International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249 – 8958 (Online), Volume-9 Issue-4, April 2020

Data Security in Cloud Computing using Three Way Mechanism

A.Vijayaraj, Irene John Ukken, Karunya.S, Sathish Raj.G

Abstract : Cloud computing is the front line innovation of the decennium. It empowers users to store enormous collection of information in distributed storage and make use of it as and when they please from any corner of the world, with any sorts of hardware. As this distributive computing is reliant on the internet facility, issues of security like privacy, security of information, authentication and data confidentiality is experienced. So as to dispose of these issues, an assortment of encryption calculations and systems are utilized. Numerous specialists pick what they discovered best and made use of these in different blends to give the security to the information in cloud. Going through a comparable circumstance, we have decided to utilize a mix of validation system and key trade calculation mixed with an encryption calculation. The blend is alluded to as a "Three way mechanism" since it guarantees all three of confirmation, information protection and inspection insurance policies. In this paper, we have proposed to utilize two-factor authentication mixed in (AES) Advanced Encryption Standard encryption calculation that secures the secrecy of information put away within cloud. Without user's private key that is special to the user, even if the key that is moving is stolen or hijacked the feature of key exchange renders it pointless and is of no use. The given proposed engineering of three way mechanism making it tedious for unauthorized personnel to break this security framework, therefore securing information put away in cloud.

Keywords: Cloud computing, Two-factor authentication, Three way mechanism, AES Encryption, Data confidentiality.

I. INTRODUCTION

The quickly rising number of digital exchanges has produced E-commerce big data. As progressively various information records are being put away locally in enterprises, the weight on nearby information stockpiling frameworks increases exponentially. Localized equipment malfunctioning leads to extreme damages or information being misplaced, which significantly influences the everyday activities of the enterprises. Luckily, cloud storage solutions appeared under such conditions.

Revised Manuscript Received on April 17, 2020.
* Correspondence Author
Dr.A.Vijayaraj*, Associate Professor, Department of Information Technology, Sri Shakthi Institute of Engineering and Technology, Coimbatore. Tamilnadu, India India satturvijay@gmail.com
Irene John Ukken, Department of Information Technology, Sri Shakthi Institute of Engineering and Technology, Coimbatore, Tamilnadu, Indiairene29997@gmail.com
Karunya.S, Department of Information Technology, Sri Shakthi Institute of Engineering and Technology, Coimbatore, Tamilnadu, Indiakarunya99shiva@gmail.com
Sathish Raj.G, Department of Information Technology, Sri Shakthi Institute of Engineering and Technology, Coimbatore, Tamilnadu, sathishwv7@gmail.com

Cloud computing can gather and sort out an enormous number of various kinds of storage hardware by different means and methods, for example by clustering applications, networking technology and distributive document frameworks.There has already been various common services provide by cloud items at home and abroad, for example, App Engine, Amazon Web Services, I Cloud and Microsoft Azure. As a lot of information are given off to distributed servers, the requirement for Data Managers to scramble the previously mentioned secondary and tertiary sorts of delicate information makes conventional plain content based information searching no longer reasonable. Also, limited by the network transmission capacity and conventional storage constraints, users face the difficulty to download all the information again to a localized storage medium and later describable it for use.

Specifically, we first structure the MYASP Cloud which is a validated list on the most well-known property (i.e., Price) of CSMs, and propose the relating verification protocol. Then, we stretch out the cloud-tree to the MyASP Cloud-tree by incorporating a multi-dimensional index method (i.e., iDistance) with Cloud-tree, to additionally improve the determination quality to diminish the process of verification trouble at the customer side. Our methodologies are demonstrated to guarantee genuineness, satisfiability and completeness of the chosen outcomes.

We have additionally tentatively contrasted our methodologies and the latest related work, and the outcomes show huge enhancements over the best in class. The novel index structure is the centre segment of the Cloud Service Selection Verification (CSSV) method, which makes use of the possibility of "partition of tasks" to promise solid security capabilities. In the precise manner, we present a trusted authority in the cloud based commission framework that isolates the errand of CSM data assortment from the administration selection. The authority doesn't straightforwardly collaborate with the cloud customers and is just accountable for collating the data from the CSMs, and thus it very well may be progressively committed into receiving modern barrier to sift through dangerous data and building a confirmed database of CSMs' profiles.

II. RELATED WORKS

Ren et al [1] proposed in his book the Security challenges for the public cloud that Cloud computing is the most energizing computer paradigm in perspective in data technology. Be that as it may, security and protection are seen as essential hindrances to its wide acceptance. S. Kamara and K. Lauter [2]

proposed their work Cryptographic distributed storage in Financial Cryptography and Data Security considered the issue of establishing a protected distributed storage administration on a public cloud foundation where the feature provider can't trusted by the user. D.Boneh et.al [3] presented a Public key encryption with catchphrase search proposed that the issue of looking for information that is encoded utilizing a public key framework. For instance, consider a mail server that collects different messages open to the public encoded for an individual. Making use of their component the particular individual will be sending the mail server a key helping the server to distinguish all messages containing some particular catchphrase, yet not deducing anything else. The introduction the idea of open key encryption with catchphrase search paved the way for new development. O.Goldreich, Oded and Rafail Ostrovsky [4] proposed the Software Protection and Simulation on Oblivious RAMS recommended that one of the most significant issues concerning PC practice is Software Protection. There exist numerous heuristics and impromptu strategies for assurance, however the issue in general has not gotten the hypothetical treatment it merits. Thereby providing only a hypothetical protection. Boneh et al [5] took into consideration the Public key encryption that permits PIR inquiries that accompanies the underlying issue: An individual A wishes to store her email utilizing a storage-supplier B, (for example, HotMail email service provider or on the other hand Yahoo).This gave a hypothetical answer for on "Public- key Encryption with Keyword Search." presented by Boneh, DiCrescenzo, Ostrovsky and Persiano. The baseline method of their response in addition took into consideration of a Single-Database PIR composition with sub linear correspondence unpredictability that was considered with utmost intrigue. C.Gentry [6] clarified a completely homomorphic encryption scheme tackling a previous open issue, they proposed the first complete homomorphic encryption scheme. Such a plan permits one to process discretionary capacities over scrambled information without the use of a decryption key. Somani uma et al. [7] upheld the actualization of digital signature with RSA algorithm and upgrading the security of data in cloud computing which meant it paved a way to give the desirable solution for everyday computing. The persistent problem that comes with cloud computing is obviously the security of cloud and the exact execution of cloud over the network on which right now they attempted surveying cloud storage methodology and Data Security in cloud with the processing of digital mark with RSA algorithm.

Rewagad et al [8] proposed to improve information security in distributed computing to with the usage of digital signature with the help of and an encryption calculation. They then said that with distributed computing, associations can utilize services and information is put away at any physical area that is out of their reach. The proposed feature brought up the different security issues like protection, privacy, honesty prompted trusting the computing, with the requirement of a framework which performed validation, checked and encoded information transfer, which maintained the information classification.

Potey,Deepak H. Sharma et al. [9] clarified the homomorphic encryption for security of cloud information and proposed completely utilizing homomorphic encryption which enabled putting away information on the cloud of the organization. The information is put away in Dynamo DB of Amazon Web Service (AWS) open platform. Computations for users are performed on encrypted information in open cloud. As and when information is required they can be downloaded on customer desktop. Current scope implements that the user's data is never saved in plaintext format on the common cloud. Singh, Ajit, and Rimple Gilhotra [10] proposed their work in information security utilized efficiently the arithmetic coding technique and has the suggestion that the present users depend not only on security yet in addition the speed of correspondence and amountof content. Right now, an idea has been proposed which utilizes the idea of compression and information encryption. Tirthani, Neha et al [11] incited the information Security in Cloud Architecture dependent on Diffie Hellman and Elliptical Curve Cryptography they utilized encryption technique, which is the mixture of linear and elliptical cryptography techniques. It has three security checkpoints: user confirmation, key generation and encryption of information. Kaaniche et al [12] introduced an information security and privacy safeguarding in distributed storage conditions dependent on cryptographic technique and gave the suggestion that the main goal of this overview is to give the predictable view about the two information security concerns and security issues that is very much anticipated by customers in distributed environments. Lee, Bih-Hwang et al [13] utilized AES under HEROKU surveyed the information security in distributed computing proposed that the cloud platform makes use of third-party information model. A case of cloud stage as a help (PaaS) is Heroku .The performance assessment shows that AES cryptography can be utilized for information security. On the other hand postpone computation of information encryption showed that bigger the size of information, it increases exponentially the information defer time for encrypting information. Khan [15] utilized cryptographic calculation and said that the most significant matter within cloud is security and how cloud supplier guarantees it. Securing the cloud implies securing the fixes, examining diverse security issues imposed to cloud and distinctive cryptographic calculations that can be adopted.

R Srinivasan & A Vijayaraj[14] suggested the new approaches purely based on the integrated Programming develop to creating the optimized FSO communication equipment construction to better the link accessibility and higher data rate, and also advised the allotment of limited bandwidth. Hemalatha, S, and R. Manickachezian [16] proposed the security strength and said that cloud computation is the most thought provoking computing difference in information technology. Throughout the network security and protection is perceived as mandatory obstructions in its acceptance all over. Here, the creator's got everyone thinking of the couple of the very naïve security challenges and ignited the fire of inspiration for further examination of security answers within a dependable public cloud condition.

III. EXISTING WORK

Cloud administrations offer a versatile assortment of extra room and registering capacities that are generally

utilized by exponentially increasing number of entrepreneurs which brought about an enormous number of Cloud Server Managers (CSMs). The accessibility of different alternatives made it hard for potential cloud customers to gauge and choose which choices suit their prerequisites and conditons. The difficulties are twofold: Difficulty is faced to assemble all the CSMs data accessible by cloud customers. It is likewise computationally costly to pick a best and appropriate CSM from an enormous CSM pool. The pre-existing techniques are centred distinctly around how to choose the administrations that fulfil user's needs and none of them considers security issues engaged with the administrative choice. As a lot of information are re-appropriated to distributed storage servers, the requirement for information proprietors to decrypt the secondary and tertiary sorts of delicate information making conventional normal content based information searching arrangements no longer reasonable. Also, limited by the systems transfer speed and local stockpiling, clients think that it's difficult to gather all the information again by re-downloading them into a nearby physical disk and afterwards decoding them for use.

Disadvantages

• Data at risk of being intercepted by unauthorized personnel
• Leak the privacy of users within cloud storage environment
• Difficult to address the demands of performance, system usability and scalability.

IV. PROPOSED WORK

In this proposed approach, our main focus revolves around the secondary and tertiary sort of information and structure a safe and effective information searching system of procedure. For ease of understanding, a down to earth foundation is introduced as follows. Initially it is expectant that every item has an interesting identifier in the entire organization and a point by point portrayal record. The record incorporates the entirety of the nitty gritty data of the item, for example, the design stream, structure standard, item highlights and market position. All of us know, releasing the item to the market sooner than the contender can increase the market value rapidly and is of more advantage to the organization extensively. Consequently, the entire data is meant to be kept from the contenders and unauthorized personnel in general, taking into account that the items are time-delicate. With the development of the organization, item data likewise increases exponentially as well. To improve the soundness and unwavering quality of an information storage framework, an instinctive plan is moving the nearby information into cloud. As a promising Information Technology (IT) framework, distributed computing is generally regarded as one due to its incredible usefulness. It can gather and rearrange colossal assets of capacity, registering and apply, implying that the clients can get to the IT benefits in an adaptable, pervasive, monetary and on-request method. An ongoing challenge is the way to ensure the privacy of the information while keeping up its search capability, plan an encoded product data recovery framework. These plans defend the user's very own information yet empower the server to come back to the objective encoded document as per the inquiry demand. Apart from this, we can give the assurance of the security of client information and protection while making sure not to decrease the efficiency in querying.

Methodologies

In this section we are going to explain basic functionality of AES encryption Algorithm and two factor authentication.

A. AES encryption Algorithm

AES is the monotonous approach with respect to the Feistel figure. It finds dependency with 'substitution and permutation technique'. AES calculations are based entirely on bytes rather than bits. Thereby treating the 128 bits of the given plain text as 16 bytes. These 16 bytes are orchestrated in four chunks and rows for being handled as a matrix

The below fig. depicts a common round of AES encryption. Each round includes four sub-processes.

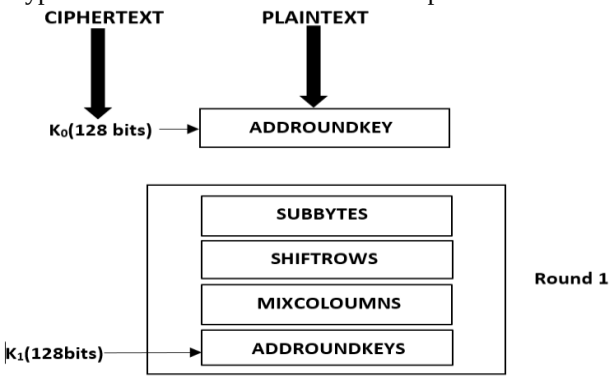

Fig:1 AES encryption round process

Byte Substitution (Sub Bytes) The 16 input bytes are substituted by going through fixed index table (S-box) that is mentioned in the figure. The outcome is in the format of four lines and four sections or more commonly known as a matrix

Shift-rows- Each row of the matrix is then shifted to the left one after the other. Any shift that results in a 'tumble off' are inserted again on the right hand side of the sequence of rows. Move is completed as follows.

- The first row does not shift.
- The next row gets shifted by one position towards the left.
- The row after the second one is shifted two positions in the same direction
- Similarly, the last one is moved three positions to the left.
- The end result is of a new matrix with the same 16 bytes but shifted among one another.

Mix-Columns- Every chunk of four bytes is then changed making use of a unique mathematical function. The function and gives four totally new bytes from four bytes of one column, which replaces the original segment. The outcome is another new network comprising of 16 new bytes which was not performed in previous round.

Add round key- The conclusion matrix is now taken into consideration as 128 bits which is then XOR ed to the 128 bits of the round key. If it adds up to or makes up the last and final round, at that point the output is the ciphered text. Or else another similar round is initiated

Decryption Process- The procedure behind decryption of the received cipher text involves the system of procedure finds similarity in the encryption order process but conducted in the reversed way.

- Adding the round key
- Mixing the columns
- Shifting the rows to the right
- Performing byte substitution

As the decryption system of procedure occurs in a reverse manner, unlike of that occurs in Feistel Cipher, both encryption and decryption processes are in the requirement to be performed separately even though there are striking similarities between the two.

B. Two Factor Authentication

User login remote system with the user id and password. Upon receiving the user id and password the cloud server check for authentication if the given user id and passwords are valid. Then for two factor authentication the received private key in the email along with the encrypted data is used to decrypt the message that has been sent.

System Architecture

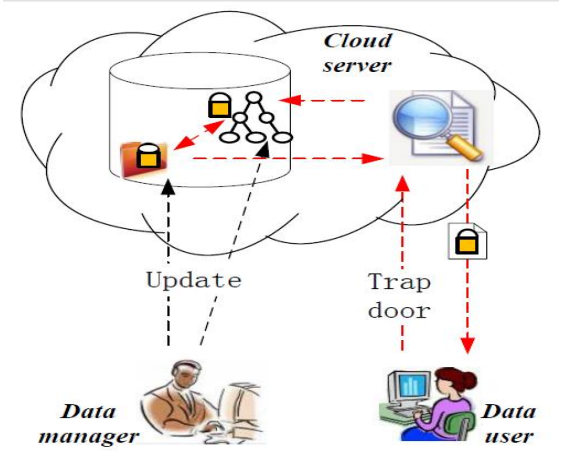

Fig: 2 Architecture of Hybrid Cryptography

The cloud serves as the main storage medium where data that is to be sent is stored in encrypted form using the AES encryption algorithm and the two factor authentication is achieved using public key and private key. The cipher text of both the user's data and the private key are stored in the cloud. To decrypt the cipher text the private key that is generated randomly is used along with the public key and the deciphered text is obtained.

Here the user's data is taken into account for storage and retrieval of the data from the cloud using the hybrid algorithms (AES and Two factor authentication).The process takes place here is

1. Upload process
2. Download process

Upload process

The data that is being sent or uploaded is plain text, the admin will specify the mail address and enter the plain text that is to be directly encrypted and also generate the public key on one hand. On the other hand, the process that is done for user registering is also undertaken by the admin, thereby specifying or limiting access to the cloud to certain individuals. The registered credentials are then given to the user to access their part of the database. The mail is then sent to user who the encrypted data is meant to along with randomly generated private key which is accessible by the user.

Download process

The user downloads cipher text C from the cloud, along with the private key and logs in using the credentials that were provided by the admin .The user then decrypt the cipher text that was received with help of the private key, cipher text data C is decrypt with AES algorithm.

Implementation

To implement the proposed method the operating system used is Windows 10 and Java 1.8 for the front end, as it is free and platform independent. For the storage purpose i.e for the database MySQL is used which is the commonly used database as it is free and code can be available in public domain .The IDE used here is Eclipse IDE which is the open source and used for java Desktop applications and the cloud server is Apache Tomcat Server 8.0.27.0 as it is open source and implements Java server pages and java servlets.

V. RESULT AND DISCUSSIONS

The below fig 3. displays how the plain text is encrypted to give a cypher text and the key is generated using the hybrid algorithm(AES and two factor authentication).This is then sent to the user that receives it cipher text along with the private key.

Fig: 3 Encryption Screen

Fig: 4 Mail that is received at the user end

The fig.4 depicted shows the cipher text that was generated along with the private key.

Fig: 5 Decryption Screen

The above fig.5 shows the decryption of the cipher text that was received along with the private key in the user's email to get the original message.

VI. CONCLUSION AND FUTURE ENHANCEMENT

The sheer accessibility of data is one of the advantages of using cloud computing. Cloud's disadvantages are the lack of greater protection and privacy. The insider threat is more serious indeed and, on the rise, worldwide. Each and every one of them that are working under an establishment have the ease of access to cloud storage. This means that any unhappy employee that is seeking ways to can inflict heavy damages on your organization can do so hereafter. Therefore all growing companies will be looking forward to having data communicated among the peers in a confidential manner. Our project proposes this idea by ensuring the data is encrypted while being sent from the admin side which can only be decrypted by the receiver if he or she has both the private and the public key.

Currently our scope is limited only to a one to one communication. This can be increased for an organization when they own their own cloud platform and can include multiple employees in the message By increasing the number of encrypted messages being sent to a wider audience, an added feature of including documents or pictures can be embedded.

REFERENCES

1. Ren, Kui, Cong Wang, and Qian Wang. Security challenges for the public cloud. IEEE Internet Computing 16, no. 1 , Pp:69-73, 2012.
2. Kamara, Seny, and Kristin Lauter. Cryptographic cloud storage.In International Conference on Financial Cryptography and Data Security, pp. 136-149. Springer,Berlin, Heidelberg, 2010.
3. D.Boneh, Dan, Giovanni Di Crescenzo, Rafail Ostrovsky, and Giuseppe Persiano. Public key encryption with keyword search. In International conference on the theory and applications of cryptographic techniques, pp. 506-522. Springer, Berlin, Heidelberg, 2004.
4. Goldreich, Oded & Rafail Ostrovsky. Software protection and simulation on oblivious RAMs. Journal of the ACM (JACM) 43, no. 3, Pp:431-473, 1996.
5. Boneh, Dan, Eyal Kushilevitz, Rafail Ostrovsky, and William E. Skeith.Public key encryption that allows PIR queries. In Annual International Cryptology Conference, Pp. 50-67. Springer, Berlin, Heidelberg, 2007.
6. C.Gentry, Craig, and Dan Boneh. A fully homomorphic encryption scheme. Vol. 20, no. 9. Stanford: Stanford University, 2009. Encryption scheme - C. Gentry - 2009
7. Somani, Uma, Kanika Lakhani, and Manish Mundra. Implementing digital signature with RSA encryption algorithm to enhance the Data Security of cloud in Cloud Computing. In 2010 First International Conference On Parallel, Distributed and Grid Computing (PDGC 2010), pp. 211-216. IEEE, 2010.
8. Rewagad, Prashant, and Yogita Pawar. Use of digital signature with diffie hellman key exchange and AES encryption algorithm to enhance data security in cloud computing. In 2013 International Conference on Communication Systems and Network Technologies, pp. 437-439. IEEE, 2013.
9. Potey, Manish M., Chandrashekhar A. Dhote, and Deepak H. Sharma. Homomorphic encryption for security of cloud data Procedia Computer Science 79, no. pp: 175-181, 2016.
10. Singh, Ajit, and Rimple Gilhotra. Data security using private key encryption system based on arithmetic coding. International Journal of Network Security. Its Applications (IJNSA) 3, no. 3: Pp: 58-67, 2011.
11. Tirthani, Neha, and R. Ganesan. Data Security in Cloud Architecture Based on Diffie Hellman and Elliptical Curve Cryptography IACR Cryptology ePrint Archive Pp:49-56, 2014.
12. Kaaniche, Nesrine, and Maryline Laurent. Data security and privacy preservation in cloud storage environments based on cryptographic mechanisms. Computer Communications, Pp: 120-141, 2017.
13. Lee, Bih-Hwang, Ervin Kusuma Dewi, and Muhammad Farid Wajdi. Data security in cloud computing using AES under HEROKU cloud. In 2018 27th Wireless and Optical Communication Conference (WOCC), Pp. 1-5. IEEE, 2018.
14. R Srinivasan & A Vijayaraj " Mobile communication implementation techniques to improve last mile high speed fso communication", Trends in Network and Communications- Springer, Berlin, Heidelberg Pp:55-63 , 2011.
15. Khan, Shakeeba S., & R.R. Tuteja. Security in cloud computing using cryptographic algorithms. International Journal of Innovative Research in Computer and Communication Engineering 3, no. 1, Pp: 148-155, 2015.
16. Hemalatha, S., & R. Manickachezian. Security Strength of RSA and Attribute Based Encryption for Data Security in Cloud Computing. International Journal of Innovative Research in Computer and Communication Engineering 2, no. 9, 2014.

AUTHORS PROFILE

Dr.A.Vijayaraj is an Associate Professor; Department of Information Technology, Sri Shakthi Institute of Engineering and Technology Coimbatore from January 2019. He has completed Master of Engineering in Computer Science and Engineering from Sathyabama University in 2005 and graduated PhD in Computer Science and Engineering from Anna University in 2019. His area of specialization is Networks and Communication,Operating Systems, Mobile Computing, Information Retrieval, Knowledge Management. He has 20 years of teaching experience from various Engineering Colleges. During tenure he was Awarded Best Teacher Award thrice. He is a Member of CSI, ISTE, IAENG, ICST, UACEE, IASTER and CSTA. He organized number of Workshops, Faculty development programs, Seminars, National and International Conferences. He has Published 30 papers in various reputed International journals and 10 Papers in IEEE International Conferences 10 papers National Level conferences. He has published 2 books and one patent.

Irene John Ukken is currently pursuing her Bachelor degree in B.Tech Information Technology, Sri Shakthi Institute of Engineering and Technology, Coimbatore, Tamilnadu, India.

S. Karunya is currently pursuing her Bachelor degree in B.Tech Information Technology, Sri Shakthi Institute of Engineering and Technology, Coimbatore, Tamilnadu, India.

G.Sathish Raj is currently pursuing his Bachelor degree in B.Tech Information Technology, Sri Shakthi Institute of Engineering and Technology, Coimbatore, Tamilnadu, India.