ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 7, July 2017

Security on Decrypting Cloud data using KP-ABE

R.S.Sanjuvigasini [1], Dr.R.Shanmugavadivu [2]

Research Scholar, Department of Computer Science, PSG College of Arts and Science, Civil Aerodrome Post, Coimbatore, India[1]

Associate Professor, Department of Computer Science, PSG College of Arts and Science, Civil Aerodrome Post, Coimbatore, India[2]

ABSTRACT: **"Cloud Computing"** Cloud computing is a type of computing that relies on *sharing computing resources* rather than having local servers or personal devices to handle applications. In cloud computing, the word cloud (also phrased as "the cloud") is used as a metaphor for "*the Internet*," so the phrase "*cloud computing"* means "a type of Internet-based computing," where different services such as servers, storage and applications are delivered to an organization's computers and devices through the Internet. Cloud is aimed at sharing of data through internet. Data security and policy are the critical issues for remote data storage. A security user enforced data access control mechanism must be provided before cloud users have the liberty to outsource sensitive data to the cloud for storage. Which can be overcome by Key-Policy Attribute-Based Encryption (**KP-ABE**) is a promising cryptographic primitive which enables fine-grained access control over sensitive data.

KEYWORDS: Access control, Cloud Computing, Security Risks, Cipher Text, KP-ABE.

I. INTRODUCTION

"*Bob Savage's"* speech delivered to Science Foundation Ireland's (SFI) forum on Cloud Computing is one of the most significant transformations in information technology with many advantages to both companies and end users. Cloud file sharing, also called *cloud-based file sharing* or *online file sharing*, is a system in which a user is allotted storage space on a server and reads and writes are carried out over the Internet. Cloud file sharing provides end users with the ability to access files with any Internet-capable device from any location. Usually, the user has the ability to grant access privileges to other users as they see fit. Although cloud file sharing services are easy to use, the user must rely upon the service provider ability to provide high availability (HA) and backup and recovery in a timely manner. In the enterprise, cloud file sharing can present security risks and compliance concerns if company data is stored on third-party providers without the IT department's knowledge. As a proposal to overcome the risk sharing in cloud is data encryption. Cloud encryption is the transformation of a cloud service customer's data into cipher text.

Cloud encryption is almost identical to in-house encryption with one important difference. The cloud customer must take time to learn about the provider's policies and procedures for encryption and encryption key management. The cloud encryption capabilities of the service provider need to match the level of sensitivity of the data being hosted. But even though data are encrypted the intruders may find some way to decrypt the data. So in this paper we use KP-ABE algorithm to decrypt data. In a key-policy attribute-based encryption (KP-ABE) system, ciphertexts are labeled by the sender with a set of descriptive attributes, while user's private key is issued by the trusted attribute authority captures an policy (also called the access structure) that specifies which type of ciphertexts the key can decrypt. KP-ABE schemes are suitable for structured organizations with rules about who may read particular documents. Typical applications of KP-ABE include secure forensic analysis and target broadcast. For example, in a secure forensic analysis system, audit log entries could be annotated with attributes such as the name of the user, the date and time of the user action, and the

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 7, July 2017

type of data modified or accessed by the user action. While a forensic analyst charged with some investigation would be issued a private key that associated with a particular access structure. The private key would only open audit log records whose attributes satisfied the access policy associated with the private key. The first KP-ABE construction was provided by Goyal et al. [5], which was very expressive in that it allowed the access policies to be expressed by any monotonic formula over encrypted data. The system was proved selectively secure under the Bilinear Diffie-Hellman assumption. Later, Ostrovsky et al. [6] proposed a KP-ABE scheme where private keys can represent any access formula over attributes, including non monotone ones, by integrating revocation schemes into the Goyal et al. KP-ABE scheme.

II. LITERATURE SURVEY

Sahai and Waters [2] first introduced the attribute based encryption (ABE) for enforced access control through public key cryptography. The main goal for these models is to provide security and access control. The main aspects are to provide flexibility, scalability and fine grained access control. In classical model, this can be achieved only when user and server are in a trusted domain. But what if their domains are not trusted or not same? So, the new access control scheme that is 'Attribute Based Encryption (ABE)' scheme was introduced which consist of key policy attribute based encryption (KP-ABE). As compared with classical model, KP-ABE provided fine grained access control. However it fails with respect to flexibility and scalability when authorities at multiple levels are considered. In ABE scheme both the user secret key and the cipher- text are associated with a set of attributes. A user is able to decrypt the cipher-text if and only if at least a threshold number of attributes overlap between the cipher-text and user secret key. Different from traditional public key cryptography such as Identity-Based Encryption [3], ABE is implemented for one-to many encryption in which cipher-texts are not necessarily encrypted to one particular user, it may be for more than one number of users. In Sahai and Waters ABE scheme, the threshold semantics are not very expressive to be used for designing more general access control system. Attribute-Based Encryption (ABE) in which policies are specified and enforced in the encryption algorithm itself. The existing ABE schemes are of two types. They are Key-Policy ABE (KP-ABE) scheme and Ciphertext-Policy ABE (CP- ABE) scheme. That can be discussed further

II. THE RISKS OF ADOPTING CLOUD COMPUTING TECHNOLOGY

1. Security

Security is typically ranked the top cloud computing adoption concern. Key threats include: abusive and nefarious usage; insecure interfaces and APIs; malicious insiders; shared technology issues; data loss or leakage; account or service hijacking, and; general uncertainty due to 'security by obscurity' [5]. Potential security attacks include denial of service attacks, side channel attacks, authentication attacks, man-in the middle cryptographic attacks, spyware and trojans [7]. For example, researchers applied a denial of service attack on a client company from hired EC2 instances, which was not detected by Amazon [11]. Also, researchers found that EC2 was susceptible to side-channel-attacks [13]. Quick easy access for customers also means quick easy access for attackers. More innocently, cloud instances have been found to contain authentication keys in the caches and credit card data, as well as the potential for malicious code to be hidden within the system [10]. Due to high levels of abstraction, it is difficult for users to know what their systems are doing in a public cloud and how they are being protected. The customer's need for visibility and transparency of operation are at odds with the service provider's need to efficiently manage entire data centers and maintain secrecy over its security measures. Opinions vary on how serious this issue is. Some argue that security threats in the cloud are no greater than in on premise data centers. Others argue that the level and quality of protection is better in the cloud due to the greater scale of operation and technical expertise of cloud computing providers. Some argue that security is a joint responsibility of the provider and customer while others claim that, ultimately, security can only ever be the customer's responsibility. Some say the good news is that the same tools for internal security can be used for cloud security. Others say, however, that existing policies, procedures and tools must be extended and supplemented to cater for the particularities of cloud requirements. Many argue that the cloud is not

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 7, July 2017

yet a secure enough option for storing and processing mission-critical or customer-sensitive data, and may never be. Some argue that, regardless, competitive pressures will overcome many cloud risks because the economics of cloud computing are so strong – for providers and consumers – that widespread adoption is inevitable. The Cloud Security Alliance [4] suggests that the issue varies with the cloud service model utilized. The lower down the service stack you go (SaaS, PaaS, IaaS), the greater the responsibility for security that the customer must assume:

• SaaS usually provides the most integrated offering, including a high level of security, with the least customer extensibility.

• PaaS is usually more extensible than SaaS, but offers fewer customer-ready features, including security features and capabilities, enabling/requiring the customer to layer-in needed security.

• IaaS provides enormous extensibility but few if any application-level features. Here, the customer must manage and secure the execution environment. Finally, an additional challenge is to integrate cloud based security with on-premise security. This raises issues of interoperability and standards, discussed next.

2.Lock-in

This category combines several critical risks with characteristics that could be positioned along a spectrum spanning fully proprietary through to standardized services. They include vendor lock-in, technology lock-in, migration, interoperability, architecture, licensing and standards. Due to the rapid emergence of cloud computing through the initiatives of individual companies, most offerings are highly proprietary in nature. This creates challenges in migrating data and applications to the cloud, or switching cloud providers, and puts customers at significant risk if the need arises for systems to interoperate across cloud and in-house environments or to retrieve data and/or applications if a cloud provider withdraws from the market. Furthermore, SaaS data may not be fully retrievable and applications developed on one PaaS may not be portable to, or executable on, another. There are few, if any, ready mechanisms to migrate data and applications to other environments. Compatibility issues tend to increase up the service stack, as described above, reflecting the degree of provider-supplied integration (and, therefore, proprietary solutions and interfaces). Switching costs are high. Hence, vendor/technology lock-in. A related aspect of cloud migration and interoperability is the architecture of existing applications (and data formats) intended to run in the cloud. There is a significant difference between an application running in a cloud environment and an application being able to benefit from cloud computing characteristics such as scalability and dynamism. To utilize the beneficial characteristics of the cloud, an application needs to be purpose-designed for the cloud (a kind of reverse lock-in or lock-out due to design/architecture). Similarly, to interoperate across hybrid environments, some customization is likely to be necessary. Typically, on-premise and legacy systems are not designed for horizontal scalability or mixed mode execution. Auto-scaling infrastructure does not automatically make an application scale or elastic. To avoid these issues, companies need to learn how to build and run applications suited for cloud computing environments. Portability requires standard interfaces but few standards exist as yet. The industry is still too immature. The question of standards, however, is contentious. Some argue that widespread adoption of cloud computing (especially by enterprise users) will remain limited until the problems of interoperability and lock-in are resolved. Others argue that a rush to standards could stifle innovation and constrain the industry from reaching the full potential of utility computing. Nonetheless, various cloud standards initiatives are already underway (see the cloud-standards.org wiki for details). Finally, software licensing may be an issue, depending on the service and software utilized. Some licensing agreements are tied to a physical server and continuous use, making it difficult to move the software to the cloud or virtual servers. In general, this is a commercial matter that must be resolved on a case-by-case basis with each software vendor.

3. Control

This category comprises risks resulting from the reality that control over an organization's data and systems execution ultimately passes to a third party service provider in cloud computing. This can raise important concerns and barriers to cloud adoption because a change in control means a change in risk. These concerns represent part of the down side to the benefits of cloud computing, resulting from not owning the infrastructure. What can be done is

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 7, July 2017

constrained by the permissions (rights) granted by the service provider. A related concern is that effective cloud computing is likely to require increased automation, which creates an increased demand on management capabilities and increased risk as hands-on control is removed. Cloud computing adoption presents significant management challenges, not the least because of the limited availability of cloud monitoring and management tools and the limited capabilities of tools that do exist. For example, tools usually do not integrate with on-premise management tools. Also, existing tools handle applications poorly (compared to hardware and operating systems), especially multi-tiered applications. Other control issues cited in the literature include the problem of instance sprawl. Users may spawn instances unnecessarily and wastefully, just because it is possible and easy. Related is the problem of keeping track of an organization's overall usage of cloud services. If it is so easy and inexpensive for anyone in any department to 'hop onto' the cloud, aggregate costs may balloon. Finally, some commentators also remind us of the human element in cloud computing. People can also feel a loss of control and resist change. Contrary to popular claims, there is a steep learning curve in cloud adoption. Also, it has been widely postulated that the IT function as we know it is under threat. As the need to maintain servers and other data center infrastructure diminishes, the form of the IT function may change. Staff cuts are likely. This can create a classic dependency where the success of transitioning to a new operating model is dependent upon the people who may become redundant as a result of the change.

4. Legal

Legal risks include compliance with jurisdictional laws and regulations, legal liability, contracts and audits. Depending on the nature of the data (and it could be as simple as emails) and the jurisdiction, regulations may apply to where data is stored, how it is handled, and the procedures under which it may be accessed or seized by the courts or governments. Special regulations often apply, for example, to personal details, financial data, and health records, or a requirement may exist for data to remain within a specific country. Cloud virtualization can cause data to be moved around cloud environments, placing it under different state and national laws and even result, unknowingly, in the owner becoming liable for breaching regulations. IaaS providers, such as Amazon Web Service (AWS), typically let the customer specify the domain in which data is to be stored, thereby mitigating some of this risk but this option is not necessarily uniformly provided across the service stack or by all service providers. A key sticking point here is: Who is responsible for compliance? The service provider who processes and stores the data or the customer? Providers argue that they cannot be held responsible because they know nothing about the nature of the data or its compliance requirements. Customers, in turn, have no visibility into the provider's infrastructure or handling of the data. However, a compliance/legal exposure can be created by a vendor leaking, breaching, losing, damaging or impeding access to data. Yet, the typical default contract from most cloud providers (such as AWS) puts the onus for compliance and privacy fully on the customer. Furthermore, cloud vendors typically offer poor service guarantees and limited financial redress if their service fails (such as a percentage of the fees due). This may represent minimal value in comparison to the real cost of service loss to a customer. It is not always clear who is responsible when problems arise or how they will be resolved. Providers also usually claim the right to change their terms and conditions in contracts without notice, by posting them on their website. These issues are major barriers to adoption for enterprises and for moving mission-critical or data-sensitive applications to the cloud. Finally, the cloud presents challenges for auditing, especially of customer data and systems. Traditional forms of auditing may not be possible or permitted by the provider. Alternative approaches may be necessary. Providers may deny access to auditors to protect other multi-tenanted users, to maintain secrecy over its security arrangements, or simply because it does not have the resources to allow each customer to inspect its systems or run audit programs outside of controlled hired instances.

5. Service

This category relates to service features and levels, service availability and reliability, and support. Clearly, quality and continuity of service are important considerations in adopting and continuing to use cloud services. Unfortunately, due to the utility nature of cloud computing, services and service levels are commodity-like in nature, with iron-clad guarantees on services, availability, reliability and support rarely provided. Typically, cloud service level agreements (SLAs) are inadequate, inflexible or nonexistent. Also, service scope varies between providers, partly as a result of differences in service model offerings and partly due to differing business policies. Limited options exist, if any, for

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 7, July 2017

customization of services. For example, a customer has no visibility into his/her relative standing in the multi-tenant environment for support following an outage (who is brought online first?) or for receiving software updates as they become available. This is usually driven by the provider's own priorities. Typically, only basic support is available from the cloud provider (such as AWS) with value-added services provided by third parties. Amazon does not provide end-to-end application support. It supports the compute infrastructure and leaves application support to the customer. While the remaining five categories account for only 16% of the risk factors found, they still amount to substantial adoption barriers in the minds of some industry analysts.

6. Performance

Network latency, data access and storage latency, and overall response and execution times are important issues for some users and applications, given the view that system performance is slower in the cloud and more variable than in on-premise environments. Performance is constrained by Internet speeds, network quality and the distance between the user and the various cloud service providers. Tests show that latency increases with distance [14]. More alarmingly, studies have found that cloud platform performance varies substantially, by up to a factor of 20, depending on the time of day the service is accessed [18]. Performance is also influenced by other factors such as application design (they must be virtualized to operate efficiently in a cloud environment). Architecting applications

for performance and scalability in the cloud is a non-trivial exercise [3]. So, if performance is critical in your service level requirements, the cloud may be a risky option.

7. Cost

One of the great benefits touted for the cloud model is that you only have to pay for what you use when you use it. Is it that simple in practice? Accurately predicting and measuring spend is more difficult under an 'on-demand' costing model. Knowing who used what services when in a large organization is also difficult to track. Add to that the uncertainty about whether the required instances were oversubscribed or under-utilized makes costing enormously difficult. The risk exists for firms to lose control and spend more than they need to under this model. Implications for charge-back to cost centers extend from these difficulties. Also, current prices are low, as vendors compete for market share. However, as the market grows and customers become locked-in, prices may rise. Finally, pay-per-use has financial and tax implications, as IT costs change from capex to opex, which can have positive and negative effects.

8. Governance

Governance involves issues of ownership, decision rights, responsibility, accountability, business risk, due diligence and business policy (such as relating to the control of sensitive data and the use of standards). Cloud computing upsets traditional IT governance arrangements because much of the control transitions to third parties. It can also change the internal structure of IT in user organizations, decentralizing much of the decision-making. This places pressure on the strategic function of IT at the center (head) of organizations. However, these issues do not necessarily weaken internal governance. Rather, they change its shape (its roles and responsibilities). Commentators argue that robust governance is an important entry requirement to benefit from the use of cloud services.

9. Competencies

While cloud computing draws on legacy client-server and service-oriented architectures, it represents a new bundling of pre-existing technologies. Most potential adopters do not have the specific skills to build and deploy cloud applications as quickly and efficiently as the hype suggests is possible. There is a steep learning curve with this computing model. Furthermore, cloud service models and platforms differ in their technical makeup and usage requirements so experiential-based learning can be a barrier to realizing benefits through cloud adoption.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 7, July 2017

10. Industry

Finally, several commentators note that cloud computing, as an industry, is immature so is likely to change over time as industry rationalization occurs. Costing, service models and cloud architectures/infrastructures may change. Providers (small or large) may fail, withdraw or be acquired, representing service continuity risks for customers. Risk averse consumers may adopt a 'wait and see' strategy before joining the cloud market.

Based on these risks, in aggregate, current opinion is that cloud use cases are limited to: when demand is unknown, uncertain or highly variable; when data and applications are not tightly coupled with other data/apps or the points of integration are well-defined; when tight security and control are not so important; when availability and performance are not critical, and; when specific data regulations do not apply.

III. KEY-POLICY ATTRIBUTE-BASED ENCRYPTION (KP-ABE)

Key-Policy Attribute-Based Encryption (**KP-ABE**) is a promising cryptographic primitive which enables fine-grained access control over sensitive data. The key abuse attacks in KP-ABE may impede its wide application especially in copyright-sensitive systems. To defend against this kind of attacks, this paper proposes a KP-ABE scheme which is able to disclose any illegal key distributor's ID when key abuse is detected. In our scheme, each bit of user ID is defined as an attribute and the user secret key is associated with his unique ID. In KP-ABE, a set of attributes is associated with ciphertext and the user's decryption key is associated with a monotonic access tree structure. [3] [4] When the attributes associated with the ciphertext gratify the access tree structure, then the user can decrypt the ciphertext. In the cloud computing, for efficient revocation, an access control mechanism based on KP-ABE and a re-encryption technique used together. It allows a data owner to reduce most of the computational upstairs to the servers. The KP-ABE scheme provides fine-grained access control. Each file or message is encrypted with a symmetric data encryption key (DEK), which is again encrypted by a public key, that is corresponding to a set of attributes in KP-ABE, which is generated corresponding to an access tree structure. The encrypted data file is stored with the corresponding attributes and the encrypted DEK. If and only if the corresponding attributes of a file or message stored in the cloud satisfy the access structure of a user's key, then the user is able to decrypt the encrypted DEK.

That can be used to decrypt the file or message. [3]

- Ciphertexts are labeled with a set of attributes
- Private keys are associated with access structures that control which ciphertext a user is able to decrypt.

KP-ABE scheme consists of the following four algorithms: [3]

- **Decrypt (c, PK, D):** The decryption algorithm takes as input the ciphertext, c which was encrypted under the set of attributes, γ, the public key parameter, PK and the private key, D for access control structure, . It outputs the message m if γ∈ .
- **Setup (1k):** The setup algorithm takes as input a security parameter, 1k and outputs the public parameters, PK and a master key, msk which is known only to the private key generator (PKG).
- **Encrypt (m, PK, γ):** The encryption algorithm takes as input a message, m, a set of attributes, γ and the public parameters, PK. It outputs the ciphertext, c
- **Key Generation (PK msk,):** The key generation algorithm takes PK, as input the public parameters, PK, the master key, msk and an access policy. It outputs the private key, D .

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 7, July 2017

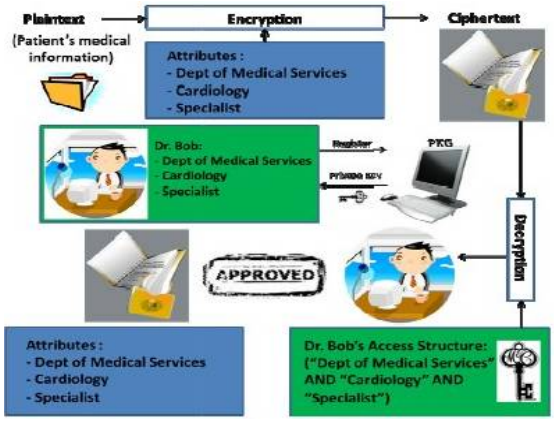


Figure 1: Key-Policy Attribute Policy Attribute-Based Encryption and Decryption

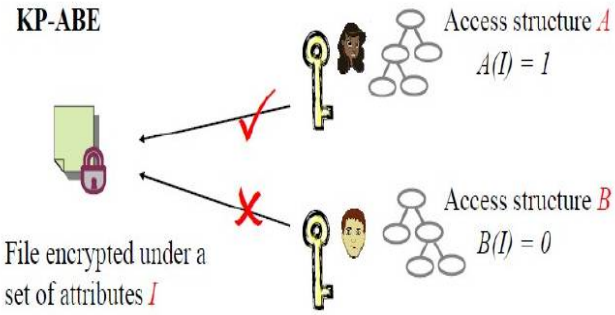


Figure 2: KP-ABE Access control

Figure 1: plain text is encrypted with attributes and the cipher text must work in the form of be decrypted using the same cipher key.

Figure 2: KP-ABE algorithm access tree Structure in which encrypt and decrypt key also the tree structure must same if one is not same then the receiver can't decrypt his data.

IV. EXPREMENTAL IMPLEMENTATION AND RESULT

C1(3,5,6,7)
- K1(1 and 2)
  - K2(3 or 5)
  - K3(1 and 2) or (3 and 7))
    - K4 (3 out of (1,2,3,4,5,6,7))
- K5 (2 out of (1,2,5))

Access Tree

- ("child" and "<120cm") or (2 of ("student", "<20", "disabled",))
- parent(x): parent of a node *x*
- *att(x): if x is a leaf node then return the attribute associated with x*
- num(x): the number of children of a node x
- k(x): threshold value, then 0<=k(x) <=num(x)
- k(x) = 1, the threshold gate is an OR gate
  - k(x) = num(x), it is an AND gate
- index(x): return node's index

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 7, July 2017

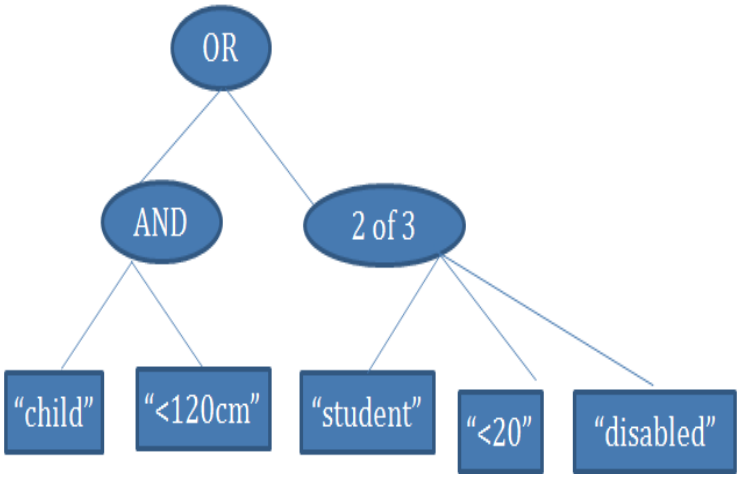


Figure 3: Experimental access tree structure of KP-ABE

Figure 3: Here is the example, we select the student with the attribute of either child with less than 120 cm or student less than 20 who is disabled person.

Set UP

- Bilinear map: e
- e: G1× G1 -> G2
- G1 has prime order p
- g is a generator of G1
- U = {a_1 = "child" , a_2 = "<120cm",….,a_n}
- U is the set of all attributes
- T: U Z_p →
- Product t1,t2,t3,..... tn $\in Z_p$
- MK(master key)
- T1,t2,….tn
- y$\in Z_p$
- PK(public key)
- T1= g^{t1}, T2=g^{t2},….Tn=g^{tn}
- Y= $e(g,g)^y$

Encryption

This algorithm is made to reduce computational load on host, the algorithm only produce a partial cipher text, that consist of encrypted message, encrypted secret key and the set of authorized attributes.

- Encrypt(M, γ,PK)
  =(γ,M γ^s,Ti^s $\forall$I $\in$ γ)
- M is message, γ is an attribute set
- M $\in$ G2, $\gamma \subseteq$ U
- example: γ = {"child", "student", "<20"}
- s $\in Z_p$

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 7, July 2017

Key Generation

This algorithm is run by the trusted authority in order to generate the secret key for a user with an attribute set.

◈ KeyGen(T, MK)

Choose a polynomial qx for each node:q1, q2, q3, … , q8.

degree(qx) = K(x) - 1

degree(q1) = 0

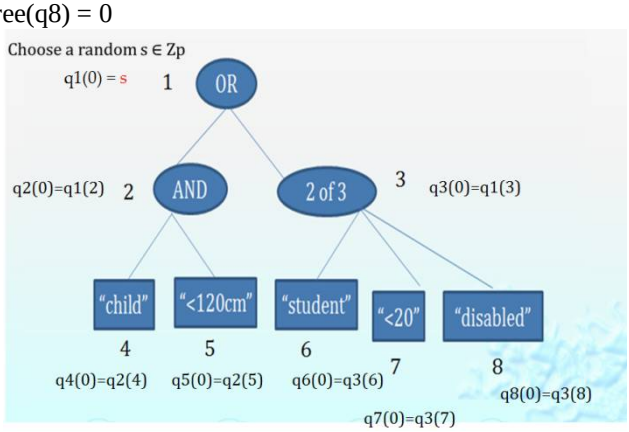
degree(q2) = 1

degree(q3) = 1

degree(q4) = 0

⁞

degree(q8) = 0



◈ For each leaf node x, give

$$Dx = g^{\frac{q_x(0)}{ti}}$$

$$D4 = g^{\frac{q_4(0)}{t_{"child"}}}$$

$$D5 = g^{\frac{q_5(0)}{t_{"<120cm"}}}$$

....

$$D8 = g^{\frac{q_8(0)}{t_{"disabled"}}}$$

Decryption

It takes as input from user the private key is decrypted with the cipher key. The plain message can now be recovered as follows.

◈ $C = (\gamma, MY^s, Ti^s \forall i \in \gamma)$

◈ $\gamma = \{$ "child", "student", "<20" $\}$

◈ Private Key : D

◈ D4...D8

◈ Access tree

$q6(0)=q3(6)$

$q7(0)=q3(7)$

$q3(0)=q1(3)$

$$\left(e(g,g)^{s\cdot q_6(0)\cdot\Delta}\right)\left(e(g,g)^{s\cdot q_7(0)\cdot\Delta}\right)$$

$$= e(g,g)^{s\cdot q_3(0)} = e(g,g)^{s\cdot q_1(0)} = e(g,g)^{s\cdot y}$$

$$e(D6, T_{"student"}{}^s) = e(g^{\frac{q_6(0)}{t_{"student"}}}, g^{s\cdot t_{"student"}}) = e(g,g)^{s\cdot q_6(0)}$$

$$e(D7, T_{"<20"}{}^s) = e(g,g)^{s\cdot q_7(0)}$$

Though this algorithm is an ultimate form of cryptography in which along with the cipher key we use a tree structure to encrypt and decrypt the data. Where the tree structure secure data from the intruder.

V.CONCLUSION

We present the KP-ABE algorithm to encryption and decryption data. This enable an access structure for each encryption key which is to same as decryption key. We demonstrate that, by using KP-ABE encryption data can be decrypted only by using the same access structure. In these schemes, the cipher keys are associated with an access

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 7, July 2017

structure while the cipher text is labeled with set of attributes. To help reduce the threat, cloud computing stakeholders should invest in implementing security measures to ensure that the data is being kept secure and private throughout its Lifecycle.

REFERENCES

1) Changji Wang and Jianfa Luo "An Efficient Key-Policy Attribute-Based Encryption Scheme with Constant Ciphertext Length" Mathematical Problems in Engineering Volume 2013 (2013), Article ID 810969, 7 pages.
2) R. Ostrovsky, A. Sahai, and B. Waters, "Attribute-based encryption with non-monotonic access structures," in Proceedings of the 14th ACM Conference on Computer and Communications Security (CCS '07), pp. 195–203, November 2007. View at Publisher · View at Google Scholar · View at Scopus
3) Parmar Vipul Kumar Ja. RajaniKanth Aluvalub" Key Policy Attribute Based Encryption (KP-ABE): A Review"
4) Paul L Bannerman" Cloud Computing Adoption Risks: State of Play" NICTA and School of Computer Science and Engineering University of NSW Sydney, Australia paul.bannerman@nicta.com.au
5) CSA, "Security Guidance for Critical Areas of Focus in Cloud Computing V2.1", Cloud Security Alliance, December 2009, accessed September 2010 at http://www.cloudsecurityalliance.org/csaguide.pdf.
6) Mr. Anup R. Nimje #1 , Prof. V. T. Gaikwad*2 ,Prof. H. N. Datir^3 "Attribute-Based Encryption Techniques in Cloud Computing Security : An Overview" International Journal of Computer Trends and Technology- volume4Issue3- 2013
7) Mr. Anup R. Nimje #1 , Prof. V. T. Gaikwad*2 ,Prof. H. N. Datir^3 "Attribute-Based Encryption Techniques in Cloud Computing Security : An Overview" International Journal of Computer Trends and Technology- volume4Issue3- 2013. John Bethencourt, Amit Sahai, Brent Waters "Ciphertext-Policy Attribute-Based Encryption" Supported the US Army Research Office under the CyberTA Grant No. W911NF-06-1-0316.\
8) Minu George1, Dr. C.Suresh Gnanadhas2, Saranya.K3," A Survey on Attribute Based Encryption Scheme in Cloud Computing" International Journal of Advanced Research in Computer and Communication EngineeringVol.2,Issue11,November2013.
9) ChangjiWang1,2,3 and Jianfa Luo1,2 "An Efficient Key-Policy Attribute-Based Encryption Scheme with Constant Ciphertext Length" Hindawi Publishing Corporation Mathematical Problems in Engineering Volume 2013, Article ID 810969.
10) Mr. Anup R. Nimje #1 , Prof. V. T. Gaikwad*2 ,Prof. H. N. Datir^3 "Attribute-Based Encryption Techniques in Cloud Computing Security : An Overview" International Journal of Computer Trends and Technology- volume4Issue3- 2013.
11) Attribute-Based Encryption Techniques in Cloud Computing Security : An Overview Mr. Anup R. Nimje , Prof. V. T. Gaikwad, Prof. H. N. Datir