International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 04 Issue-17
December 2017

Supporting Attribute-Based Encryption for Secure Data Sharing in Big Data Environments

Y. Prabhu Kumar & M. Vijaya
Assistant Professor, Dept of CSE, Vidya Jyothi Institute of Technology, India.

ABSTRACT— *As the data become an important issue in every research. Big data security has been increasingly concerned. In this scenario to control the access of users where data is stored in the cloud, we use a Technique called CP-ABE (Cipher text – Policy Attribute Based Encryption) which uses some attributes of data consumers to encrypt their data under the access policies, and use this attributes to decrypt the data. Even CP-ABE access policy is attached to the cipher text in plain text form, which also leaks some end-users information. To overcome this we use CP-ABE with a novel distributed Publish-Driven Secure Data sharing for ICIOT (DPD-ICIOT) which allows authorized users and publishers to access the IOT data from distributed storage network. In this proposed system we use the key mechanism which is efficient for cryptographic operate like self-updating attributes automatically without querying the centralized servers. It also achieves lower bandwidth and cost compared to the existing CP-ABE and end users privacy without employing much overhead.*

1. INTRODUCTION

In the generation of big data, a huge amount of data can be generated from heterogeneous sources. Emerging of big data, conventional computers are unable to compete it. In the processing and storage of data [1], [2].Cloud computing helps in improving the flexibility and efficiency of storing protecting data. Even though there are challenges to face. Attribute based access control end-users first define access policies for their data and encrypt the data by following the access policies [3], [5]. This is proposed by advantaging attribute based encryption [6], [7]. It has the attribute revocation problem [3], [5] which leaks privacy. The basic theme to demonstrate the access policy in Linear Secret Sharing Scheme (LSSS).ABF is used to evaluate the presence of attribute and to reduce communication overhead.

For more convenience, we take the help of IOT, the new era of the world that makes the world digital. IOT is nothing but connecting the things to the internet.IOT is used to store huge amount of data and perform various data applications. ICN is an upcoming technology that allows users to retrieve data from near caches without the servers [6], [8], [9] to reduce the redundant traffic overhead and data retrieval latency by moving data from clouds to caches near to Content Centric Network(CCN) users or Named Data Network(NDN)[6], [9] is the one of the most important architectures includes security, heterogeneity, fast configuration and diverse communication paradigms [10], [11], [12], [13], [14], [15], [16], [17], [18], [19].

ICIOT is used to support to IOT application and services like smart cities [10], smart grid [16], smart home [14] etc. It is solution to provide to flexible IOT services to users[11], [12], [19].Authentication Authorization Access control[AAA] [22], [23] have been investigated .Cipher text Policy –Attribute Based Encryption(CP-ABE) [21] is used for flexible and fine grained access control in cloud computing [39].It has restriction scalability of IOT systems.

To overcome this challenge, we introduce (DPD-ICIOT) to allow IOT data to be securely shared based on publisher-defined policy. It gives flexible authorization from publishers to users. In DPD-ICIOT, CPABE B is involved to provide flexible Authorization, balance, the centralized management and distributed retrievals for attributes, Attribute Manifest (AM) and Data Manifest (DM) are introduced and distributively stored in the network. Automatic Attribute Self-Update Mechanism (AASM) to enable the update of attribute without querying the distinct server to reduce the large traffic overhead of attribute updates .The cost of bandwidth in packet transmission concerned for attribute retrievals can be highly reduced.

2. RELATED WORK AND LITERATURE SURVEY

Encryption based access control is an effective method where data are encrypted by end users and only authorized users are given decryption keys. This can also prevent the threats during transmission of data [13], [15]. Traditional Public Key (PK) methods are not suitable for data encryption because it may give multiple samples of ciphertext for the same data where infinite data receivers in the system.

To address this issue, attribute based access control schemes [3],[5] are evaluated by address attribute based encryption [6]. This only gives a single copy of ciphertext for each data without considering the number of data consumers during the data decryption. Searchable encryption algorithms [16], [17] are introduced to enable search on encrypted cloud data.

Based on this problem, work in [8], [12], [18-21] is used to hide the access policy. These are two constructions are to hide the access policy CAPABE IS ONE of the construction with AND gates with multi valued attributes with wildcards [8], [9].It is a fully secure ciphertext – policy attribute based encryption scheme. To support this, a method to hide attributes value in access policy expressed in LSSS structure.

Hidden vector encryption [10] and inner product encryption [11] are the existing schemes that partially hide the access policy. The attribute names are not privacy oriented in this access policy. To overcome the issue, we have seen a distributed publisher Driven secure data sharing for ICIOT (DPD-ICIOT) to enable IOT data to be securely shared based on publisher defined policy. To improve this Attribute Manifest (AM) and Data Manifest (DM) are introduced and distributed on the networks manifest describe the attribute and data .To avoid overhead Automatic Attribute Self Update Mechanice (AASM) is used. By this work we came to know the total bandwidth cost is reduced and computation overhead is minimized.

3. EXISTING SYSTEM MODEL (BIG DATA)

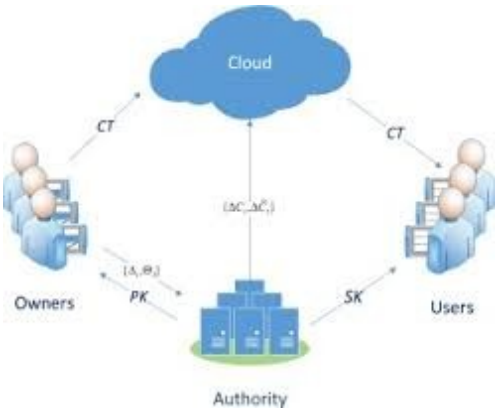


Fig2 system model

The data access in control System, shown in fig.2 the model has 4 elements, they are

1) Cloud Server

2) Attribute Authority
3) End Users
4) Data Consumer

1) Cloud Servers:(data storage or Big data publishers)

The servers involved in storage, share and process big data (large volume of data) in the system are called as cloud servers. The cloud servers are lead by cloud service providers. These cloud servers has no right to access decision. The cloud servers are less trusted by end users to use the access policy by them. They don't contact with the end users or data consumers.

2) Attribute Authority (Authority of attributes)(Attribute Management)

Authority that maintain and control all the attributes in the system and give attributes from attribute space to end users; this authority is called attribute authority. It is also known as key generation centre. It is trusted by the end users in the system. It gives secret keys and generates public parameters to end users.

3) End User

End users are the owners or producers of the data, who stores their data into the cloud. They encrypt their data with CP-ABE. End users are supposed to be the honest persons in the system.

4) Data Consumers

These are the people who request for the data from cloud server. Data consumers can consume the data, when their attributes meet the conditions or the access policies of the data.

Existing system involves in algorithms like SetUp, KeyGen, Encrypt, Decrypt.

Existing algorithm is constructed using these algorithms.

B. Definition of Our Scheme

Our big data access control scheme consists of the following algorithms: Setup, KeyGen, Encrypt, and Decrypt.

• *Setup(1λ) → (PK,MSK):* The setup algorithm takes as input a security parameter λ. It outputs the PK and master secret key.

• *KeyGen(PK,MSK, S) → SK:* The key generation algorithm takes as inputs the PK, the master key MSK and a set of attribute *S*. It outputs the corresponding secret key *SK*.

• *Encrypt(PK,m, (*M, *ρ)) → (CT, ABF):* The data encryption algorithms contains: data encryption subroutine Enc and ABF building subroutine ABFBuild.

*Enc(PK,m, (*M, *ρ)) → CT:* The data encryption subroutine takes as inputs the PK, the message *m*

and access structure *(*M, *ρ)*. It outputs a ciphertext*CT*.

– *ABFBuild(*M, *ρ) → ABF:* The ABF building subroutine takes as input the access policy *(*M, *ρ)*. Itoutputs the ABF.

• *Decrypt(*M, *ABF, PK, SK, CT) → m:* The decryption algorithm consists of two subroutines: ABFQuery and Dec.

– *ABFQuery(S, ABF, PK) → ρ_:* The ABF query algorithm takes as inputs the attribute set *S*, the ABF and the PK. It outputs a reconstructed attribute mapping $\rho\_ = \{$(rownum,

International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 04 Issue-17
December 2017

att)}S, which shows the corresponding row number in the access matrix M for all the attributes att ∈ S.

– *Dec(SK, CT, (*M, ρ_*))* → *m or* ⊥*:* The data decryption algorithm takes as inputs the secret key *SK*, the ciphertext *CT* as well as the access matrix M and the reconstructed attribute mapping ρ_. If the attributes can satisfy the access policy, it outputs the message *m*. Otherwise, it outputs ⊥.*C*

Exiting System Advantages:

1. It is an Efficient & fine grained big data access control scheme with privacy, in this, the whole attributes are hidden in access policy rather than only the values of attributes.
2. A novel ABF to know the presence of attribute in access policy and place at the right location or position in it.
3. Security proof and reduce computation overhead to some extent.

Existing System Disadvantages:

1) It has a chance of privacy leakage using traditional methods and algorithms.
2) It has to face challenges in decrypting the data, construction is cost orientated.

4. PROPOSED SYSTEM

The proposed system is a combination of internet of things and big data. In this first work to investigate, publisher driven fine grained access control in a ubiquitously distributed catching methods for ICIOT.

We combine CP ABE with the complex ICN, CCN / NDN [6], [9] and give novel PDP-ICIOT process for providing, a system with distributed, secure and flexible data sharing for ICIOT. A key chain mechanism for efficient data encryption and decryption; AM to enable the close copy retrieves of attributes and introduced an AASM to employ efficient updating of attribute.

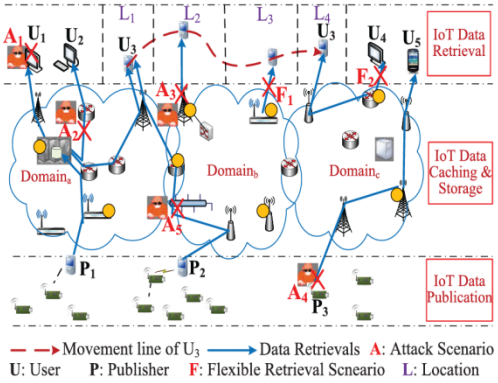


Figure1. System Description (IOT)

1. User
2. Publisher
3. Network Operator and Authority (NOA)
4. Data Sharing Authority (DSA)

Users:

The people who receive the data

Publisher:

The entity who publishers IOT data for users

Network Operator & Authority (NOA):

This element involves in operating network containing of routers, gateways and access points, which are potentially equipped with caches (storages). Security policies functions for the dev ices in the network i.e.) identify management, authentication.

International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 04 Issue-17
December 2017

Data Sharing Authority:

The element remembers publishers to give access privileges to users for providing their data securely.

Security Requirements

1) S1-integrity for IOT data name and database.
2) S2-efficient and flexible authentication.
3) S3-publisher identity authentication.
4) S4-User identity authentication.

5. DPD-ICIOT SCHEME OR METHOD

TABLE I
SECURITY NOTATIONS

Symbols	Descriptions
PT	Policy tree, the graph representation of the access policy
S	The set of attributes of a User
MK	Master key for key server with CP-ABE [21]
PK	Public key for key server with CP-ABE [21]
$PriK$	Private key generated based on a set of attributes using CP-ABE
$PriK_{ti,\ Ux}$	Private key generated based on a set of attributes using CP-ABE at time ti for U_X
SK	Symmetric key for data encryption
KEK	File lockbox key
$\{M\}_{(PK,\ PT)}$	Encryption of data M using CP-ABE with the public key as PK and policy tree as PT
$KeyGen(MK,\ S)$	Key generation using CP-ABE with the master key as MK and attribute set as S
$Decrypt(CT, PriK)$	Encryption using CP-ABE with the cipher-text as CT and private key as $PriK$
$\{M\}_K$	Encryption of data M using key K
$H(M)$	Hash of data M

There are 4 components in Data Access Authorization.

1) Setup :

Select the bilinear group & master key (M_k) public key DSA gives P_k to publishers & users then generates AMS;DMS by following the requests of publishers, & keeps in the network by the help of approach called ICN.

2) Generation of key:

In DSA, the private keys are generated. For user by the help of function key Gen (M_k, S) accruing the attributes, & the updated values of the attributes based on AASM.

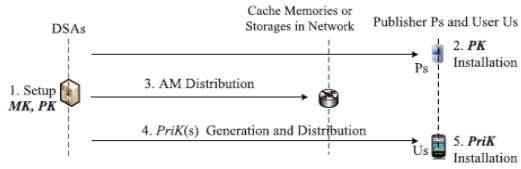
DSA sends the private keys to users. Users install there private keys with the related attributes.

3) Encryption:

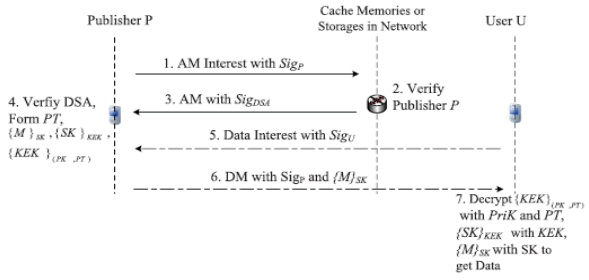
After searching for a set of IOT data, the publisher receives the related. This is done using Internet or data paradigm from network obtains values for attributes using AASM. Publisher from a PT depending on the values of attribute corresponding to its demands. Publisher encrypt Message M, with key chain mechanism or scheme, where ' S_k' is used to encrypt data using symmetric encryption.

To lock 'S_k' , KEK is used Encyption is CP-ABE is used to encrypt KEK & get KEK(P_k ,PT).

Users are friendly with the attackers, those users should be excluded or eliminated from the policy while encrypt data, he or she get the revoked list from the network & excludes there users from data access by eliminating their corresponding attributes from the access policy trees.



(a)



(b)

4) Decryption:

In this phase user selects the private key from the PriK set as per the current time for the talent attributes. Next decrypt the {KEK}(P_k ,PT) using the private key using function Decryt (C_T ,PriK).

The key exchange & operation in DPD – ICIOT are provided.

6. SYSTEM EVALUATIONS

The existing CP-ABE scheme, all the attribute values and attribute updates need to be provided through centralized servers, such as attribute server and DSAs. In contrast, the attribute values are described in AMs and retrieved from close caches. Herein, we perform system evaluations to compare the existing CP-ABE scheme with the proposed DPD-ICIoT scheme. We consider that the metric for comparison is the ratio between the bandwidth cost of the DPD-ICIoT scheme at the lowest performance situation with at most one cached copy in one domain and the bandwidth cost for CP-ABE. The bandwidth cost is defined as the bandwidth consumption for communications.

Assume that the network is divided into many domains. In each domain, one piece of AM or DM or data chunk can only be cached at most once, which is the lowest performance for CCN. If more AMs are cached, the cost for AM retrieval will be reduced further. CCN is utilized as the method for data retrieval.

Based on the above assumptions, a proposed network can be modeled as an undirected, connected graph $G = (V; E)$, where V is a finite set of vertices (network nodes), and E is the set of edges (network links) representing connection of those vertices. N denotes the total number of nodes in V. It is assumed that each domain has the same size and K represents the number of nodes in one domain. For each domain, there are m gateway for connecting globally with other domains.

Thus, the total number of gateways is $m \cdot N/K$. Let l be the average physical hops for one node to send packet to another node in one domain, and L be the average number of hops to send packets from one domain to another domain. The packet size is assumed to be PSType. That is, Interest size is PSInterest, and AM packet size is SAM. To transmit one packet in one domain, the bandwidth cost consumed for transmission is $l \cdot$ PSType. It is assumed that g denotes the total number of cached induplicate attributes in the entire network. We assume each attribute is associated with one AM. Let f be the average number of copies for each AM. It is assumed that the attributes are averagely updated R times during the period that one publisher uses it, and each data can only be cached at most once in one domain. We assume T to be the average retrieval times for one piece of AM in a period by different publishers. Let pL be the probability for intradomain AM retrieval when an AM request occurs. The interdomain AM retrieval occurs with the probability $1 - pL$. We assumed that AASM can be used throughout the period in the DPD-ICIoT scheme. That is, after AM is retrieved, publishers do not need to retrieve it from the network again. The notations for performance analysis are summarized in Table II.

The objective is to model the bandwidth cost for AM retrievals in the proposed network in a period. The total cost consumed during a period equals to the sum of the cost consumed in AM retrieval procedures. We need to model the bandwidth cost of AM retrievals during a

International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 04 Issue-17
December 2017

period through the DPD-ICIoT scheme. For the AM retrieval, the publishers obtain AM from the local domain with probability *pL* and from other domains with probability 1−*pL*. Here, we do not consider the complex situation on caching, and just assume the data are precached in *f* times in the whole network. It can be obtained that $pL = f/(N/K)$ in the DPD-ICIoT scheme. Then, we obtain the total bandwidth cost consumed in the AM retrieval procedures in DPD ICIoT in a period as follows:

$$\begin{aligned} \mathrm{TC}_{\mathrm{AM}}^{\mathrm{DPD-ICIoT}} &= \sum_{i=1}^{T}\sum_{j=1}^{g}\{p_L \cdot \mathrm{BC_{LD}} + (1-p_L)\cdot \mathrm{BC_{GN}}\} \\ &= \sum_{i=1}^{T}\sum_{j=1}^{g}\left\{\frac{f}{N/K}\cdot \mathrm{BC_{LD}} \right. \\ &\qquad \left. + \left(1-\frac{f}{N/K}\right)\cdot \mathrm{BC_{GN}}\right\} \end{aligned} \quad (2)$$

Where, BCLD and BCGN denote the bandwidth cost for local domain AM retrieval and global area interdomain AM retrieval, respectively, through the DPD-ICIoT scheme.

7. CONCLUSION

Security is increased for data sharing. We researched the IOT data sharing problem with regard to unauthorized access, illegal modification, & irrpersonation attack, when IOT data are cached in distributed manner in the network.

We contributed in this paper as follows. We provided system descriptions & identified the security requirements for a complex IOT data sharing scenario n distributed caching environment we proposed a novel DPD-ICIOT Scheme. This is to enable secure & flexible access-control for IOT data, which absorbs the merits from both CP-ABE & CNN. DPD-ICIOT Scheme involves a key chain mechanism to give efficient cryptographic operations. The AM & DM are introduced in DPD-ICIOT which are discriminated in the network for fast attribute & data retrieval AASM to realize the updating the attribute automatically in a distributed manner. System evaluations have been performed, DPD-ICIOT. Scheme can normally reduce the bandwidth cost of attribute retrieval compared to existing server-based CP-ABE.