iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 3 **Issue:** III **Month of publication:** March 2015

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Secure and Efficient Data Retrieval Using Attribute-Based Encryption in Distributed System

Mandar Parande[1], Manoj Shukla[2], Jay Patel[3], Prof.Vijaya Sagvekar[4]
[1,2,3] Student member (Comp), [4]Assistant Prof.(Comp), Atharva College of Engg.

Abstract- ***Attribute-based encryption (ABE) is a public-key based one-to-many encryption that allows users to encrypt and decrypt data based on user attributes. A promising application of ABE is flexible access control of encrypted data stored in the distributed system, using access polices and ascribed attributes associated with private keys and cipher text. One of the main efficiency drawbacks of the existing ABE schemes is that decryption involves expensive pairing operations and the number of such operations grows with the complexity of the access policy. To overcome this drawback we have proposed a method in which we will provide rich expressiveness of index terms by exploiting ABE, thus providing data security. The data will be stored in the form of trie structure, which will reduce the search complexity and will support one upload many download feature because of use of attribute based encryption.***

Keywords- ***CipherText,Encyrption,Cryptography***

I. INTRODUCTION

In today's networked world, computers rarely work in isolation. They collaborate with each other for the purpose of communication, processing, data transfer, storage etc. Distributed system is a system where the hardware and software components have been installed in geographically dispersed computers that coordinate and collaborate their actions by passing messages between them [1]. Distributed system is an application that communicates with multiple dispersed hardware and software in order to coordinate the actions of multiple processes running on different autonomous computers over a communication network, so that all components hardware and software cooperate together to perform a set of related tasks targeted towards a common objective. Distributed system has been built with the objective of attaining the following: Transparency, Openness, Reliability, Performance and Scalability. There are many security threats to this type of infrastructure as it contains the data from different systems. So this threats may hinder the storage of data which is centralized at one place or system. To overcome this we use some of the cryptographic techniques viz. attribute-based encryption, searchable encryption etc. searchable encryption is a technique which provides the user to search over the encrypted text i.e. ciphertext using encrypted keywords. Attribute-based encryption uses attributes of the user or data owner in generating private key which he/she can use to encrypt the plain text. This techniques provides data integrity, anonymity, less key storage, data confidentiality etc.

II. LITERATURE REVIEW

A. Distributed system and security

In today's networked world, computers rarely work in isolation. They collaborate with each other for the purpose of communication, processing, data transfer, storage etc. Distributed system as "a system where the hardware and software components have been installed in geographically dispersed computers that coordinate and collaborate their actions by passing messages between them. Distributed system is an application that communicates with multiple dispersed hardware and software in order to coordinate the actions of multiple processes running on different autonomous computers over a communication network, so that all components hardware and software cooperate together to perform a set of related tasks targeted towards a common objective. Distributed system has been built with the objective of attaining the following: Transparency, Openness, Reliability, Performance and Scalability. In order to achieve the above objectives, security of the system must be given adequate attention as it is one of the fundamental issues in distributed system [2].

B. Cluster Computing

A set of computers that are grouped together in such a manner that they form a single resource pool is called a cluster. Any task that

©IJRASET 2015: All Rights are Reserved

has been assigned to the cluster would run on all the computers in the cluster in a parallel fashion by breaking the whole task into smaller self contained tasks. Then, the result of the smaller tasks would be combined to form the final result[3].
Protein sequencing in biomedical applications, earth quake simulation in civil engineering and petroleum engineering and replicated and distributed storage and backup servers for high demand web based business applications are a few examples for applications which primarily run on clusters [3]

C. *Attribute-based encryption*

Attribute-based encryption [10] provides good solutions to the problem of anonymous access control by specifying access policies among private keys or ciphertext over encrypted data. In ciphertext-policy attribute-based encryption (CP-ABE), each user is associated with a set of attributes, and data is encrypted with access structures on attributes. A user is able to decrypt a ciphertext if and only if his attributes satisfy the ciphertext access structure. CP-ABE is very appealing since the ciphertext and data access policies are integrated together in a natural and effective way. Attribute-based encryption is a one's identity can be viewed as a combination of several attributes expressing the characteristics of the user in the form of access policy by using Boolean expressions such as AND, OR, or NOT.

III. ARCHITECTURE

We describe the architecture of the storage system. As depicted in Fig. , the system consists of the following four entities:
Trusted authority: This is the key generation center, which is fully trusted by all other participants of the system. It generates public parameters and the master secret key, which are the primary key materials for the entire process of the proposed scheme. It also generates user-specific private keys which correspond to the set of attributes for data access, ciphertext decryption for receivers, and anonymous keys for data owners.
Service provider: This is an entity that provides data storage and retrieval service to subscribing users. It stores the data content outsourced by the data owner. This content is searchable and downloadable to intended receivers who have sufficient credentials. We assume that the SP is semi-trusted, which means that it follows the protocol specified in the system.
Data owner: This is the storage subscriber who wants to upload its data content anonymously to the distributed system storage system after encryption. The encrypted content can be shared with intended receivers who have sufficient credentials as specified by the data owner.

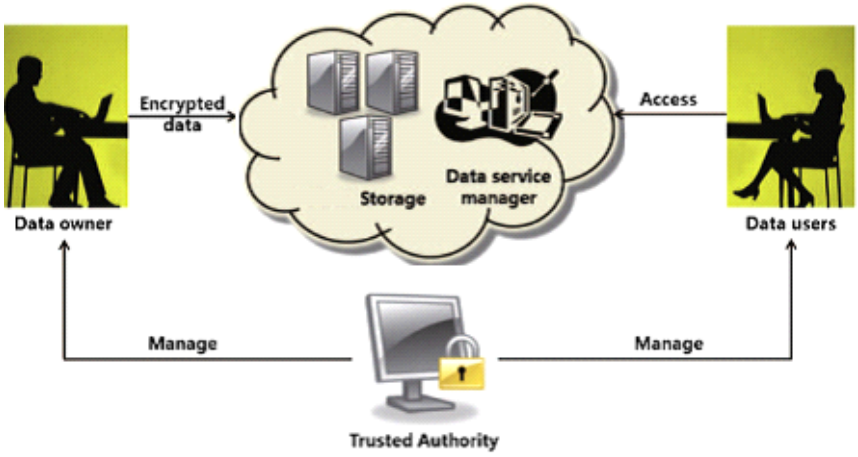


Fig. 3 Architecture of a storage system[5]

Retriever: This is another storage subscriber which queries the SP for encrypted data in the storage system by using a pseudonym of the data owner. Only retrievers who have legal rights satisfying the access policy specified by the data owner can access the encrypted content and restore the original message from it. Henceforth, we will use the terms retriever and receiver interchangeably.

A. *Definitions and Preliminaries*

©IJRASET 2015: All Rights are Reserved

A brief review of the formal definitions and notations essential in the construction of the proposed scheme:

1) *Access structure:* Let $\{P_1, P_2 \ldots P_n\}$ be a set of parties. A collection $A \subseteq 2^{\{P_1, P_2, \ldots, P_n\}}$ is monotone if $\forall$ B, C: if B $\in \mathbb{A}$ and B $\subseteq$ C then C $\in \mathbb{A}$. An access structure (respectively, monotone access structure) is a collection (respectively, monotone collection) A of non-empty subsets of $2^{\{P_1, P_2, \ldots, P_n\}} \setminus \{\phi\}$. The sets in $\mathbb{A}$ are called the authorized sets, and the sets not in $\mathbb{A}$ are called the unauthorized sets.
2) *Bilinear Diffie Hellman:* The Diffie-Hellman key exchange, created in 1976, is one of the most widely used cryptographic tools, with several different versions. The process allows two people to create a common key to a cypher, even if there are eavesdroppers listening to their conversation.

In the first step, one of Alice or Bob communicates a prime p and a nonzero integer g modulo p. The integer g is best to have a large order, so g is typically a primitive root. That is, the order of g is p□1. With this common information, Alice chooses a secret integer a, Bob chooses a secret integer b, and they both raise g to that power.
This gives:

A = g^a mod p and B = g^b mod p
A and B are now communicated between the two, with Eve observing both values.
Now, Alice raises B to the power of her secret integer a, and Bob does the same with A to his secret integer b, giving:
$B_0 = B^a$ mod p and $A_0 = A^b$ mod p:
These values are the secret key, as they are equal (shown below) and have not been
broadcast to Eve.
$B_0 = B_a = (g^b)^a = (g^a)^b = A_b = A_0$ mod p

If Eve, knowing A and B, can determine one of the secret integers a and b, she can reconstruct the key. Thus, without loss of generality, given A, g and p, she must be able to a such that A = g^a mod p

Common Parameters Communicated $p = 1223, g = 158$ $\longleftrightarrow$	
Secret Integers	
Alice: $a = 125$	Bob: $b = 421$
First Computations	
$A = 322 \equiv 158^{125} \bmod 1223$	$B = 873 \equiv 158^{421} \bmod 1223$
Communication	
$A = 322 \longrightarrow$ $\longleftarrow B = 873$	
Common Key Computation	
$A' = 199 \equiv 873^{125} \bmod 1223$	$B' = 199 \equiv 322^{421} \bmod 1223$

Fig.3.1 Diffie Hellman Key Exchange

3) *Bilinear maps*
Let G_1, G_2 and G_T be three cyclic groups of prime order p. Let g be a generator of G_1 and e be a bilinear map,
e : $G_1 * G_2$ G_T with the following properties:

a) Bilinearity: for all u $\in$ G_1, v $\in$ G_2 and a, b $\in$ Z_p, we have e (u^a, v^b) = e $(u, v)^{ab}$.
b) Non-degeneracy: e (g, g) ≠1.
c) Computability: There is an efficient algorithm to compute e (u, v) for any u $\in$ G_1 and v $\in$ G_2.

©IJRASET 2015: All Rights are Reserved

Like many pairing-based cryptographic approaches, we also use a special form of bilinear map called a symmetric pairing where $G_1 = G_2$. Therefore, it is notable that $e(g^a, g^b) = e(g, g)^{ab} = e(g^b, g^a)$. In the rest of the paper, all bilinear pairings are symmetric, and we simply denote $G_1 = G_2$ as G.

IV. PROBLEM STATEMENT

To create an application providing security to an Encrypted data which is uploaded by data owner in a secure distributed server with the help of access structure policy. When the new user is registered then trusted server automatically generate public key and master key one for all user. Data Owner can upload plaintext files with the help of access structure policy and even user can download the files by satisfying the access structure policy. The advantage of this scheme is that it provides efficient and secure retrieval of data by comparison of user attributes and the access structure in the encrypted file.

V. CONCLUSION

Widely spread Distributed system paradigm enables third-party storage to provide retrieval services without direct communication between senders and receivers. While previous public key systems supporting searches on previously encrypted data emulated existing public key encryption systems without encryption and decryption algorithms, we presented a secure anonymous ABE system supporting searches on encrypted data.In attribute-based encryption systems, keywords as a part of attributes can be served as index terms to be searched. The keywords let anyone search on a given set of encrypted data[3].In this paper, a new searchable cryptosystem is proposed by exploiting attribute-based encryption with proper obfuscation of attributes. It provides enhanced quality of the retrieval service via simple comparisons for data retrieval. Comparatively, complicated retrieval operations for a specific encrypted data in existing approaches are not appropriate for an environment where numerous receivers request frequently for huge amount of data. Through integration of searching ability into attribute-based encryption, remarkable data retrieval performance of the proposed scheme is shown via analysis in terms of computational complexity. It means that our scheme describes more fine-grained access control than previous ones and might reduce the number of searching index terms by using Boolean operators rather than simple concatenation.In other words, scrambled index terms can be used as database indexes while preventing information leakage without exhaustive searches on stored data. This implies our cryptosystem is more suitable to Distributed system[6].

VI. FUTURE WORK

In a world overrun with digital identities and passwords, network access privileges are often outdated and overly broad. A new technology--called attribute-based encryption (ABE)--promises to significantly advance the field of trustworthy computing by basing access on a person's job description or constellation of role-based characteristics rather than identity.

VII. ACKNOWLEDGMENT

We are extremely grateful to Ms. Vijaya Sagvekar for her constant guidance and support.

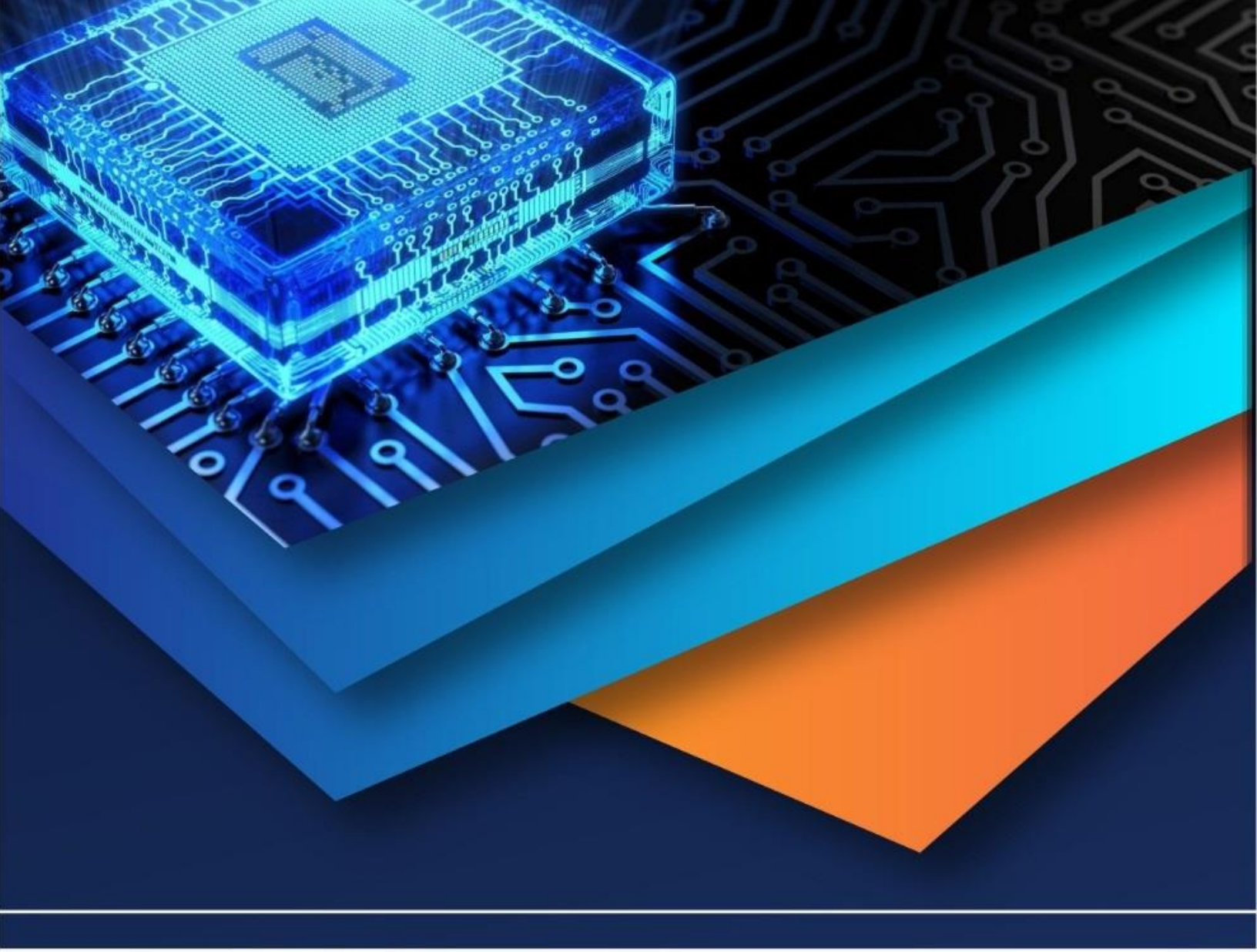
REFERENCES

[1]George Coulouris, Jean Dollimore, and Tim Kindberg, "Distributed Systems - Concepts and Design," 4th ed. London, England: Addison - Wesley, 2005.
[2] Zhidong Shen and Xiaoping Wu, "The Protection for Private Keys in Distributed Computing System Enabled by Trusted Computing Platform," in International Conference On Computer Design And Appliations (ICCDA 2010), Qinhuangdao, Hebei, China, 2010, pp. 576-580.
[3] Mark Baker and Rajkumar Buyya, "Cluster Computing at a Glance," in High Performance Cluster Computing: Architectures and Systems - Volume 1, Rajkumar Buyya, Ed. Upper Saddle River, NJ, USA: Prentice Hall, 1999, ch. 1, pp. 3-47.
[4] Tao Xie and Xiao Qin, "Security-Aware Resource Allocation for Real-Time Parallel Jobs on Homogeneous and Heterogeneous Clusters," IEEE Transactions on parallel and distributed Systems, vol. 19, no. 5, pp. 682-697, May 2008.
[5] Yuri Demchenko, Cees de Laat, Oscar Koeroo, and David Groep, "Re-thinking Grid Security Architecture," in IEEE Fourth International Conference on eScience, 2008 (eScience '08), Indianapolis, IN, USA, 2008, pp. 79-86.
[6] Xiao Gao Yu and Wei Xing Li, "A new network storage architecture based on NAS and SAN," in 10th International Conference on Control, Automation, Robotics and Vision (ICARCV 2008), Hanoi, Vietnam, 2008, pp. 2224 - 2227.
[7] Ali Safari Mamaghani, Mostafa Mahi, Mohammad Reza Meybodi, and Mohammad Hosseinzadeh Moghaddam, "A Novel Evolutionary Algorithm for Solving Static Data Allocation Problem in Distributed Database Systems," in Second International Conference on Network Applications, Protocols and Services (NETAPPS), Alor Setar, Kedah, 2010, pp. 14-19.

©IJRASET 2015: All Rights are Reserved

[8] Boneh D, Waters B. Conjunctive, subset, and range queries on encrypted data. In: Vadhan S, editor. Theory of cryptography, vol. 4392. Berlin Heidelberg: Springer; 2007. p. 535–54. doi:http://dx.doi.org/10.1007/978-3-540-70936-7_29.
[9] Katz J, Sahai A, Waters B. Predicate encryption supporting disjunctions, polynomial equations, and inner products. In: Proceedings of the theory and applications of cryptographic techniques 27th annual international conference on Advances in cryptology, EUROCRYPT'08. Berlin, Heidelberg: Springer-Verlag; 2008. p. 146–62.
[10] Sahai A, Waters B. Fuzzy identity-based encryption. In: Cramer R, editor. Advances in cryptology, EUROCRYPT 2005, vol. 3494. Berlin Heidelberg: Springer; 2005. p. 557–57. doi:http://dx.doi.org/10.1007/11426639_27.

©IJRASET 2015: All Rights are Reserved



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)