isrjournals

International Journal of Advanced Research in Computer Science Engineering and Information Technology

Volume: 6 Issue: 3 Mar,2017,ISSN_NO: 2321-3337

ENSURING SECURITY USING EMF TECHNIQUE IN CLOUD COMPUTING

Prasanth.D[1], Irfan Ahamed.K.S[2], SubaPriya.V[3]

Student, Dept. of Information Technology, Mohamed Sathak AJ College of Engineering,India.[1,2]

Asst.professor, Dept. of Information Technology, Mohamed Sathak AJ College of Engineering, India.[3]

(prasanth9522@gmail.com)[1],(ahamed2irfan@gmail.com)[2], (subapriyarajesh@gmail.com)[3]

Abstract—Cloud computing means storing and accessing data and program over the internet instead of computer's hard drive.It applies high performance computing power, normally used by military and research facilities to perform tens of trillions of computation per seconds.The cloud server might tamper or replace the data owners original cipher text for malicious attacks and respond a false transformed cipher text. In this project, providing highly secure data and compress the data size which are the user stored in the cloud storage.

Keywords—Cloud,ASCII , Specialised language , Morse.

I.INTRODUCTION

Nowadays the cloud computing is increasing and its receiving a growing attention in the scientific and industrial communities . the cloud server might cheat the authorised uses for cost saving .though the server cloud not respond a correct transformed ciphertext to an unauthorised user, attackers cloud cheat an authorised one that they are not eligible
This technique provides to overcome as the challenges such as the security issues and theft of a intellectual property. there are three major roles in this technique

- **Cipher text –** This original data transfer into cipher text using ASCII
- **Specialised language -** The Encrypted data can be changed into particular language
- **Morse –**The specialised language can be converted into code formatted file type that can reduce the bit size of the original data .

In ASCII each character (letter , number , space , etc) is represented by a number ranging from 0 to 127 (each character is encoded on eight bits). The translation of the digit to the character is done via the ASCII . Then the converted ASCII data's are again converted into Morse code this stage the bit size are decreased from the original size .In this above action the specialised language only known by developers so that the data threat can be control in this process .

II.PROBLEM CREATION

In today's world, every establishment is facing growing challenges which need to be secured up quickly and efficiently. In this cloud computing faces many security risks in every company's loss or theft intellectual property , compliance violations and regulatory actions, loss of a control over end user actions, malware infection that unleash a targeted attacks .

Data breach requiring disclosure and notification to victims , these are all the security issues that can be occurs in the cloud . this process is to highly secure data and reducing the bit size and improve the security.

III.EXISTING METHOD

In the existing system, The servers used to handle and calculate large number of data according to the users demands.we can view the risks of cloud computing in the existing system. As applications move to cloud computing platform, ciphertext-policy attribute-based encryption (CP-ABE) and verifiable delegation (VD) are used to ensure the data confidentiality and the verifiability of delegation on dishonest cloud servers.It put a large amount of data in the cloud for reducing data storage costs.Cloud computing security risks every company faces

1. Loss or theft of intellectual property
2. Compliance violations and regulatory actions
3. Loss of control over end user actions
4. Malware infections that unleash a targeted attack
5. Contractual breaches with customers or business partners
6. Diminished customer trust
7. Data breach requiring disclosure and notification to victims

3.1. RELATED WORKS

"Attribute-based encryption for fine-grained access control of encrypted data"

Vipul Goyal, Omkant Pandey, Amit Sahai, Brent Waters 2006

As more sensitive data is shared and stored by third-party sites on the Internet, there will be a need to encrypt data stored at these sites.

One drawback of encrypting data, is that it can be selectively shared only at a coarse-grained level .ciphertexts are labeled with sets of attributes and private keys are associated with access structures that control which ciphertexts a user is able to decrypt. We demonstrate the applicability of our construction to sharing of audit-log information and broadcast encryption.

"Outsourcing the decryption of ABE ciphertexts "

M.Green,S.Hohenberger,B.Waters 2011

Attribute-based encryption (ABE) is a new vision for public key encryption that allows users to encrypt and decrypt messages based on user attributes. For example, a user can create a ciphertext that can be decrypted only by other users with attributes satisfying ("Faculty" OR ("PhD Student" AND "Quals Completed")). Given its expressiveness, ABE is currently being considered for many cloud storage and computing applications. However, one of the main efficiency drawbacks of ABE is that the size of the ciphertext and the time required to decrypt it grows with the complexity of the access formula. In this work, we propose a new paradigm for ABE that largely eliminates this overhead for users. Suppose that ABE ciphertexts are stored in the cloud. We show how a user can provide the cloud with a single transformation key that allows the cloud to translate any ABE ciphertext satisfied by that user's attributes into a (constant-size) El Gamal-style ciphertext, without the cloud being able to read any part of the user's messages. To precisely define and demonstrate the advantages of this approach, we provide new security definitions for both CPA and replayable CCA security with outsourcing, several new constructions, an implementation of our algorithms and detailed performance measurements. In a typical configuration, the user saves significantly on both bandwidth and decryption time, without increasing the number of transmissions.

"Securely Outsourcing Attribute-Based Encryption with Checkability"

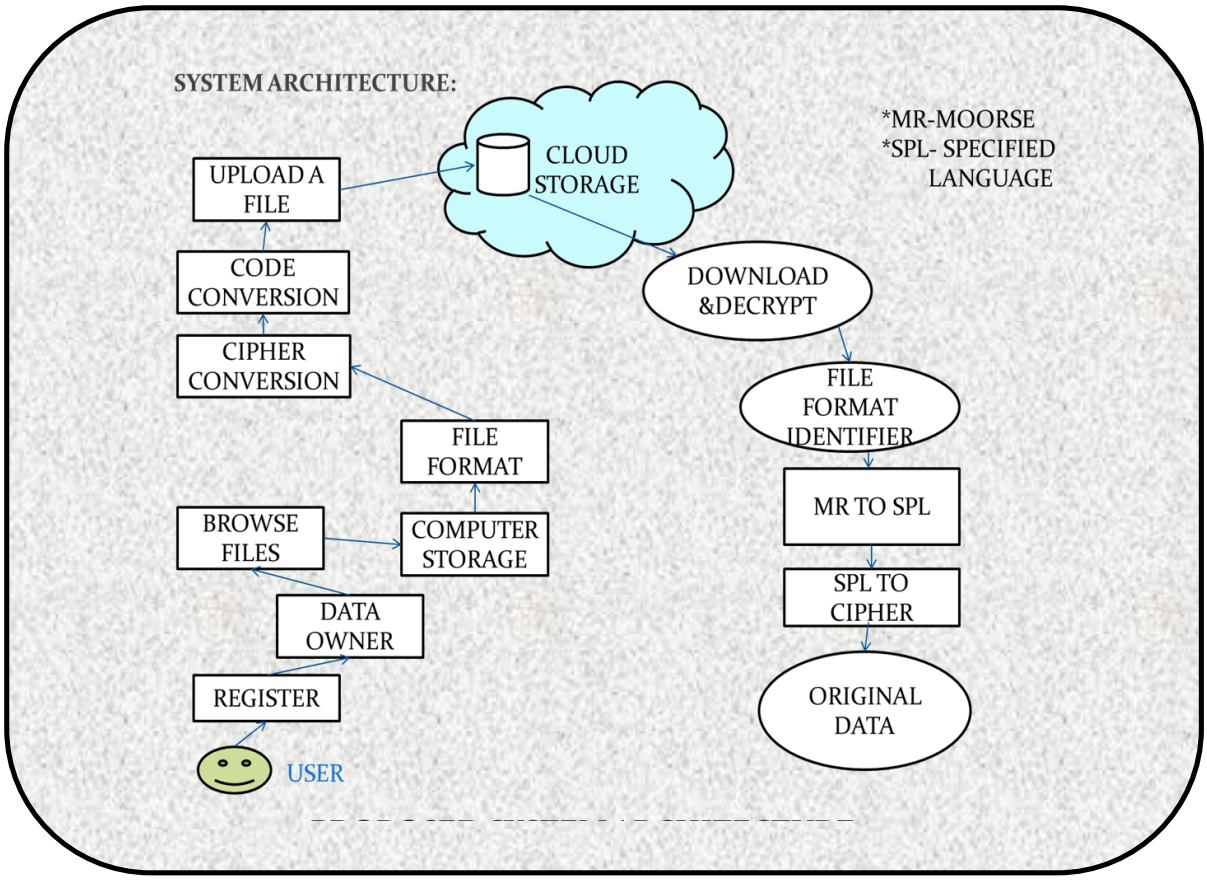
Michael Armbrust, Armando Fox, Rean Griffith, Anthony D. Joseph, Randy H. Katz, Andrew Konwinski, Gunho Lee, David A. Patterson, Ariel Rabkin, Ion Stoica and Matei Zaharia2009

Attribute-Based Encryption (ABE) is a promising cryptographic primitive which significantly enhances the versatility of access control mechanisms. Due to the high expressiveness of ABE policies, the computational complexities of ABE key-issuing and decryption are getting prohibitively high. Despite that the existing Outsourced ABE solutions are able to offload some intensive computing tasks to a third party, the verifiability of results returned from the third party has yet to be addressed. Aiming at tackling the challenge above, we propose a new Secure Outsourced ABE system, which supports both secure outsourced key-issuing and decryption. Our new method offloads all access policy and attribute related operations in the key-issuing process or decryption to a Key Generation Service Provider (KGSP) and a Decryption Service Provider (DSP), respectively, leaving only a constant number of simple operations for the attribute authority and eligible users to perform locally. In addition, for the first time, we propose an outsourced ABE construction which provides checkability of the outsourced computation results in an efficient way. Extensive security and performance analysis show that the proposed schemes are proven secure and practical.

IV.PROPOSED METHOD

We firstly Present the cipher text is converted into specialised language . In this process the data are highly secured when comparing to the existing cloud encryption projects.
This is an next level of a encryption process . the developer only known that particular language so that the data can be highly secured from the attackers .The next process from the specialise language is converted into Morse. This process can reduce the bit size of the

Encrypted data . In the converter Morse code file are stored in the cloud storage . These kind of process are the next level of encryption process in the cloud storage



V.IMPLEMENTATION

5.1Client Registration:

INPUT : USER ID & PASSWORD.
OUTPUT : STORED IN DATABASE.

- In this model, the client can register with the website by entering his (name , user id ,mail-id, contact,city and password field) . on clicking the register button the user will get the confirmation mail to his mail
- once the user get the mail-id they consider as Data owner and they allowed to encrypt the files.

5.2 Data Owner:

INPUT : CIPHERTEXT
OUTPUT : SPECIFIED LANGUAGE

- Data owner will have to register initially to get access to the profile.
- Data Owner will upload the file to the cloud server in the encrypted format.
- Random encryption key generation is happening while uploading the file to the cloud.

5.2 Cloud Server:

INPUT : MOORSE CODE.
OUTPUT : FILE FORMAT WILL BE STORE IN CLOUD**.**

- Cloud server needs to decrypt the files available under their permission.
- Cloud server will have the access to files which are uploaded by the data owner
- Furthermore data user will have to decrypt the data to access the original text by providing the respective key. File has been decrypted successfully and provided for consumer.
- Encrypted file will be stored on the cloud.

5.3 Data Consumer:

INPUT : ENCRYPTED FILE FORMAT.
OUTPUT : DECRYPTING REVERSEPROCESS

- Data consumer will initially ask for the key to the Authority to verify and decrypt the file in the cloud.
- Data consumer can access the file based on the key received from mail id.
- As per the key received the consumer can verify and decrypt the data from the cloud.

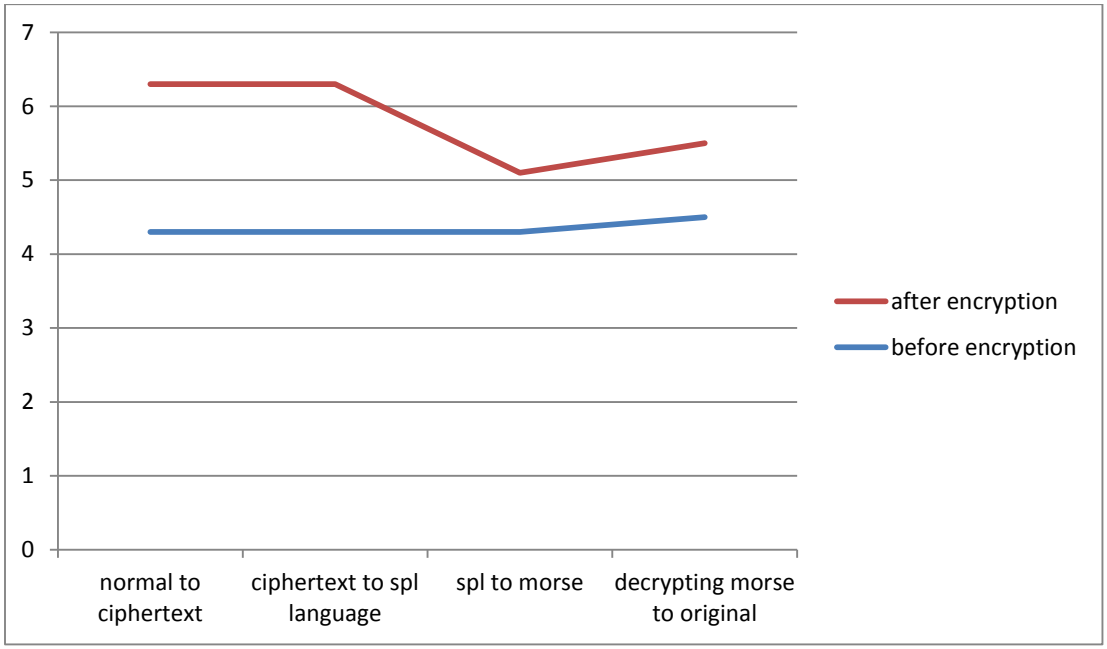


Fig:5Encryption and Decryption process

VI.CONCLUSION

This process is providing secure access to the user and reducing the bit size . The proposed scheme isproven to be secure based on Cipher text is converted into code (morse) that could be stored on the cloud storage.

VII.FUTURE WORK

To the future gen to enhance the multimedia pixel size and setting up the accurate pixel size during the compression process and reducing bit size more than a 50% of original data .

VIII.REFERENCE

[1] TaJie Xu, Qiaoyan Wen, Wenmin Li, and Zhengping Jin, "Circuit Ciphertext-Policy Attribute-Based Hybrid Encryption with Verifiable Delegation in Cloud Computing", IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 27, NO. 1, JANUARY 2016.

[2] A. Sahai, B. Waters, "Fuzzy Identity-Based Encryption", *Proc. Adv. Cryptol.-EUROCRYPT*, vol. LNCS 3494, pp. 457-473, 2005.

[3] T. Nishide, K. Yoneyama, K. Ohta, "Attribute-Based Encryption with Partially Hidden Encryptor-Specified Access Structures", *Proc. Appl. Cryptogr. Netw. Security*, vol. LNCS 5037, pp. 111-129, 2008.

[4] Hao Jin, Hong Jiang, *Senior Member, IEEE,* and Ke Zhou, "Dynamic and Public Auditing with Fair Arbitration for Cloud Data", IEEE TRANSACTIONS ON CLOUD COMPUTING 2016

[5] Shulan Wang, Junwei Zhou, *Member, IEEE,* Joseph K. Liu, *Member, IEEE,* Jianping Yu, Jianyong Chen, and Weixin Xie, "An Efficient File Hierarchy Attribute-Based Encryption Scheme in Cloud Computing", IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 11, NO. 6, JUNE 2016.

BIOGRAPHY

PRASANTH.D pursuring his B.TECH in "Mohamed Sathak AJ College of Engineering", Anna University in Chennai , India , in March 2017

IRFAN AHAMED.K.S pursuring his B.TECH in "Mohamed Sathak AJ College of Engineering", Anna University in Chennai , India , in March 2017

SUBAPRIYA.V Received Her B.E. In Cse Department From Annai Mathaummal Sheela Engineering College, Anna University In Namakkal, India, In May 2006,And Got Her M.E. In Cse Department From Sathyabama University In Chennai, India In August 2015. She Secured Gold Medal And Remained University Topper For The Same. She Also Presented Her Paper Named "Ensuring Security In Cloud Computing Using Biometric Schemes" In International Journal Of Applied Engineering Research.