A Review on Attribute Based Encryption

Hye-jin Kim

Abstract

Cloud computing is an emerging technology. It is a basic paradigm which satisfies all the needs of a customer and it may even serve as a fifth utility in near future. In general it refers to both the applications delivered as services over the Internet and the hardware and systems software in the data centers that provide those services. The data center hardware and software is known as a cloud. A huge amount of data is being processed and shared. So, while we are sharing a large amount of data through online there is a chance for the data to get modified by someone else. In order to protect this data from getting modified we provide several security mechanism like access control. One of the mechanism would be by encrypting and sending the data. Encryption plays a major role in protecting the data. Many encryption schemes were proposed but it cannot survive long due to efficiency constraint. So firstly attribute based encryption was proposed which was later modified to key policy based encryption scheme which was again modified by cipher text encryption scheme is and was later again switched to file hierarchy cipher text based encryption. So my project mainly concentrates on File Hierarchy Attribute Based Encryption scheme in which we make use of Hierarchical structures and attributes matching which is mainly important for providing access control to the data.

Keywords: attribute, encryption, hierarchy, security, access control, cipher.

1. Introduction

Although many researchers have tried to outline cloud computing, no single, agreed-upon definition exists nevertheless. The North American country National Institute of Standards and Technology (NIST) defines it as follows: cloud computing may be a model for facultative convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) which will be speedily provisioned and free with stripped-down management effort or service supplier interaction. This cloud model promotes accessibility and is composed of 5 essential characteristics, 3 delivery models, and 4 readiness models.

To understand the importance of cloud computing and its adoption, we have a tendency to should perceive its principal characteristics, its delivery and readiness models, however...
customers use these services, and the way to safeguard them. The 5 key characteristics of cloud computing embody on-demand self-service, ubiquitous network access, location independent resource pooling, fast snap, and measured service, all of that square measure in gear toward exploitation clouds seamlessly and transparently[1][2].

Measured services are primarily derived from business model properties and indicate that cloud service suppliers management and optimize the employment of computing resources through machine-driven resource allocation, load leveling, and metering tools. Applications running on or being developed for cloud computing platforms create varied security and privacy challenges looking on the underlying delivery and readying models[3-5].

The 3 key cloud delivery models square measure code as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS). In IaaS, the cloud supplier provides a collection of virtualized infrastructural parts like virtual machines (VMs) and storage on that customers will build and run applications. The applying can eventually reside on the VM and also the virtual software package. Problems like trusting the VM image, hardening hosts, and securing inter-host communication square measure vital areas in IaaS. PaaS allows programming environments to access and utilize further application building blocks. Such programming environments have an obvious impact on the applying design, like constraints on that services the applying will request from associate OS. As an example, a PaaS atmosphere would possibly limit access to well-defined elements of the filing system, so requiring a fine-grained authorization service.

Finally, in SaaS, the cloud suppliers alter and supply application code as on-demand services. As a result of shoppers acquire and use code parts from completely different suppliers, crucial problems embody securely composing them and guaranteeing that info handled by these composed services is well protected. Cloud readying models embody public, private, community, and hybrid clouds. Public clouds square measure external or in public offered cloud environments that square measure accessible to multiple tenants, whereas private clouds square measure usually tailored environments with dedicated virtualized resources for explicit organizations. Similarly, community clouds square measure tailored for explicit teams of shoppers.

2. Attribute Based Encryption

Attribute based mostly coding is a vital security idea which will be applied to virtually any role based system these days to supply knowledge confidentiality and integrity.
A user’s knowledge is encrypted and keep on the net. One downside of ancient coding schemes is that this knowledge is solely shared at a rough grain level, which means that any user with the secret writing key will decipher this knowledge. ABE permits a user to encode knowledge in such the simplest way that the user will share it at a fine grained level.

Let’s inspect an example.

Suppose a user Adam has several social connections that he categorizes into one or several of the teams friends, colleagues, family and neighbors. Adam includes a knowledge X that he would really like to share along with his friends and colleagues. So as to share this knowledge along with his friends and colleagues, Adam should generate a coding and secret writing key combine, encode the information and share the key along with his friends and colleagues. Adam has another knowledge Y he would really like to share along with his family and friends and family. Again, Adam has to generate a key combine, encode knowledge Y and share the secret writing key with friends and family. The matter here is that for every content that Adam produce, he should generate a replacement key combine. A straightforward answer to the on top of answer would be to come up with a key combine for every class of social connections. Thus Adam would generate a key combine for friends, one for family so on. Currently to share knowledge X, Adam encrypts this knowledge with friends coding key and share this cipher text with friends and encrypts knowledge X with colleagues coding key and share this knowledge with colleagues. This answer would work nice and improve potency we tend as storage used since we generate less keys and store less keys.

However, social relations don’t seem to be as straightforward as outlined on top of, and one social association of Adam might be quite one amongst the given classes. As an example, a social association is each a disciple and family or each a disciple and colleague. Also, Adam might want to limit sharing an information to a lot of advanced set of users. Let’s assume that Adam has another knowledge Z that he would solely prefer to share with persons United Nations agency are each his friend and colleague. With our current theme, to try and do this Adam would encode knowledge Z with the coding key of friends to induce a ciphertext CT, so more encode this ciphertext CT with the coding key of colleagues. Currently solely someone United Nations agency is each a disciple and a colleague will decipher this knowledge.

The on top of theme but is simply broken through collision. knowledge Z is encrypted by each the coding keys of friend and colleague. albeit this knowledge is supposed for someone United Nations agency is each a disciple and a colleague, if someone United Nations agency has the friend secret writing key and another United Nations agency has the colleague secret writing key conspire, they will still decipher this knowledge.
ABE solves the on top of drawback. In ABE policies ar delineate through attributes (age, relationship, trust, location, etc.). From AN OSN perspective, the classes of social connections ar treated as attributes. Adam is ready to encode the information in such the simplest way that as long as the attributes match a given key then the information is decrypted. Users colluding cannot decipher the information.

ABE uses a tree-based access structure that should be happy with a given set of attributes so as to decipher the information. The tree-based access structure permits the encryptor to specify that attributes will decipher the information. It uses operators like AND, OR and k-of-n. AND is sometimes best-known as ‘n of n’ and OR is thought as ‘1 of n’. As an example, if Adam needs to encode an information P specified solely somebody with the attributes friend AND colleague or the attribute family will decipher it, the tree-based access structure would seem like Figure 1.

![Fig. 1] ABE Access Structure

In figure one, we have a tendency to see that every leaf on the tree returns true or false. The tree is traversed from leaves to root. We have a tendency to see that from the lowest right, a user desires all 2 of the attributes friend and colleague to satisfy this branch. Then once this level is traversed, the second level is traversed, and here we have a tendency to see if a user could be a family or glad the previous traversal, it might come true since the k of n needs her is one out of two. There area unit 2 sorts of variant of attribute primarily based cryptography, one is key-policy attribute primarily based cryptography (KP-ABE) and alternative is cipher-policy attribute based cryptography (CP-ABE).

### 3. Key-policy Attribute Based Encryption (KP-ABE)

In KP-APE, the owner of the info creates a key. Victimization the key, the owner encrypts
the info such a ciphertext is labelled with a group of attributes. The non-public key (decryption key) given to others to decode the info is related to a tree-based access structure that specifies that ciphertext the key will decode. The tree-based access structure contains leaves that are related to attributes. A user is in a position to decode a cipher text if the attributes related to the ciphertext satisfies the user’s key access structure[2]. Below are some applications of KP-ABE taken directly from the work in [2].

3.1 KP-ABE Applications

An necessary application of KP-ABE deals with secure rhetorical associate analysis: one in all the foremost important wants for electronic rhetorical analysis is an “audit log” containing a close account of all activity on the system or network to be protected. Such audit logs, however, raise important security concerns: a comprehensive audit log would become a prized target for enemy capture. Simply encrypting the audit log isn’t spare, since then any party that must lawfully access the audit log contents (for instance a rhetorical analyst) would need the key - thereby giving this single analyst access to primarily all secret data on the network. Such problematic security problems arise in nearly each secure system, and significantly in large-scale networked systems like the worldwide data Grid, wherever various secret, high secret and extremely classified data can get to seem mixed in distributed audit logs.

The KP-ABE system provides a beautiful resolution to the audit log downside. Audit log entries may be annotated with attributes like, for example, the name of the user, the date and time of the user action, and also the sort of information changed or accessed by the user action. Then, a rhetorical analyst charged with some investigation would be issued a secret key related to a specific “access structure” - which might correspond to the key granting a specific quite encrypted search; such a key, as an example, would solely open audit log records whose attributes happy the condition that “the user name is Bob”.

Another application of KP-ABE would be a brand new broadcast situation that we tend to decision targeted broadcast. Think about the subsequent setting. A broadcaster broadcasts a sequence of various things, every one labeled with a group of attributes describing the item. For example, a TV broadcaster may broadcast associate episode of the show “24”, and label this item with attributes like the name of the program (“24”), the genre (“drama”), the season, the episode range, the year, month, and date of original broadcast, the present year, month, and date, the name of the director, and also the name of the manufacturing company. Every user is signed to a unique “package”. The user package describes associate access policy, that
in conjunction with the set of attributes describing any specific item being broadcast; verify whether or not or not the user ought to be ready to access the item. As an example, a TV user might want to subscribe a package that enables him read episodes of “24” from either the present season or Season three. this might be encoded as policy as (“24” AND (“Season: 5” OR “Season: 3”)).

4. Ciphertext-policy Attribute Based Encryption (CP-ABE)

Contrary to KP-ABE, in CP-ABE system, a user’s personal key’s related to a group of attributes. Once a celebration encrypts a message during this system, they specify associate associated access structure over attributes and associate this access structure with the ciphertext. A user can solely be ready to rewrite a ciphertext if that user’s attributes withstand the cipher text’s access structure.

CP-ABE is analogous to the recent work of Sahai and Waters, and KP-ABE by Goyal but CP-ABE need considerably new techniques. In KP-ABE, ciphertexts area unit related to sets of descriptive attributes, and users' keys area unit related to policies (the reverse of CP-ABE). In KP-ABE, the encryptor exerts no management over UN agency has access to the information she encrypts, except by her selection of descriptive attributes for the information. Rather, she should trust that the key-issuer problems the acceptable keys to grant or deny access to the acceptable users. In alternative words, in the intelligence is assumed to be with the key establishment, and not the encryptor. In CP-ABE, the encryptor should be ready to showing intelligence decide UN agency ought to or shouldn’t have access to the information that she encrypts [3]. CP-ABE permits for a brand new kind of encrypted access management wherever user’s personal keys area unit such by a group of attributes and a celebration encrypting knowledge will specify a policy over these attributes specifying that users area unit ready to rewrite. CP-ABE is appropriate for imposing access management on knowledge supported a group of attributes. Below area unit some applications of KP-ABE taken directly from the work of Bethencourt .

4.1 CP-ABE Applications

In several things, once a user encrypts sensitive knowledge, it’s imperative that she establish a particular access management policy on UN agency will decipher this knowledge. As an example, suppose that the FBI public corruption offices in city And San Francisco are work an
allegation of felony involving a San Francisco persuader and a Tennessee legislator. The top
government man might want to code a sensitive note so solely personnel that have sure
credentials or attributes will access it. As an example, the top agent might specify the
subsequent access structure for accessing this information: (("Public Corruption Office" AND
("Knoxville" OR "San Francisco")) OR (management-level 5) OR ("Name: Charlie Eppes")). By
this, the top agent might mean that the note ought to solely be seen by agents UN agency
work the general public corruption offices at city or San Francisco, FBI officers terribly high
within the management chain, and a advisor named Charlie Eppes. As illustrated by this
instance, it can be crucial that the person in possession of the secret data be able to choose an
access policy based on specific knowledge of the underlying data. Furthermore, this person
may not know the exact identities of all other people who should be able to access the data,
but rather she may only have a way to describe them in terms of descriptive attributes or
credentials.

5. Hierarchical Attribute Set Primarily Based Encoding

Hierarchical attribute set primarily based encoding (HASBE) that is associate degree extension
of HABE (Hierarchical Attribute primarily based Encryption). In HASBE every information
owner/consumer is managed by a site authority. A site authority is directed by its parent
domain authority or sure authority. Information house owners, Domain authorities, information
customers, and also the sure authority ar planned in a very hierarchical data structure. HASBE
uses linear mapping system for encoding and decoding. Information encryptor specifies
associate degree access structure for a cipher text that is stated because the cipher text policy.
Solely users with decoding keys whose associated attributes, laid out in their key structures,
satisfy the access structure will rewrite the cipher text. HASBE uses a algorithmic set primarily
based key structure wherever every part of the set is either a group or a part love associate
degree attribute.

User stores information on the cloud which may be retrieved by decrypting a similar
through a personal key provided. This keeps the non-public information confidential. Firstly, a
user must register together with his entire attributes. Once user fills register kind then the
corporate executive approves all the small print of user, then corporate executive give one key
to user. Once user gets that key he will access it sort of a arcanum at the time of login. User
can store all information by encoding public key and user will retrieve decrypted information
that uses same public key and personal key. After that, if user desires to ascertain his own
information then he uses the assigned non-public key and arcanum. Once manager desires to access employee’s attribute, that is generated by selecting the accessible attributes. If any lower authority is absent then higher authority is liable for all work associated with lower authority. Once user is transferred from one location to a different location, then all his information is updated in information itself. The manager can assign tasks and guide the staff operating below him. Therefore the management of assignment of tasks to workers ought to be wiped out a way that’s famous to himself and various worker with the permission of corporate executive publically domain. Conjointly at the time of viewing of his personal data mistreatment non-public domain ought to be specified he might access it instead of some unauthorized user.

6. Conclusion

To understand the importance of cloud computing and its adoption, we have a tendency to should perceive its principal characteristics, its delivery and preparation models, however customers use these services, and the way to safeguard them. The 5 key characteristics of cloud computing embody on-demand self-service, ubiquitous network access, location independent resource pooling, fast physical property, and measured service, all of that are intermeshed toward mistreatment clouds seamlessly and transparently. More security related issues should be considered deeply later[6-8].

References


