RESEARCH ARTICLE

SAMRIDDHI Volume 14, Special Issue 2, 2022 Print ISSN : 2229-7111 Online ISSN : 2454-5767

Data Storage Security in Cloud Computing Using Aes Algorithm and Md5 Algorithm

Anil Kumar J Kadam[1*], Vaibhav Varma[2], Sonal Patil[3], Mohit Patil[4], Madhuri Patil[5]

[1*-5] Department of Computer Engineering, College Name- AISSMS COE, Pune, India, e-mail : ajkadam@aissmscoe.com

ABSTRACT

The most intriguing computing paradigm shift in information technology today is cloud computing. However, security and privacy are seen as major roadblocks to widespread adoption. The authors present a list of important security concerns and encourage more research into security solutions for a secure public cloud environment. Cloud computing is a new term for a long- awaited technology. Computing as a utility is a vision. The cloud gives on-demand network access to a centralised pool of programmable computing resources that may be deployed quickly and effectively as well as little management overhead

Keywords: Cloud Computing, Security, AES Algorithm, MD5 Algorithm.

SAMRIDDHI:AJournalofPhysicalSciences,EngineeringandTechnology,(2022);DOI:10.18090/samriddhi.v14spli02.17

INTRODUCTION

Since its beginnings, cloud computing has been used by billions of users all over the world as an innovation and final solution for utility and distributed computing on Web applications. Its use and impact are felt in a variety of industries, disciplines, and businesses all around the world. Nonetheless, cloud computing has encountered some challenges; the purpose of this research is to identify the factors impacting performance and provide some remedies or advice to cloud users who may encounter performance issues:

1. Information integrity and protection in the cloud domain, as opposed to the traditional approach to information storage.
2. The ability to transform data from a variety of sources into intelligence and deliver it to the appropriate individuals and systems.
3. When several users access the cloud service, load balancing and traffic control are required.
4. Large-scale data, high-performance computing, automation, response speed, rapid prototyping, and rapid time to production are all issues that must be addressed.
5. End-users of cloud services have concerns about security, privacy, and trust.
6. Using the cloud as a platform to help create a more dynamic business intelligence environment.

Corresponding Author: Anil Kumar JKadam, Department of Computer Engineering, College Name- AISSMS COE, Pune, India, e-mail : ajkadam@aissmscoe.com

How to cite this article : Kadam, A.K.J., Varma, V., Patil. S., Patil, M., Patil, M. (2022). Data Storage Security in Cloud Computing Using Aes Algorithm and Md5 Algorithm.

SAMRIDDHI : A Journalof Physical Sciences, Engineering and Technology, Volume 14, Special Issue (2), 296-300.

Source of support : Nil

Conflict of interest : None

LITERATURE SURVEY

1. Paper Name : Security Challenges for the Public CloudAuthor : Kui Ren, Cong Wang, and Qian Wang

   Description : The most intriguing computing paradigm shift in information technology today is cloud computing. However, security and privacy are seenas major roadblocksto widespreadadoption. The authors present a number of significant security

concerns and encourage more research into security solutions for a secure public cloud environment.

2. Paper Name: Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data

Author : Vipul Goyal Omkant Pandey Amit Sahai Brent Waters§

Description : As more sensitive data is exchanged and stored on the Internet by third-party sites, the demand to encrypt data saved on these sites will grow. One disadvantage of encrypting data is that it can only be communicated in a coarse-grained manner (i.e., giving another party your private key). We create Key-Policy Attribute-Based Encryption, a new cryptosystem for fine-grained sharing of encrypted data (KPABE). Ciphertexts are labelled with sets of attributes in our cryptosystem, and private keys are linked to access structures that control which ciphertexts a user can decipher. We show how our design can be used to share audit-log data and encryptbroadcast data. Hierarchical Identity-Based Encryption is subsumed by our structure, which allows delegation of private keys (HIBE).

3. Paper Name: Ciphertext-Policy Attribute-Based Encryption: An Expressive, Efficient, and Provably Secure Realization Author: Brent Waters

Description: A new way for realising Ciphertext-Policy Attribute is presented. Encryption (CPABE) is accomplished in the standard model under concrete and noninteractive cryptographic assumptions. Any encryptor can express access control in terms of any access formula over the system's attributes using our solutions. The amount of the ciphertext, encryption time, and decryption time all scale linearly with the complexity of the access formula in our most efficient approach. The only previous effort that had been done to obtain these parameters was a proof in the generic group model. Within our framework, we show three constructions. The decisional Parallel Bilinear Diffie-Hellman Exponent (PBDHE) assumption, which can be thought of as a generalisation of the BDHE assumption, is used to argue that our first system is selectively secure. Our following two solutions suggest performance compromises to achieve provable security under the (weaker) decisional Bilinear-Diffie-Hellman scheme.

4. Paper Name: A New Kind of Conditional Proxy Re-Encryption for Secure Cloud Storage

Author: PENG ZENG 1 AND KIM-KWANG RAYMOND CHOO

Description : Secure cloud storage has crucial uses in our big data-driven world, and we need to implement robust access control mechanisms to enable secure cloud storage. PRE (proxy re-encryption) has been proved to be a useful technique for building cryptographically enforced access control schemes. Once the proxy has the required re-encryption key from the delegator, a semi-trusted proxy can transform all ciphertexts for a delegator to ciphertexts for a delegate in a classic PRE scheme. However, in many real applications, fine-grained delegation of decryption abilities is required, hence the concept of conditional PRE (C-PRE) is proposed, which allows the proxy to convert only the ciphertexts that satisfy a specific criteria. We develop a new type of C-PRE called sender- specified PRE (SS-PRE) in this paper, which allows the delegator to delegate the decryption right of ciphertexts from a certain sender to a delegate. A formal definition of SS-PRE and its security model is provided. We also present concrete constructions of an IND-CPA secure SS-PRE scheme and an IND-CCA secure SS-PRE scheme with the properties of unidirectionality and single-use, as well as proofs of security in the standard model for both schemes. Our new IND-CCA secure SS-PRE scheme outperforms traditional C-PRE schemes in terms of calculation cost and ciphertext size, according to a rigorous examination.

5. Paper Name : oPass: A User Authentication Protocol Resistant to Password Stealing and Password Reuse Attacks Author :Hung-Min Sun, Yao-Hsin Chen, and Yue-Hsun Lin Description: Because of their convenience and simplicity, text passwords are the most used form of user authentication on websites. Users' passwords, on the other hand, are vulnerable to being stolen and compromised due to a variety of risks and vulnerabilities .For starters, people frequently choose weak passwords and reuse them across multiple websites. Reusing passwords on a regular basis has a domino effect; if an adversary gains access to one website, she will use that password to obtain access to others. Second, inputting passwords into untrusted computers exposes you to the risk of a password thief. To obtain passwords, an adversary can use phishing, keyloggers, and malware, among other methods. In this work, we propose oPass, a user authentication system that uses a user's smartphone and short message service to prevent password theft and reuse threats. oPass merely asks that each participating website have a unique phone number and that the registration and recovery phases involve a telecommunication service provider. Users only need to remember a long-term password for all websites when using oPass.

6. Paper Name: Generalized Digital Certificate for User Authentication and Key Establishment for Secure Communications

Author: Lein Harn and Jian Ren

Description: The use of a public-key digital certificate to offer user public key authentication is common in public-key infrastructure (PKI). The public key digital certificate, on the other hand, cannot be utilised as a security element for user authentication. The notion of a generalised digital certificate (GDC) is proposed in this work, which can be utilised to offer user authentication and key agreement. A GDC contains a digital signature of the public information signed by a trusted certificate authority, as well as the user's public information, such as the information from a digital driver's license, a digital birth certificate, and so on (CA). The GDC, on the other hand, does not hold any user's public key. Key management with GDC is significantly easier than with a public-key digital certificate because the user does not have a private and public key pair. The GDC's digital signature serves as a hidden token for each user that is never revealed to any verifier. Instead, by answering to the verifier's challenge, the owner proves to the verifier that he is aware of the signature. We propose discrete logarithm (DL) and integer factoring (IF)-based methods for user authentication and secret key establishment based on this approach.

7. Paper Name : Ensuring Data Storage Security in Cloud Computing With Advanced Encryption Standard (AES) and Authentication Scheme (AS)

Author: Mohamed Ismail, Badamasi Yusuf

Description:- Identification of different security threats related to stored data in cloud computing storage, strategies used to safeguard stored data while in cloud storage, system development using Advanced Encryption Standard as algorithm for data encryption and Authentication Scheme valid users verification and prevention of unauthorised access to all functional units of the system, and examination of the significance of using Advanced Encryption Standard as algorithm for data encryption and Authentication Scheme valid users verification and prevention of unauthorised access to all functional units of the system are some of the main objectives of this paper. This paper includes a general introduction, cloud storage and its key challenges, strategies for protecting saved data privacy while in storage, a literature review, methodology, the suggested system, a conclusion, and future improvements.

PROPOSED SYSTEM

The first user registration has been completed. After that, upload the file to the server with the id. Then convert plain text files into cypher text. Each file is secured with a unique encrypted key using the AES technique. The AES algorithm is a symmetrical block cypher that turns plain text into cypher text in blocks of 128 bits utilizing keys of 128, 192, and 256 bits. Using the md5 and sha1 algorithms, the file is stored on the server with a unique id called message digest. MD5 (Message Digest Method 5) is a cryptographic hashing technique that produces a 128-bit digest from any string. The digests are represented as 32-digit hexadecimal numbers. Hashing is the process of converting ordinary data into an unrecognisable format using a hash function. These hash functions, often known as the hash digest or digest in general, are a collection of mathematical calculations that convert the original information into hashed values. Regardless of the input size, the digest size for a hash function like MD5 is always the same. If a user wants to download a file, the AES algorithm is used to decrypt it. For each file, a unique decryption key is generated. Simple text was converted from cypher text. The user can download a file in readable format.

Figure 1: Architecture of The Proposed System

ALGORITHM

The researcher has chosen the Encryption Standard as the method for data encryption and decryption. The AES was usedby the US government as a symmetric encryption standard for data processing (Gueron, 2012). After a 5-year standardisation process, the National Institute of Standards and Technology (NIST) announced this encryption method as the best symmetric encryption standard on November 26, 2001.

AES KEY AND BLOCK:-

There are 2^{128} potential keys for 128 bits, which is equal to 3.4 x 10^{38}. According to APC, breaking the AES cypher with 2^{55} keys per second would take about 149.00 billion years.

There are 2^{198} potential keys for the 192 bits, which is equal to 6.2 x 10^{57}.

There are 2^{256} potential keys for the 256 bits, which is equal to 1.1 x 10^{77}.

For a variable length key equal to (128, 192 and 256 bit). They are represented as a byte matrix having an Ai column and four rows, with Ai denoting key length split by 32 bits, as shown below:

(Ai = 4) represents 128 bits of key = 16 bytes.

(Ai = 6) represents 192 bits of key = 24 bytes.

(Ai = 8) represents 256 bits of key = 32 bytes.

A block of 128 bits, or 16 bytes, can be represented in a byte matrix with four rows and Ab columns, where Ab = block length divided by 32

PROCESS OF ENCRYPTION

The AES encryption technique consisted of four phases, as detailed below (Kak, 2016):

The first stage is to substitute bytes; the second step is to shift row; the third step is to mix columns; and the fourth step is to add a round key.

The final step was an exclusive-OR (XOR) of the output from the first three phases, with a four-word key schedule. There is no mix column in the last round of encryption.

PROCESS OF DECRYPTION

As with encryption, the decryption procedure included four rounds. The distinction between the encryption and decryption processes is that the decryption process reverses the shifting and substitution operations of the encryption process. The steps for decryption are:

The first step is to do an inverse shift round. The second step is to do an inverse bytes substitution.

The third step is to add a circular key.

The fourth step is to create an inverse mix column. Exclusive oaring (XOR) of the first two steps made up the third step. There is no inverse mix column in the final phase of decryption. An example of AES encryption and decryption is provided below:

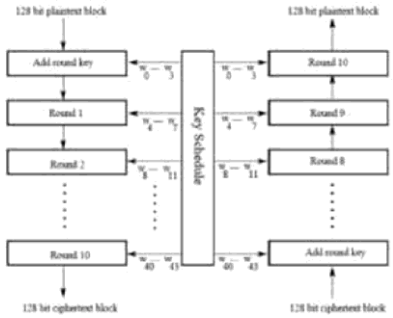

Figure 2: AES encryption and decryption process

MD5 Algorithm **:-**

The MD5 message-digest hashing algorithm uses 512-bit strings that are separated into 16 words of 32 bits each. As a result, MD5 generates a 128-bit message digest value. Each 512-bit block of data is processed along with the value produced in the previous stage to produce the MD5 digest value. In the first stage, the message-digest values are initialised using sequential hexadecimal numerical integers. Each stage includes four message-digest passes, which change values in the current data block as well as values digested from the previous block. The MD5 digest for that block is calculated using the previous block's final value.

CONCLUSION

In the proposed system, with all data stored on the cloud and the internet, it is critical to maintain data security as a top priority. To encrypt confidential data, we utilised the most secure algorithm we've ever used. To guarantee the highest level of security, we used the AES, and MD5 algorithms in the suggested system. However, there are still numerous holes that can be addressed by improving the effectiveness of these strategies.To make cloud computing acceptable to cloud service users, further effort is needed in this field. This project is about data security and privacy, with a focus on data storage and use in the cloud. It aims to develop trust between cloud service providers and consumers by protecting data in cloud computing environments.

REFERENCES

[1] K. Ren, C. Wang, and Q. Wang, "Security challenges for the public cloud," IEEE Internet Computing, no. 1, pp. 69–73, 2012.

[2] L. Zhou, Y. Zhu, and A. Castiglione, "Efficient k-NN query over encrypted data in cloud with limited key-disclosure and offline data owner," Computers & Security, vol. 69, pp. 84–96, 2017.

[3] S. Hu, Q. Wang, J. Wang, Z. Qin, and K. Ren, "Securing SIFT: Privacy-preserving outsourcing computation of feature extractions over encrypted image data," IEEE Transactions on Image Processing, vol. 25, no. 7, pp. 3411–3425, 2016.

[4] H.-M. Sun, Y.-H. Chen, and Y.-H. Lin, "oPass: A user authentication protocol resistant to password stealing and password reuse attacks," IEEE Transactions on Information Forensics and Security, vol. 7, no. 2, pp. 651–663, 2012.

[5] Nalluri, S. K., & Parasaram, V. K. B. (2016). Early Approaches to Robotic Process Automation in Enterprise Systems. International Journal of Humanities and Information Technology, 1(01), 12-28. https://doi.org/10.21590/ijhit.01.01.06

[6] L. Harn and J. Ren, "Generalized digital certificate for user authentication and key establishment for secure communications," IEEE Transactions on Wireless Communications, vol. 10, no. 7, pp. 2372–2379, 2011.

[7] Nalluri, S. K., Parasaram, V. K. B., & Bathini, V. T. (2021). Autonomous Manufacturing Operations Using Intelligent MES and Cloud-Native Analytics. Journal of Multidisciplinary Knowledge, 1(1), 45–55. Retrieved from https://jmk.datatablets.com/index.php/j/article/view/127

[8] P. Zeng, K.-K. R. Choo, "A new kind of conditional proxy re-encryption for secure cloud storage", IEEE Access, vol. 6, pp. 70017-70024, 2018.

[9] Mohamed Ismail, Badamasi Yusuf " ENSURING DATA STORAGE SECURITY IN CLOUD COMPUTING WITH ADVANCED ENCRYPTION STANDARD (AES) AND AUTHENTICATION SCHEME (AS)" International Journal of Information System and Engineering Vol. 4 (No.1), ISSN: 2289-7615

[10] Khalid, U., Ghafoor, A., Irum, M. & Shibl, M. A., 2013." Cloud Based Secure and Privacy Enhanced Authentication and Authorization Protoco. Procedia", Volume 22, pp. 680-688.

[11] Nalluri, S. K., Parasaram, V. K. B., & Bathini, V. T. (2021). Autonomous Manufacturing Operations Using Intelligent MES and Cloud-Native Analytics. Journal of Multidisciplinary Knowledge, 1(1), 45–55. Retrieved from https://jmk.datatablets.com/index.php/j/article/view/127

[12] Tidke, P. M. P. a. P. B., 2014. "Improving Data Integrity for Data Storage Security in Cloud Computing". International Journal of Computer Science and Information Technologies (IJCSIT), 5(5), pp. 6680-6684

[13] Singh, R., Kumar, S. & Agrahari, S. K., 2013. "Ensuring Data Storage Security in Cloud Computing". International Journal Of Engineering And Computer Science ISSN:2319- 7242 , 2(3), pp. 825- 826

[14] Parasaram, V. K. B., & Nalluri, S. K. (2016). A Comparative Analysis of Risk Management Frameworks in Enterprise IT Projects. SAMRIDDHI : A Journal of Physical Sciences, Engineering and Technology, 8(02), 147-155. https://doi.org/10.18090/samriddhi.v8i2.

[15] Kokane, M., Jain, P. & Sarangdhar, P., 2013."Data Storage Security in Cloud Computing". International Journal of Advanced Research in Computer and Communication Engineering , 2(3), pp. 1388- 1389.

[16] Gadichha, N. M. Y. a. V. B., 2013. "Third Party Auditing (TPA) for Data Storage Security in Cloud with RC5 Algorithm." International Journal of Advanced Research in Computer Science and Software Engineering , Volume 3(11), pp. 1032-1037

[17] Wang, G., Q. Liu, J. W. & Guo, M., 2011. "Hierarchical Attribute Based Encryption and Scalable User Revocation for Sharing Data in Cloud Servers. Computers and Security", 30(5), pp. 320-331.