INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact Factor: 6.078
(Volume 9, Issue 2 - V9I2-1166)
Available online at: https://www.ijariit.com

Forward secure public key encryption with a keyword search for outsourced cloud storage

B. Venkatesu Goud
venkatesugoud@gmail.com
Annamacharya Institute of Technology and Sciences, Rajampet, Andhra Pradesh

C. Ramadevi
chennaramadevi7@gmail.com
Annamacharya Institute of Technology and Sciences, Rajampet, Andhra Pradesh

C. Naga Jyothi
jyothichalla01@gmail.com
Annamacharya Institute of Technology and Sciences, Rajampet, Andhra Pradesh

B. Lavanya
Bellamlavanya.2002@gmail.com
Annamacharya Institute of Technology and Sciences, Rajampet, Andhra Pradesh

D. Narasimha
narasimhadabbarapalli1704@gmail.com
Annamacharya Institute of Technology and Sciences, Rajampet, Andhra Pradesh

L. Narashimha Reddy
narashimha215@gmail.com
Annamacharya Institute of Technology and Sciences, Rajampet, Andhra Pradesh

ABSTRACT

Cloud computing is a self-driven word that offers information outsourcing services without contention, alleviating customers of the pressures of nearby storage problems. Many industries, such as the military, hospitals, businesses, colleges, and so on, already employ cloud computing to store enormous volumes of data or information. The client may seek permission to view the files or information from the cloud. Generally speaking, there are three types of information: confidential, public, and personal. The infrastructure that stores all of the data on the cloud belongs to someone else. It is never simple to trust outside cloud service suppliers with critical data. Even the largest cloud market players assert that security is a shared responsibility between the customer and the business. The customer should consider how critical it is for the encryption to be robust in order to restrict people from reading data saved in the cloud. One of the many issues that arise from cloud data storage is information security. To solve these problems, numerous algorithms were created. Unfortunately, securing a sizable chunk of the cloud with a single computation or technique is ineffective. By utilising cryptographic techniques, security problems are reduced in this study effort. In addition, networking, server, and storage are all merged so at infrastructure level in cloud computing. This research project suggests employing cryptographic techniques to store data safely in the cloud.

Keywords: *Data Storage, Security, Encryption, And Cloud Computing*

1. INTRODUCTION

The self-motivated term "cloud computing" gives information outsourcing services without debate, relieving the client of the obligations of regional storage issues. Cloud computing is currently employed by many areas, including military, hospitals, business, institutions, and others, to store vast volumes of data or material. Distributed computing is a consequence of the amalgamation of new alternatives inventions that have

developed at varied rates and in various situations. Cloud computing aims to let users reap from all these advancements. Because it allows users to store their data on the cloud and access it at any time from anywhere, the cloud is just being embraced by many organisations. Information invasion is feasible since the cloud collects data from several clients and business partners. They do this by uploading their data to the cloud. Owners of the information hand over ownership of it to a potential security threat. On rare occasions, the cloud service supplier (CSP) will misuse to degrade the data itself.

The categorization, integrity, and accessibility of data are only a few of the significant privacy and security concerns that distributed computing still faces. It is a simple setup to scramble the data before sending it to the cloud. Although this methodology makes certain the data is most surely hidden coming from external clients and cloud executives, it has the disadvantage of making typical content-based calculations meaningless. In this post, we go into information stockpiling security problems and the means to solve them. Because of a number of circumstances, cloud computing inescapably brings new, challenging security concerns in the area of data protection, which has always been a crucial aspect of services.

This method calls for an information verification procedure, however without a clear knowledge of general information, it can be difficult to confirm the proper information. When considering the varied forms of data that each client stores in the cloud and asks of the rendered permanent proof of their information safety, the process of assessing the precision of material stored on cloud storage becomes expressibly more difficult. Its client has the opportunity to regularly update the data saved in the cloud, among other activities like addition, erasure, adjustment, attaching, and recovery. In order to stop data loss from cloud data storage facilities, Innovation needs to be developed further for all of this dynamic activity. Digital photo customers are switching to mobile devices and saving digital photographs in the cloud for ease thanks to the development of edge apps or cloud computing that leverages remote assistance. Yet, security is an oversight in reasonable requests. Cloud cloud is a public environment that is governed by outside parties that are frequently unreliable for data in space. Several image collections, however, like those of clinical photos displaying symptomatic outcomes for various clients, are security-sensitive.

Being sent and kept, these pictures should be safeguarded in this manner. For example, clinical photos or "A thorough research of both the trustworthy testing techniques as in cloud technology," Society of System Scientific Study, v. 9, eds. 1- 30, 2017 are just two examples of valuable materials that are routinely saved in the cloud. photos, and for their inherent qualities and security assurance, these photographs should be encoded. A foundation that integrates knowledge gathering and retention far outside mobile devices is known as "cloud computing." Additionally, The increasing use of the cloud offers a great way to manage a lot of visual data and the appearance of infinite computer resources [1].

As there is no faith there in cloud expert organisation, concerns arise when a file or data point is delivered to

the cloud. Multiple tenures could jeopardise security and cause the loss of sensitive client data [2]. Security in photographic storage and transmission is a growing concern as more people use the cloud. To solve the problem of cloud storage and encoding, a photo compression technique based on CS and an encryption algorithm connected to authentication were developed.

2. LITERATURE REVIEW

ICSCC, vol. 125, pp. 691-697, 6th International Congress on Clever Computing and Communications, 2018. The paper "Exploring data security difficulties and answers in cloud computing" was written by P. Ravi Krishna, P. Herbert Raj, and P. Jelciana.

Cloud computing is one of the computing technologies that is advancing the quickest. Many advantages of cloud computing outweigh the few security issues it raises. This paper addresses its many data security issues that may develop with cloud computing in a multi-tenant environment and offers solutions. cloud computing models, This study also discusses tools utilised for patient care and deployment. A corporation or Cloud Computing could fail as a result of information leakage or corruption damaging the public's trust in those entities. Many companies use cloud computing today, both or in some way, and in the event of a data breach, it will affect both of the service and the business's operations. This is one of the main reasons cloud computing companies are increasing their dedication to data security. both Nima Jafari Navimipour and Matin Chiregi, Quick and simple access to a stock of reconfigurable computing resources is made possible through an unique strategy called "cloud computing." .

With this kind of computing platform, customers cannot judge the reliability of both the cloud service providers. As a result, determining the trust value is one of the most important concerns in this environment so that users may select trustworthy resources. Towards the extent that we know, there aren't many in-depth analyses of the most important tactics in this field. As a result, the state-of-the-art techniques and procedures in this field are thoroughly and in-depthly analysed in this work. We also discuss the two main groups of distributed and centralised trust evaluation techniques utilised in cloud computing.

Also, we talked about the applications of trust, including as surveillance and tracking, and we named trust properties like authenticity, safety, accessibility, stability, predictability, safe, dynamicity, and scalability. A discussion of the variations among the approaches that were taken into account in regard to honesty, security, availability, reliability, health, versatility, secrecy, and scalability is included in this survey article along with recommendations for further research. Practice and Experience in Concurrency and Computing, volume. 31, issue. 2, "Research on secured retrieval over unencrypted data in the cloud," by Vietnam Phan, Jason Triggs, and Mohsen Amini Salehi.

Now, businesses and individuals can use cloud computing to outsourcing personal data into distant yet

conveniently accessible machines. The possibility of cloud storage has not yet been fully realised because of customers' concerns regarding data security and privacy. However, once an information is scrambled, no analysis (such as scanning) could be undertaken here on outsourced data. User-side encryption techniques can be employed to reduce security concerns. Searchable Encryption (SE) techniques have been thoroughly studied in order to enable looking on the data while it is encrypted A Tool For data collection Mechanism for Data Preservation Security in the Cloud, by Sanjay 2017.

These techniques offer varying degrees of security and permit various types if inquiries upon that encrypted data. These techniques have different details and a variety of search kinds, but they all share the same structural elements. We give a complete analysis of several secure search techniques in this work, along with a greater architecture for these systems. as well as a security and performance analysis of these systems. "Identity-based encrypting including search term from lattice assumption," Asia Telecommunications.

This public key encryption technique with search term (PEKS) allows us to search any encryption keys in a public cloud using a keyword, and nobody is able to retrieve the encrypted files without employing the trapdoor that matches to the phrase. Keeping track of massive data storages, like the one in the cloud, is made easier by the PEKS. during management. In order to guard against attacks from quantum computers, we present a matrix identity-based encryption approach with keyword search in this study. We have shown that our approach can achieve both ciphertext indistinguishability and trapdoor security in the arbitrary oracle paradigm. In particular, our method may appoint a sole person to test and give the search results, so it does not need a secure channel.

Our approach represents the initial identity-based encryption technique with matrix assumption keyword search that we are aware of. In order to retain its privacy, important material in a backup system typically must be protected by encryption before being sent to the server. Thus, the issue of how to use search terms for encrypted data has emerged. In 2004, Boneh et al.[1] developed the first technique for keyword scanning unencrypted information stored in a server using a public key encryption scheme. Their work established public key encryption techniques with keyword search as a new arena (PEKS).

Fantastic computational and data storage capabilities are available to customers thanks to cloud computing. There are no limitations or prohibitions on how many users can store different sorts of data in the cloud. A safe cloud-based storage option with a dependable monitoring system that can independently confirm the reliability of information which is outsourced is required for increased security. .

Data is still being sent widely via the Internet and stored in far-off cloud data centres. Using the insecure cloud network, unauthorised users or hackers may have access to the data files. This causes sensitive information to leak or causes data to be lost during network transfer. Thus, cloud security is essential in a cloud environment. Data transit over intercontinental wireless connections must be protected against unauthorised cloud usage.

Even more security precautions should be taken in order to defend both data sets as remote network infrastructure from hacking and other intruders. In this sense, data auditing in conjunction with secrecy, safety, and dynamic capabilities serves as an efficient method for fending off different cloud attacks that is taken into consideration in this work. The success of this project's attempts to safeguard the cloud environment depends on an efficient auditor.

3. EXISTING SYSTEM

Several systems available today can either offer allusion person re or attribute-based searching capabilities. identification-based encryption with an equality test (IBEET). Attacks using chosen ciphertext and chosen identity are prevented. Identity-based encryption and concurrent keyword search (IBECKS). Both searching and multi-keyword encryption are supported by this technology. a PHR system with several authorities that uses attribute-based encryption to safeguard user privacy (ABE), It makes swift revocation and detailed access control possible. This innate quality encryption (ABE) technology was used to develop an allusion keyword search engine with a successful revocation approach (AKSER). The issue is that the software is stationary and cannot support a multi-keyword search.

4. PROPOSED SYSTEM

The research on several cloud-based solutions for secure lexicon searching and data transmission is briefly summarised in this project. Encryption is the essential technique for safeguarding the confidentiality of sensitive data. Despite still, there are some significant challenges, such as carrying out safe data searches and sending data through encrypted channels. Many application frameworks and encryption techniques are available. Several of them efficiently do both searching and sharing operations.

5. ALGORITHM

AES ALGORITHM

The most popular and widely utilised symmetric encryption technique that is most likely utilized nowadays is the Strong Encryption Standard (AES). It can be detected at no fewer than six times faster than triple DES. A successor was needed since DES's key length was insufficient. It was believed that as processing power rose, it would be susceptible to a thorough key search attack. Triple DES was developed to solve this problem, however it was found to be slow.

The attributes of AES are as follows:

- More powerful and rapid than Triple-DES
- symmetric block cypher with a symmetric key, 128-bit data, and 128/192/256-bit keys
- Detailed specification and design information
- Software that can be implemented in both C and Java.
-

HOW AES IS USED

AES is iterative in opposition to a Feistel cypher. A "substitution-permutation network" is used to construct

it. It consists of several interrelated processes, some of which involves substituting certain inputs for specific outputs (substitutions), and others of which involve shifting bits about (permutations). It's interesting to notice that AES does all calculations using bytes, not bits. As a result, AES treats a plain block's 64 bits as 16 bytes. . Those 16 bytes are organized as a matrix with four columns and four rows for use during processing. In contrast to DES, the round count in AES might vary and is determined by the key length. AES uses 10, 12, or 14 rounds for 128-bit keys, and 12 or 14 rounds for 192- or 256-bit keys.

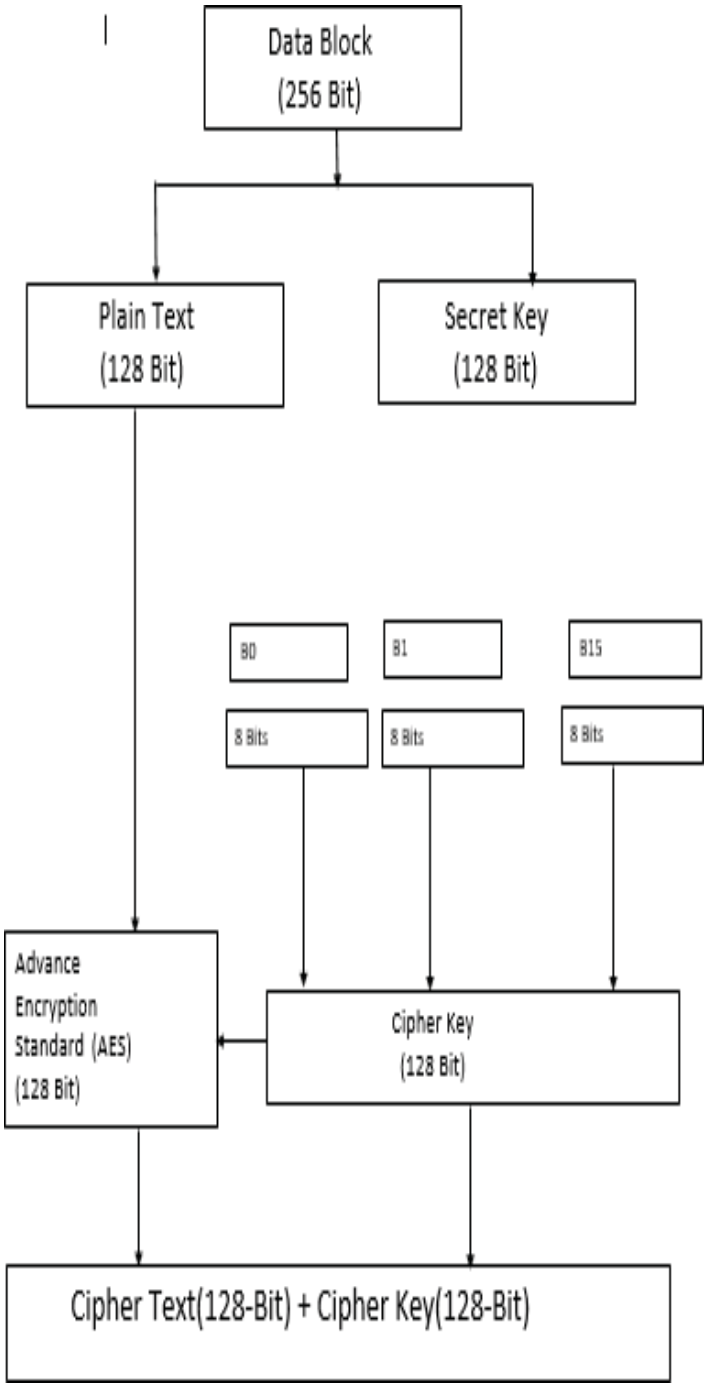

Figure 1: Encryption process for storing data.

Encryption is one thing, decoding is another. Data for the encryption is split into two 128-bit segments for

each segment. The left halves of the 128-bit chunk was provided to the AES algorithm in hopes of restoring the texts in plain text, and the right half was given to the Feistel algorithm in hopes of restoring the key. Key and plain text are merged after this operation and given to the designated customer as production or output information.

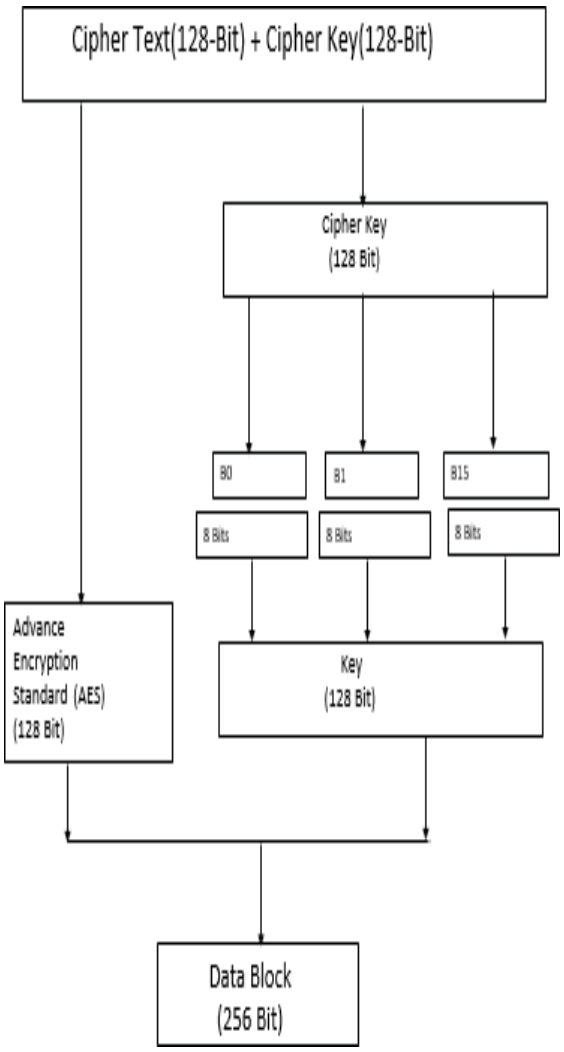

Figure 2: Decryption process for retrieving data

6. CONCLUSION

Cloud computing is swiftly becoming into a crucial and useful computing paradigm for consumers due to its wide range of services, notably for data storage. Cloud services provide users with on-demand services and unrestricted data storage space. Anyone ought to select the cloud in the present era to store their crucial data. Nonetheless, it is necessary to store sensitive data in a secure manner. In this article, we've covered a few cloud computing-related problems from various data processing perspectives. The security and privacy with the cloud are its main drawbacks. As a result, encryption is the primary technique used to protect sensitive data. Making data access and search activities over encrypted data secure is a contemporary challenge.

7. REFERENCES

[1] P. Ravi Kumar, P. Herbert Raj, and P. Jelciana, "Exploring data security issues and solutions in cloud computing," 6th International Conference on Smart Computing and Communications, ICSCC, vol. 125, pp.691- 697, 2018.

[2] Matin Chiregi, and Nima Jafari Navimipour, "A comprehensive study ofthe trust evaluation mechanisms in the cloud computing," Journal of Service ScienceResearch, vol. 9, pp. 1- 30, 2017.

[3] Hoang Pham, Jason Woodworth, and Mohsen Amini Salehi, "Survey on secure search overencrypted data on the cloud," Concurrency andComputation Practice and Experience, vol. 31, no. 2, 2019, DOI: 10.1002/cpe.5284.

[4] L. Wu,Y. Zhang, K.-K.R. Choo, and D. He, "Efficientand secure identity-based encryption scheme with equality test in cloud computing," Future Generation Computer Systems, Vol. 73, pp. 22-31, 2016. [5] Yang Lu, Gang Wang, Jiguo Li, and Jian Shen, "Efficient designated server identify based encryption with conjunctive keyboard search," Annals of Telecommunications, vol. 72, pp. 359-370, 2017.

[6] Xiaojun Zhang, Chuxiang Xu, Liming Mu, and Jie Zhao, "Identity-based encryption with keyword search from lattice assumption,"China Communications, vol. 15, no. 4, pp. 164-178, IEEE, 2018.

[7] Huiling Qian, Jiguo Li,Yichen Zhang, and Jinguang Han, " Privacypreserving personal health record usingmulti-authority attribute-based encryption withrevocation," International Journal of Information Security, vol. 14, pp. 487-497, Springer, 2015.

[8] Jin Li, Yinghui Zhang, Xiaofeng Chen, and Yang Xiang, "Secure attribute-based data sharing for resource- limited users in cloud computing," Computers and Security, vol. 72, pp. 1-12, 2017.

[9] Jie Cui, Han Zhou, Hong Zhong, and Yan Xu,"AKSER: Attribute-based keyword search withefficient revocation in cloud computing," Information Sciences, vol. 423, pp. 343-352, 2017.

[10] Baishuang Hu, Qin Liu, Xuhui Liu, Tao Peng, Guojun Wang, and Jie Wu, "DABKS: Dynamic attribute-based keyword search in cloud computing," 2017 IEEE International Conference on Computations (ICC), IEEE, 2017.

[11]Viswanath, G., &Krishna, P. V. (2020). Hybrid encryption framework for securing big data storage in multi-cloud environment. EvolutionaryIntelligence, 1-8.

[12]Li, H., Yu, C., & Wang, X. (2020). A novel1D chaotic system for image encryption,authentication and compression in cloud. Multimedia Tools and Applications, 1-38.

[13]Rad, P., Muppidi, M., Jaimes, A. S., Agaian, S. S., & Jamshidi, M. (2015, April). Anovel image encryption method to reduce decryption execution time in cloud. In 2015 Annual IEEE Systems Conference (SysCon)Proceedings (pp. 478-482). IEEE.

[14]Boopathy, D., & Sundaresan, M. (2019). Anovel multi-dimensional encryption technique to secure the grayscale images and color images in public cloud storage. Innovations in Systemsand Software Engineering, 15(1), 43-64.

[15]Vandana, R., Raj, L. B., & Kumar, B. J. (2020). Information Integrity and Authentication over Cloud Using Cryptographic Techniques. European Journal of Molecular & Clinical Medicine, 7(2), 5227- 5235.

[16]Garg, P., Sharma, M., Agrawal, S., &Kumar, Y. (2019). Security on cloud computingusing split algorithm along with cryptography and steganography. In International Conferenceon Innovative Computing and Communications(pp. 71-79). Springer, Singapore.

[17]Muthurajkumar, S., Vijayalakshmi, M., & Kannan, A. (2017). Secured data storage and retrieval algorithm using map reduce techniques and chaining encryption in cloud databases. Wireless Personal Communications,96(4), 5621-5633.

[18]Bala, B., Kamboj, L., & Luthra, P. (2018).SECURE FILE STORAGE IN CLOUD COMPUTING USING HYBRID CRYPTOGRAPHY ALGORITHM.International Journal of Advanced Research in Computer Science, 9(2).

[19]Hidayat, T., & Mahardiko, R. (2020). A Systematic literature review method on aes algorithm for data sharing encryption on cloud computing. International Journal of Artificial Intelligence Research, 4(1), 49-57.

[20]Rawal, B. S. (2020). Proxy re-encryption architect for storing and sharing of cloud contents. International Journal of Parallel, Emergent and Distributed Systems, 35(3), 219-235.[21]Awan, I. A., Shiraz, M., Hashmi, M. U.,Shaheen, Q., Akhtar, R., & Ditta, A. (2020).

