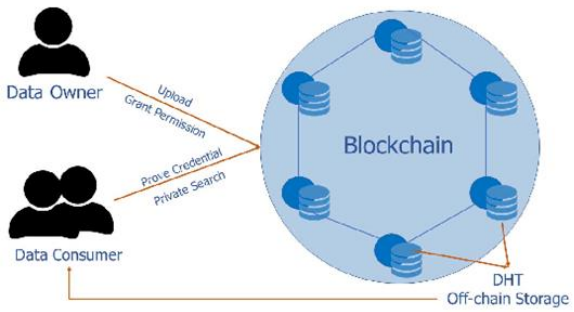

Figure 1: Two side Authentication method

Our performance review demonstrates the efficacy of TKSE and demonstrates its security. The following desirable characteristics best describe TKSE.

• Keyword using the outsourced encrypted data can be searched through by the user. Elliptical Curve Digital Signature Algorithm (ECDSA)-based encrypted data index.

• Verifiability on the user's side. The output script of a joint transaction can have search criteria included in it so that the cloud server can only redeem it if and when using the returned search result as a basis, the output script evaluates to true. TKSE as a result makes user-side verifiability possible and equips the data owner to fight off hostile cloud services.

• Server-side code that is verifiable. Server-side verifiability is accomplished by the cloud server by recognizing fraudulent data owners. Fair Recompense, lack of TTP due to its dependence on hash functions, and block can be used without adding any TTP. Chain allow for a fair payment system in TKSE.

2.1.6 Secure Hashing Algorithm

A 160-bit (20-byte) hash value is produced using the cryptographic hash function of Secure Hash Algorithm 1 (SHA-1). The "messages digest" is the term used to describe this hash value. This message digest frequently produces a 40-digit hexadecimal number. It was created by the US National Security Agency and is a Federal Information Processing Standard. The Java package's Message Digest Class is used to compute cryptographic hashing values security.

Algorithm for Pseudo-Random Number Generator

- Accept a seed or key input number as the first step.
- In step 2 uses that seed to prompt a series of calculations to produce the outcome. The random number is that outcome.
- Use the generated random number as the seed for the subsequent iteration in step three.
- Repeat the procedure in Step 4 to simulate randomness.

3. RESULT AND DISCUSSION:

3.1.1. Existing System

Furthermore, even if the cloud or user is evil, block chain technology. Since Based on digital signature technology offered by TKSE, the encrypted data index, a user can search through Verify that the cloud's search results match your defined criteria by accessing encrypted data. Our analysis the reliability and security of TKSE are demonstrated by its performance and security, making it appropriate for cloud computing. On the basis of our initial SSE technique with additionally, user-side verifiability has attained ide verifiability. Additionally, without adding any TTP, fair payment is accomplished via block chain technologies and hashing. The Drawbacks of Data confidentiality and privacy has been achieved but identity privacy neglected. It has Less safety. It does not include any data.

3.1.2. Proposed System

Because the terms for Searchable encryption techniques have been created in the symmetric key configuration and the user scenario, two examples. And CSP must agree on the search costs' redemption, which calls for the MAC secret key. This prevents the concept from being immediately integrated with block chain technologies. Cryptography hash function server considered a key component is a digital signature is one example of a security application or protocol that uses this aspect of information security. The creation of MAC signature schemes and random number generation are two techniques for safeguarding the integrity of data and authenticating its provenance. Many different applications, such as databases, computer vision, and the storage of passwords, use hashing algorithms. Benefits of the suggested system save money on data management. To protect the confidentiality and security of user data. Code for message authentication and protection of integrity we suggest a reliable The TKSE keyword search method uses encrypted data. It's necessary to involve a third party, to fully handle the aforementioned difficult concerns in cloud computing.

3.1.3 Functional Requirements

It is necessary for the technological requirements of the software products. The functional, performance, and security requirements for particular software systems are included in this phase of the requirement analysis process

[16]. Performance of the system is mostly determined by the high-quality hardware used to run the programmer with the necessary capabilities.

Usability

It explains how user-friendly a system must be. Short or long questions can be asked with ease because the Porter stemming algorithm prompts the user's chosen response [17]-[23].

Robustness

It describes a programmer that operates effectively both in typical and unexpected circumstances. It is the user's capacity to handle execution faults for pointless requests.

Security

Security is the condition of allowing restricted access to resources. Unauthorized users cannot access the system because of the system's strong security measures.

Reliability

It is the likelihood of how frequently the software malfunctions. MTBF is a common unit of measurement (The average time between failures). To ensure that procedures are completed completely and without interruption, the requirement is required. It is capable of supporting any weight, enduring indefinitely, and even overcoming failures.

Compatibility

The version above all web browsers supports it. Any web server, including a local host, can be used to make the system real-time.

Flexibility

The project's adaptability is set up in a way that allows it to function in many surroundings while being used by various users.

Safety

Safety is a precaution done to avoid problems. Each enquiry is handled securely without revealing any personal information to third parties.

3.1.4 Non- Functional Requirements

Portability

The usability of the same software in various settings. Any operating system can be used to run the project.

Performance

The software's adaptability to different settings. The project can be executed on any operating system.

Accuracy

The information is retrieved quickly and with great accuracy thanks to the requesting query. The system offers a high level of security that is both efficient and reliable.

Maintainability

The project is straightforward since it is simple to make updates without compromising its stability. In essence, maintainability refers to how simple it is to maintain the system. It refers to how simple it is to test software, analyze data, make changes, and maintain systems. This project is easily maintainable because new modifications may be made without negatively impacting its stability.

4. CONCLUSION

We propose a system that combines secure utilizing block chain technology and the service provides keyword search capabilities with distributed data storage. The system distributes content to cloud nodes, permits users to submit data in encrypted form, and makes use of cryptographic methods to guarantee data availability. By achieving server-side verifiability, it stops dishonest data owners from using legitimate cloud servers as pawns. Additionally, Block chain technology and hash functions enable the payment Regardless of whether the user or cloud is malicious; search fees can be collected without the involvement of third parties. The results of our analysis of TKSE's effectiveness and security demonstrate that it is both, making it suitable for cloud computing.

REFERENCES:

[1] J. Li, J. Li, X. Chen, C. Jia, and W. Lou, "Identity-based encryption with outsourced revocation in cloud computing," IEEE Transactions on Computers, vol. 64, no. 2, pp. 425–437, 2015

[2] X. Chen, J. Li, X. Huang, J. Ma, and W. Lou, "New publicly verifiable databases with efficient updates," IEEE Transactions on Dependable and Secure Computing, vol. 12, no. 5, pp. 546–556, 2015

[3] H. Li, F. Zhang, J. He, and H. Tian, "A searchable symmetric encryption scheme using block chain, "arXivpreprint, 2017. [Online].Available: https: //arxiv.org/pdf/1711.01030.pdf

[4] H.G.DoandW.K.Ng,"Blockchainbasedsystemforsecuredatastoragewithprivatekeywordsearch,"inServices (SERVICES), 2017IEEEWorld Congress on. IEEE, 2017, pp. 90–93.

[5] R. K. Dhanaraj, L. Krishnasamy, O. Geman and D. R. Izdrui, "Black hole and sink hole attack detection in wireless body area networks," Computers, Materials & Continua, vol. 68, no.2, pp. 1949–1965, 2021. doi:10.32604/cmc.2021.015363

[6] Ramakrishnan, V., Chenniappan, P., Dhanaraj, R. K., Hsu, C.-H., Xiao, Y., & Al-Turjman, F. (2021). Bootstrap aggregative mean shift clustering for big data anti-pattern detection analytics in 5G/6G communication networks. In Computers & Electrical Engineering (Vol. 95, p. 107380). Elsevier BV. https://doi.org/10.1016/j.compeleceng.2021.107380

[7] Chandraprabha, M., & Dhanaraj, R. K. (2020, November 5). Machine learning based Pedantic Analysis of Predictive Algorithms in Crop Yield Management. 2020 4th International Conference on Electronics, Communication and Aerospace Technology (ICECA). 2020 4th International Conference on Electronics, Communication and Aerospace Technology (ICECA). https://doi.org/10.1109/iceca49313.2020.9297544

[8] Sathyamoorthy, M., Kuppusamy, S., Dhanaraj, R.K. et al. Improved K-Means Based Q Learning Algorithm for Optimal Clustering and Node Balancing in WSN. Wireless Pers Commun 122, 2745–2766 (2022). https://doi.org/10.1007/s11277-021-09028-4

[9] Rajesh Kumar D, & ManjupPriya S. (2013, December). Cloud based M-Healthcare emergency using SPOC. 2013 Fifth International Conference on Advanced Computing (ICoAC). 2013 Fifth International Conference on Advanced Computing (ICoAC). https://doi.org/10.1109/icoac.2013.6921965

[10] Rajesh Kumar Dhanaraj, Lalitha Krishnasamy et al Black-Hole Attack Mitigation in Medical Sensor Networks using the Enhanced Gravitational Search Algorithm, International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems. https://doi.org/10.1142/S021848852140016X

[11] Lalitha, K., Kumar, D. R., Poongodi, C., & Arumugam, J. (2021). Healthcare Internet of Things – The Role of Communication Tools and Technologies. In Blockchain, Internet of Things, and Artificial Intelligence (pp. 331–348). Chapman and Hall/CRC. https://doi.org/10.1201/9780429352898-17

[12] Dhanaraj, R. K., Rajkumar, K., & Hariharan, U. (2020). Enterprise IoT Modeling: Supervised, Unsupervised, and Reinforcement Learning. In Business Intelligence for Enterprise Internet of Things (pp. 55–79). Springer International Publishing. https://doi.org/10.1007/978-3-030-44407-5_3

[13] Sathish, R., & Kumar, D. R. (2013, March). Proficient algorithms for replication attack detection in Wireless Sensor Networks—A survey. In 2013 IEEE International Conference ON Emerging Trends in Computing, Communication and Nanotechnology (ICECCN) (pp. 1-7). IEEE.

[14] Sathya, K., & Kumar, D. R. (2012, February). Energy efficient clustering in sensor networks using Cluster Manager. 2012 International Conference on Computing, Communication and Applications. 2012 International Conference on Computing, Communication and Applications (ICCCA). https://doi.org/10.1109/iccca.2012.6179177

[15] Prasanth, T., Gunasekaran, M., & Kumar, D. R. (2018, December). Big data Applications on Health Care. 2018 4th International Conference on Computing Communication and Automation (ICCCA). 2018 4th International Conference on Computing Communication and Automation (ICCCA). https://doi.org/10.1109/ccaa.2018.8777586

[16] Ali, M., Dhanaraj, R.K. (2023). IoT and Blockchain Oriented Gender Determination of Bangladeshi Populations. In: Santosh, K., Goyal, A., Aouada, D., Makkar, A., Chiang, YY., Singh, S.K. (eds) Recent

Trends in Image Processing and Pattern Recognition. RTIP2R 2022. Communications in Computer and Information Science, vol 1704. Springer, Cham. https://doi.org/10.1007/978-3-031-23599-3_25

[17] Rajesh, E., Basheer, S., Dhanaraj, R. K., Yadav, S., Kadry, S., Khan, M. A., Kim, Y. J., & Cha, J.-H. (2022). Machine Learning for Online Automatic Prediction of Common Disease Attributes Using Never-Ending Image Learner. In Diagnostics (Vol. 13, Issue 1, p. 95). MDPI AG. https://doi.org/10.3390/diagnostics13010095

[18] V. Juyal, Nitin Pandey and Ravish Saggar, "Opportunistic message forwarding in self organized cluster based DTN,"" 2017 International Conference on Infocom Technologies and Unmanned Systems (Trends and Future Directions) (ICTUS), Dubai, 2017, pp. 497-502. doi: 10.1109/ICTUS.2017.8286060"

[19] V. Juyal, Nitin Pandey and Ravish Saggar, "Performance comparison of DTN multicasting routing algorithms-opportunities and challenges,"" 2017 International Conference on Intelligent Sustainable Systems (ICISS), Palladam, 2017, pp. 53-57. doi:10.1109/ISS1.2017.8389238"

[20] V. Juyal, Nitin Pandey and Ravish Saggar, "An anatomy on routing in delay tolerant network," 2016 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC), Chennai, 2016, pp. 1-4. doi: 10.1109/ICCIC.2016.7919724

[21] V. Juyal, Nitin Pandey and Ravish Saggar, "A heuristic lightweight security algorithm for resource constrained DTN routing," 2016 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC), Chennai, 2016, pp. 1-4. doi: 10.1109/ICCIC.2016.7919695

[22] V. Juyal, Nitin Pandey and Ravish Saggar, "Impact of varying buffer space for routing protocols in delay tolerant networks," 2016 International Conference on Communication and Signal Processing (ICCSP), Melmaruvathur, 2016, pp. 2152- 2156. doi:10.1109/ICCSP.2016.7754562"

[23] V. Juyal, Ajay Vikram Singh and Ravish Saggar, "Message Multicasting in Near-Real Time Routing for Delay/Disruption Tolerant Network,"" 2015 IEEE International Conference on Computational Intelligence & Communication Technology, Ghaziabad, 2015, pp. 385-390. doi: 10.1109/CICT.2015.79."