"Data Security using Hybrid Cryptography in Cloud"

[1]Prof. Ansar I. Sheikh, [2]Twinkle Athole, [3]Kunal Wankhede, [4]Chandan Kawle, [5]Mona Kshirsagar

[2345]Student of Computer engineering

[1]Assistant Professor of computer engineering

Computer Engineering Department

Suryodaya College of Engineering & Technology, Nagpur, India

Abstract*:* Now a day's cloud computing is used in lots of regions like enterprise, military colleges etc to storing huge quantity of facts. We can retrieve records from cloud on request of person. To shop data on cloud we need to face many troubles. To provide the answer to those issues there are n number of methods. Cryptography and steganography techniques are more popular now a day's for statistics security. Use of a single algorithm is not powerful for high level safety to data in cloud computing. In this paper we've delivered new safety mechanism the usage of symmetric key cryptography algorithm and steganography. In this proposed gadget AES, blowfish, RC6 and BRA algorithms are used to offer block smart security to information. All set of rules key length is 128 bit. LSB steganography method is introduced for key statistics security. Key information includes which a part of report is encrypted using by which algorithm and key. File is splited into eight parts. Each and every a part of report is encrypted the usage of one of a kind algorithm. All parts of file are encrypted concurrently with the assist of multithreading approach. Data encryption Keys are inserted into cowl image the usage of LSB method. Stego picture is ship to legitimate receiver using e mail. For document decryption cause opposite method of encryption is applied.

Key Words**:** Hybrid cryptography, ABE Encryption, ABE Decryption, Blow fish.

1. INTRODUCTION

Distributed computing is started from before giant scale appropriated processing innovation. NIST characterizes Cloud figuring as "a model for empowering exceptional, on request put together access to a mutual pool of configurable registering property (e.g. structures, stockpiling, applications and administrations) that may be quick provisioned and discharged with negligible management exertion or expert co-op conversation". In Cloud registering, the two information and programming aren't absolutely contained at the patron's PC. Record safety worries emerge in mild of the fact that both customer's software and application are living in provider premises. The cloud provider can deal with this difficulty by means of encoding the files through using encryption calculation. This paper shows a report safety model to offer a productive solution for the fundamental trouble of protection in cloud condition. In this model, 1/2 breed encryption is applied in which information are scrambled by using blowfish combined with report element and SRNN(modified RSA) is applied for the secured correspondence amongst customers and the servers.

1.1 WHAT IS CLOUD?

Cloud computing is a trendy term for the delivery of hosted services over the Internet. It has always been divided into three broad services categories:

Infrastructure as a Service (IaaS),

Platform as a Service (PaaS) and

Software as a Service (SaaS).

Cloud Computing is the name given to the latest trend in computing service provision. This trend has seen the technological and cultural shift of computing service provision from being provided locally to being provided remotely and en masse, by third-party service providers. Functionality such as storage, processing and other functionality is no woffered on demand, as a service and both freely and at cost. Data that become once housed beneath a purchaser's personal administrative and protection area, has now been extracted and positioned beneath the area of the Cloud Service Provider (CSP). The consumer has effectively lost control over how their data is being stored, shared and used, and also over the security used to protect their data. Moreover, it is able to be the case that a surreptitious employee of the service company could have get admission to for your data for legitimate purposes but will abuse this electricity for his or her very own way. Users are not in full manage over the security of their statistics and the protection offered via the carrier issuer is not absolute. There is a want for customers to have extra control over the safety of their data within the cloud: Users want to turn out to be empowered.

1.2 HYBRID CRYPTOGRAPHY

Hybrid encryption is a style of encryption that merges or more encryption systems. It carries a combination of uneven and symmetric encryption to benefit from the strengths of every shape of encryption. These strengths are respectively described as speed and security. Hybrid encryption is taken into consideration a incredibly secure kind of encryption so long as the public and personal keys are absolutely stable. A hybrid encryption scheme is one which blends the convenience of an uneven encryption scheme with the effectiveness of a symmetric encryption scheme. Hybrid encryption is executed through information switch using unique session keys along side symmetrical encryption. Public key encryption is applied for random symmetric key encryption. The recipient then uses the general public key encryption technique to decrypt the symmetric key. Once the symmetric key's recovered, it's far then used to decrypt the message.

2. PROJECT OBJECTIVE

Provide security to user individual data. Protect from data breach and data loss attacks. Implementation of ABE algorithm, Data Security and the Cloud. The preliminary stage sought to offer a clean definition for Cloud Computing and the security troubles there in, seeking to discover precisely where and whilst threats can occur to records and the way those threats have to be mitigated.

Predicate Based Encryption. The next stage centered solely upon PBE schemes discussing how they work and what they allow for. This provided a basis upon which their deployment as part of a crypto-system might be explored and to define the types of trouble that PBE schemes can be used to resolve Leveraging PBE. The final level of the investigation built upon, and blended the results, of the preceding ranges. Here the investigation regarded to determine the troubles that PBE schemes can be used to clear up within the Cloud, and the first-class of answer provided.

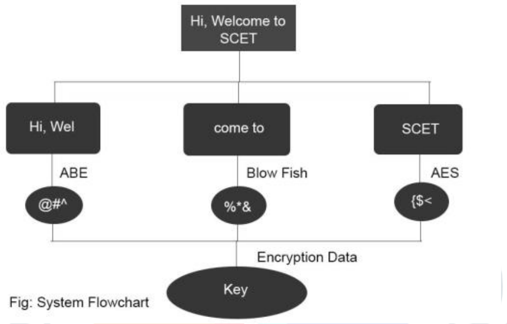


Figure 1: System Flowchart

2.1 LITERATURE SURVEY

Key feature of scheme aim to minimize the expense of storage and manage secret keys for general cryptographic use. Key undertaking scheme purpose to decrease the price in storing and dealing with mystery keys for trendy cryptographic use. Key undertaking schemes maximum probable non-consistent decryption key size, symmetric or public key for a predefined hierarchy is used. Only hash features are used for a node to derive a descendant’s key from its personal key. The area complexity of the public information is similar to that of storing hierarchy and is asymptotically most efficient; the non-public facts at a node consists of a unmarried key related to that node and updates are treated locally within the hierarchy.

Attribute-primarily based encryption (ABE) permits every cipher text to be related to an characteristic, and the grasp-secret key holder can extract a mystery key for a coverage of those attributes in order that a cipher text may be decrypted by means of this key if its associated characteristic conforms to the coverage. In a multi- authority ABE scheme, multiple characteristic-authorities monitor extraordinary units of attributes and issue corresponding decryption keys to customers and encryptors can require that a person achieve keys for appropriate attributes from every authority before decrypting a message.

The Cloud computing revolution is redesigning modern networking, and offering promising environmental protection prospects as well as economic and technological advantages.

3. PROPOSED SYSTEM

3.1 ARCHITECTURE

In this architecture, users encrypt a message now not handiest underneath a public- key, however additionally under an identifier of cipher text known as elegance. That approach the cipher texts are in addition classified into distinctive instructions. The key owner holds a grasp-secret known as grasp-secret key, which may be used to extract mystery keys for one of a kind lessons.

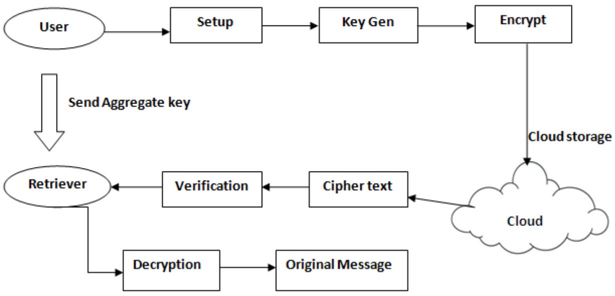


Figure : System Architecture

Figure 2: System Architecture

More importantly, the extracted key have may be an aggregate key that's as compact as a mystery key for a single magnificence, however aggregates the energy of many such keys, i.e., the decryption energy for any subset of ciphertext training. With our solution, user can truely send retriever a unmarried aggregate key through a stable electronic mail. Retriever can download the encrypted photos from person’s Dropbox area after which use this combination key to decrypt those encrypted pictures.

3.2 ALGORITHM

3.2.1 BLOW FISH

Blow Fish is a symmetric block cipher which makes use of a Fiesta community, sixteen rounds of iterative encryption and decryption practical layout. The block size used is of 64- bits and key size can range from any length to 448. Blowfish cipher makes use of 18 sub arrays each of 32-bit usually referred to as P-bins and 4 Substitution packing containers every of 32-bit, every having 256 entries .The set of rules design is proven in discern. It consists of levels : one is Key Expansion phase any other is Data Encryption section. In Key enlargement section, key is converted into several sub-keys and in Data Encryption phase, encryption happens thru 16-spherical networks. Each spherical includes a key based permutation and a key and facts-dependent substitution.

3.2.2 ABE ENCRYPTION

Attribute-based encryption is a type of public-key encryption in which the secret key of a user and the ciphertext are dependent upon attributes (e.g. the country in which he lives, or the kind of subscription he has). In such a system, the decryption of a ciphertext is possible only if the set of attributes of the user key matches the attributes of the ciphertext. A crucial security aspect of attribute-based encryption is collusion-resistance: An adversary that holds multiple keys should only be able to access data if at least one individual key grants access.

4. MODULES

4.1 NEW USER GRANT MODULE

In this module normal registration for the multiple users. There are multiple owners, multiple AAs, and multiple users. The attribute hierarchy of files – leaf nodes is atomic file categories while internal nodes are compound categories. Dark boxes are the categories that a PSD’s data readers have access to.

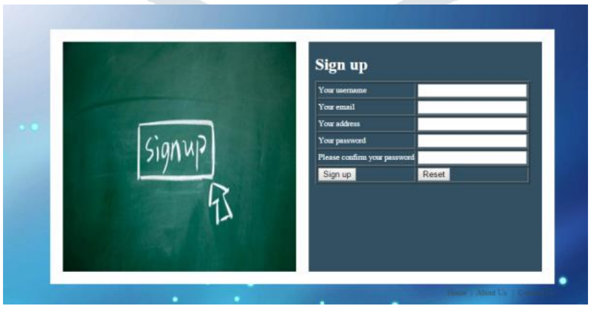
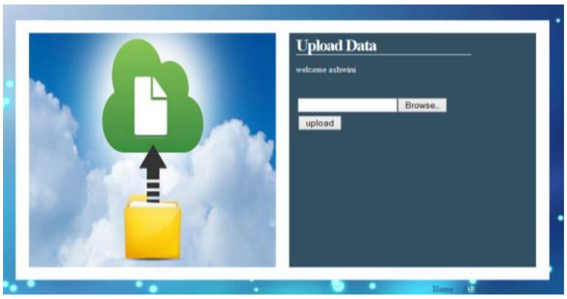


Figure 3: New User Grant Module

4.2 FILE UPLOAD

In this module, users upload their files with secure key probabilities. The owners upload ABE-encrypted PHR files to the server. Each owner’s PHR file encrypted both under a certain fine grained model.



Upload Data

welcome ashwini

Figure 4: File Upload

4.3 File Access

In this module ABE to realize fine-grained access control for outsourced data especially, there has been an increasing interest in applying ABE to secure electronic healthcare records (EHRs). An attribute-based infrastructure for EHR systems, where each patient’s EHR files are encrypted using a broadcast variant of CP-ABE that allows direct revocation. However, the cipher text length grows linearly with the number of un revoked users. In a variant of ABE that allows access rights is proposed for encrypted EHRs applied cipher text policy ABE (CP-ABE) to manage the sharing of PHRs, and introduced the concept of social/professional domains investigated using ABE to generate self-protecting EMRs, which can either be stored on cloud servers or cell phones so that EMR could be accessed when the health provider is offline.

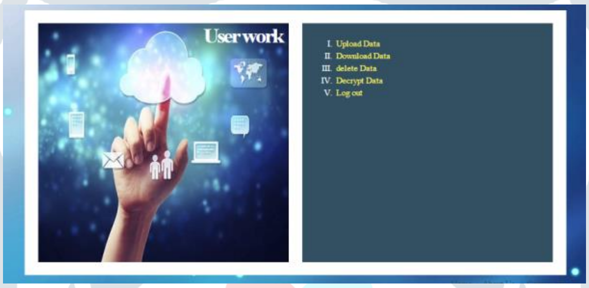
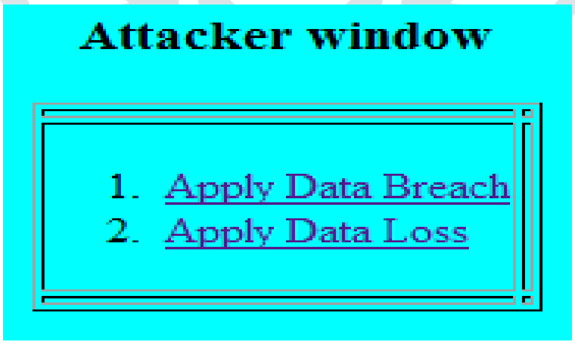


Figure 5: File Access

4.4 Attack Prevention

Attackers have been using the web to compromise user’s computers and perform malicious activities such as steal sensitive data. Security challenges in SaaS applications are not different from attacks, so new approaches are necessary. The Open Web Application Security Project (OWASP) has identified the ten most criticalweb applications security threats. There are more security issues, but it is a good start for securing web applications. However, flaws in web applications may create vulnerabilities for the SaaS applications.



Attacker window

Figure 6: Attack Prevention

4.5 Result And Analysis

Data security is a common concern for any technology, but it becomes a major challenge when SaaS users have to rely on their providers for proper security. In SaaS, organizational data is often processed in plaintext and stored in the cloud. The SaaS provider is the one responsible for the security of the data while is being processed and store.

```
[illegible]
```

Figure 7: Result and Analysis

5. Future Scope

According to Gartner's Hype cycle, cloud computing has reached a maturity that leads it into a productive phase. This means that most of the main issues with cloud computing have been addressed to a degree that clouds have become interesting for full commercial exploitation. This however does not mean that all the problems listed above have actually been solved, only that the according risks can be tolerated to a certain degree. Cloud computing is therefore still as much a research topic, as it is a market offering. What is clear through the evolution of Cloud Computing services is that the CTO is a major driving force behind Cloud adoption.[92] The major Cloud technology developers continue to invest billions a year in Cloud R&D; for example, in 2011 Microsoft committed 90% of its $9.6bn R&D budget to cloud. WE can use ABE and AES together for better encryptions of data.

With the improvements in Cloud computing, there may be now a developing attention on implementing information sharing skills in the Cloud. It is likewise used as a center technology behind many online offerings for personal packages. On cloud all and sundry can share statistics as a great deal they need to i.e. Most effective decided on content material can be shared. Cryptography allows the information owner to share the information to in safe manner. So person encrypts data and uploads on server. Key aggregate cryptosystem approach used for records sharing in cloud storage is greater steady. This approach is beneficial for securely, efficiently, and flexibly proportion information with others in cloud storage. It is an efficient public-key encryption scheme which helps bendy delegation.

6. Conclusions

Cloud Computing embodies the as-a-Service paradigm and allows for services to be provided en masse to consumers. The problems associated with the use of cloud based services can be summarized by the unknown risk profile and unknown expectation of privacy Section.

When service users push data to the cloud they need to rely upon Cloud Service Providers (CSPs) adhering to their remit, and doing so dutifully. However, when looking to build solutions to protect data in the cloud it is important to remember that for the service user the CSP can be trusted, albeit at arm's length. The threat models presented in Traditional privacy models are too user-centric and CSP-fearing when trying to address the problem of protecting data. A privacy model centered around Kafka's The Trial helps to address this problem, this privacy model indicates that when protecting one's data one should also have control over its use rather than solely preventing its collection: CSPs and service users need to work together.

The encryption and decryption of any data has a secure key, which is used for data encryption. For this purpose asymmetric key is used. This work secures the data, using linear block cipher algorithm. The block cipher algorithm is more efficiently using in symmetric encryption technique. The result of the proposed research plan shows that processing time is more efficient other algorithm. Thus AES algorithm along with the use of RSA algorithm for key management will provide an efficient technique to ensure the security of transmitted data. The security RSA AES better than RSA-DES and our proposed algorithm is efficient than RSA AES during the application of data transmission. Finally we illustrated the new directions for the future research. We can develop the derivatives of outburst attack. Thus the proposed Hybrid Encryption Algorithm using Block cipher and symmetric key provides a more secure and convenient technique for secure data trans-mission for all kind application.

REFERENCE

1. P. Mell and T. Grance, “The NIST denition of cloud computing,” Special Publication 800-145, 2011.
2. S. Yu, C. Wang, K. Ren, and W. Lou, “Attribute based data sharing with attribute revocation,” in Proceedings of the 5th ACM Symposium on Information, Computer and Communication Security (ASIACCS '10), pp. 261–270, April 2010. View at Publisher · View at Google Scholar · View at Scopus
3. A. Sahai and B. Waters, “Fuzzy identity based encryption,” in Proceedings of the 24th Annual International Conference on Theory and Applications of Cryptographic Techniques (EUROCRYPT '05), vol. 3494 of Lecture Notes in Computer Science, pp. 457–473, Springer, 2005.
4. D. Boneh and M. K. Franklin, “Identity-based encryption from the Weil pairing,” in Proceedings of the Annual International Cryptology Conference (CRYPTO '01), vol. 2139 of Lecture Notes in Computer Science, pp. 213–229, Springer, 2001.
5. V. Goyal, O. Pandey, A. Sahai, and B. Waters, “Attribute-based encryption for fine-grained access control of encrypted data,” in Proceedings of the 13th ACM Conference on Computer and Communications Security (CCS '06), pp. 89–98, November 2006. View at Publisher · View at Google Scholar · View at Scopus.
6. V.S. Mahalle, A. K. Shahade, "Enhancing the Data Security in Cloud by Implementing Hybrid (Rsa & Aes) Encryption Algorithm", IEEE INPAC, pp. 146-149, Oct. 2014.
7. P. S. Bhendwade, R. T. Patil, "Steganographic Secure Data Communication", IEEE International Conference on Communication and Signal Processing, pp. 953-956, April 2014.
8. Yingbing Zhou, Yongzhen LI, "The Design and Implementation of a Symmetric Encryption Algorithm Based on DES", IEEE ICSESS, pp. 517-520, June 2014.
9. N. Sharma, A. Hasan, "A New Method Towards Encryption Schemes (Name-Based-Encryption Algorithm)", IEEE International Conference on Reliability Optimization and Information Technology, pp. 310-313, Feb 2014.
10. V. Chang” Towards data analysis for weather cloud computing “,Knowledge -Based Systems, Elsevier,Vol.127, 2017, pp. 29-45.