International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 07
March 2018

# Achieving Protection of Data in Cloud Using Flexible Cipher Text Policy – Attribute Based Encryption

Shaik Haseena & Shaik Khaja Mohiddin
[1] MCA Student at VVIT Guntur, [2] Asso. Prof. Dept. of CSE VVIT Nambur, Guntur

**Abstract:** *Self-protection capacities of outsourced information turn out to be note worthily critical in distributed computing. Ciphertext-Policy Attribute Based Encryption (CP-ABE) can powerfully control the client gathering of the scrambled information by characterizing decoding attributes; henceforth has certain capacity of access control. In spite of the fact that there are distinctive plans of CP-ABE, to the extent we know, the greater part of these plans can just express straightforward arrangements with AND, OR and edge attribute tasks, which can't bolster conventional access control approaches. Keeping in mind the end goal to adequately incorporate access control with encryption to fabricate an independent information protection system, this paper proposed an Extended CP-ABE (ECP-ABE) conspire based on the current CP-ABE plot. The ECP-ABE plan can express any Attribute Based Access Control (ABAC) approaches spoke to by number juggling correlation and legitimate articulations that include NOT,<,≤,>,≥,[ ],( ),( ]NOT,<,≤,>,≥,[ ],( ),( ] and )[ ) administrators notwithstanding AND, OR and limit administrators. We demonstrate the Chosen-plaintext Attack (CPA) security of our plan under the Decisional Bilinear Diffie-Hellman (DBDH) supposition in the standard model, and furthermore talk about the test aftereffects of the proficiency of ECP-ABE.*

**Keywords:** Self-contained data protection, Ciphertext-policy attribute based encryption (CP-ABE), Extended CP-ABE, Attribute based access control, Cloud computing.

## 1. INTRODUCTION

Cloud computing incorporates a gathering of PCs that are mutually used to give diverse calculations and assignments. Cloud computing is a standout amongst the most vital IT standards over the most recent couple of years. One of the key advantages that is offered from this IT innovation for the organizations is diminished time and expenses available. Cloud computing is giving organizations and associations to utilize shared capacity and computing assets. It is superior to create and work with the possess foundation. Cloud computing additionally gives associations and organizations to have an adaptable, secure, and financially savvy IT framework. It can be contrasted and the national electric networks that allow associations and homes to connect to a halfway oversaw, productive and financially savvy vitality source. Principle enterprises including Google, Amazon, Cisco, IBM, Sun, Dell, Intel, HP, Oracle, and Novell have put resources into cloud computing and propose a scope of cloud-based answers for people and organizations.

There are distinctive writes and models in cloud computing with respect to the diverse gave administrations. Along these lines, the cloud computing include open cloud, private cloud, crossover cloud, and group cloud. Administration conveyance models, then again, could be sorted as SaaS (Software as an administration), PaaS (Platform as a Service), and IaaS (Infrastructure as a Service). Cloud computing could be normally ordered by two courses: by cloud computing area, and by the offered kinds of administrations. By the area of the cloud, cloud computing is normally grouped: out in the open cloud (where the

computing foundation is facilitated by the cloud seller); private cloud (where the computing framework is relegated to a particular association and not imparted to different associations); cross breed cloud (the utilization of private and open clouds together); and group cloud (it includes sharing of IT foundation in the middle of associations of a similar group) [1]. In the event that the order is based on kind of offered administrations, clouds are grouped in these ways: IaaS (Infrastructure as an administration), PaaS (Platform as a Service), and Software as a Service (SaaS) [1].

Cloud computing as a novel innovation for preparing and exchanging information electronically is these days utilized as a part of relatively every PC framework. It keeps running on a system foundation that is opened for various kinds of assaults. DDoS (Distributed Denial of Service) is a standout amongst the most known assaults that are utilized. Syn treats and also restriction of the clients that are associated with the cloud innovation to the server could be utilized as measures for ceasing Distributed Denial of Service.

Other sort of assault on the cloud computing innovation is man in the center assault. Secure Socket Layer (SSL) is security strategy to defeat this sort of assault. Along these lines, if this security system isn't designed legitimately, verification of the customer and the server won't not execute as it ought to ensure the clients of the cloud innovation from man in the center.

In this way, security difficulties of information protection when utilizing cloud computing must be properly fathomed and limited. When we use cloud computing we run our product on hard plates and CPUs that are not before us. That is the reason clients are having more questions about the security issues when they are utilizing this innovation. In this way, a variety of kinds of assaults could occur in the cloud innovation. Other than the previously mentioned, most known assaults include phishing, IP parodying, message alteration, activity examination, IP ports, and so forth. There are a ton of security methods for information protection that are acknowledged from the cloud computing suppliers, and they all give verification, secrecy, get to control and approval.

## 2. Authentication in Cloud Computing

Validation in cloud computing guarantees that the correct element or individual is gaining admittance to the gave information from the cloud innovation supplier. At the point when confirmation is guaranteed in the cloud computing, it implies that the client's personality is demonstrated to the cloud specialist co-op while getting to the put away data in the cloud. Open and private kinds of cloud are utilizing different plans for verification with RSA. RSA cryptosystem acknowledged diverse models for verification like two factor validation, knowledge based confirmation, and versatile confirmation. AWS (Amazon Web Services) is focused on the secret data exchange between the web server and the program including virtual private cloud [2]. In this setting distinctive confirmation plans are actualized, for example, multifaceted verification, get to administration, AWS character. Figure 1 displays the multifaceted confirmation system from AWS. There is additionally a procedure for validation that is enabling clients to utilize only one secret word keeping in mind the end goal to confirm themselves to numerous administrations [3]. With this system the clients are inclined to honeypot and word reference assaults. The most celebrated IT organizations are utilizing this method like Google, Microsoft, and Facebook.

Keeping in mind the end goal to empower validation of the required IP delivers to some outer site when cloud computing is utilized, Proxy

setting could be utilized. Intermediary URL empowers just trusted destinations to be gotten to.

Subsequently, we can finish up here that for information protection of the cloud innovation the most utilized verification components are: learning based validation, two factor confirmation, versatile verification, multifaceted verification and single watchword confirmation. Information based verification, two factor confirmation and versatile validation are empowered with RSA and advantages of them are lessened expenses and enhanced security.

Multifaceted verification is utilized by AWS to secure the information in the cloud. Advantages of this confirmation component are that it empowers character administration and access administration. Single watchword verification is utilized from Facebook to empower information protection in the cloud. Advantages of this sort of verification system are that it empowers security from honeypot assaults and word reference assaults.

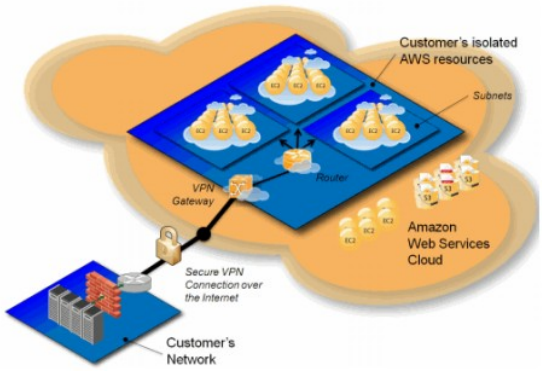


Figure 1. Multi-Factor Authentication from AWS

### 3. Confidentiality in Cloud Computing

Secrecy is a standout amongst the most vital security systems for clients' information protection in the cloud. It incorporates encryption of the plaintext in figure message before the information is put away in the cloud. This procedure ensures the clients' information and even cloud specialist organizations can't change or read the substance that is put away along these lines in the cloud. This sort of protection is offered from Dell information protection and encryption where clients' information is ensured when it is put away on the outer drive or media. Encryption should be possible either utilizing programming or equipment. Extraordinary advantage of this sort of protection is that clients don't have to waste time with the authorize approaches of Dell information protection and encryption. Dell additionally utilizes Transparent File Encryption to control the clients that are getting to the information.

Wuala cloud is another merchant that empowers encryption for the information in the cloud. Encryption is empowered here before PCs are sending the information to the cloud. This is amazing protection in light of the fact that even the supplier can't get to the information. Creators in [4] are proposing encryption technique for cloud computing that is based on progressive attribute. This proposed security strategy for classification in cloud computing gives superior exhibitions and incredible access control. Creators in [5] are proposing encryption technique where proprietors can control the information they have in the cloud.

Privacy is likewise given by the merchant Online Tech which acquires classification in the cloud computing utilizing encryption techniques (like Full Disk Encryption) that scramble put away information on hard plate all through the booting procedure. Entire Disk Encryption is additionally utilized for scrambling the information with the notable AES (Advanced Encryption Standard) calculation. In the event that the gadget that is utilizing cloud computing innovation is lost or stolen there is likewise a bit locker secret word which secures the information on the lost or stolen gadget.

Henceforth, we can deduce in this segment privacy is critical for ensuring the information in the cloud and distinctive sellers offer diverse security methods for guaranteeing the classification. Per illustration, DELL offers equipment and programming based encryption, and also straightforward document encryption. The advantages of this sort of encryption strategies are that they are anything but difficult to execute and mediation of the client isn't required. Wuala is utilizing encryption strategies on PCs and this technique for encryption in the cloud gives preferred standpoint of the clients for getting to the information. Online Tech offers Full Disk Encryption and Whole Disk Encryption so as to empower privacy of the information in the cloud. Advantages of these encryption strategies are that information that are parceled could be unscrambled and information is scrambled very still.

## 4. Access Control in Cloud Computing

Access control is imperative security system for empowering information protection in the cloud computing. It guarantees that exclusive approved clients approach the asked for information that is put away in the cloud. There are distinctive security strategies that empower appropriate access control in the cloud computing. Interruption identification frameworks, firewalls and also isolation of commitments could be executed on various system and cloud layers. Firewall is empowering just substance that is sifted to go through the cloud arrange. Firewall is normally designed agreeing characterized security arrangements set by the clients. Firewalls are typically identified with Demilitarized zones (DMZ) which give extra security of the information.


Figure 2. McAfee Cloud Identity Manager

McAfee is merchant that empowers get to control in the cloud computing. It offers distinctive strategies for get to control as McAfee Single Sign On, McAfee Web Gateway, and McAfee one time secret key. These sorts of security methods empower policy administration and aversion of information to be lost. Figure 2 introduces the cloud personality supervisor offered by McAfee for cloud computing. Fujitsu is another seller that offers get to control with various approval procedures like Virtual System Management and Central Management Authorization. These security systems are successful for averting cross-site scripting and infusion assaults.

## 5. Authorization in Cloud Computing

Approval in the cloud computing is vital for the clients when they login to some cloud benefit since it empowers demonstrate of their personalities. In this way, approval is generally utilized after the confirmation. Prophet Database Vault is a case of security method that empowers approval in the cloud. This security strategy is offered by the merchant Oracle. Application information from various authoritative clients are ensured with this approval technique. Creators in [6] utilize policy based approval technique that is ensuring the security of the clients empowering them to set protection arrangements without anyone else. Along these lines clients are shielding

their information in viable route from unapproved get to.

Approval in the cloud is likewise offered by VMware which incorporates specialist co-ops' strategies with the corporate catalogs and distinctive approaches. Authentications or delicate tokens are utilized for approval of the end clients in secure way. Desert garden Cloud approval empowers security methods based on administration of approvals. Clients logs are kept up with this technique which give area of the clients and data about the utilized gadgets from the clients.

## 6. Recommendations for Improved Data Security in Cloud Computing

We will specify now the most vital proposals keeping in mind the end goal to have secured cloud condition. One of the proposals is a cloud purchaser to be guaranteed that productive administration, hazard and consistence forms exist. This implies security controls must exist in cloud computing like those utilized as a part of customary IT frameworks. Anyway, cloud computing may have distinctive dangers to an association than conventional IT arrangements. In this way, when the association utilizes cloud computing, it is imperative customers to appreciate the level or hazard resistance.

Other proposal is that cloud customers must be guaranteed that the cloud supplier has usefulness and procedures that oversees who approaches the shopper's applications and information. This is fundamental with a specific end goal to have confirmation that entrance to the cloud condition is overseen and controlled. So administration of individuals, parts and personalities is critical to be executed in the cloud condition. At the point when some customer application is moving to the cloud it is vital the supplier to enable the buyer to appoint their client characters into get to gatherings and parts that mirror their business and operational security arrangements [7].

Important factor for secure cloud condition is protection of sufficient protection of information and data. Security contemplations must be connected to information that is hung on some type of capacity framework, and in addition to information that is exchanged over some correspondence interface. Information for cloud computing have different types of hazard as danger of robbery of unapproved divulgence of information, danger of altering, danger of misfortune or inaccessibility of information. Keeping in mind the end goal to secure the information in cloud computing, sufficient controls are required as: thought of all types of information and protection prerequisites, machine of secrecy, formation of information resource index, uprightness and accessibility, and in addition apparatus of personality and access administration [8].

Critical proposal to secure the information on the cloud is to be guaranteed that cloud systems and associations are secure. Cloud buyers must know about interior system assaults like privacy ruptures or exposure of classified information, respectability breaks as unapproved alteration of information, or accessibility ruptures like dissent of administration. That is the reason it is critical for cloud purchasers to assess the inward system controls of the cloud specialist organization with respect to their prerequisites and security strategies that may have. One of the key suggestions is likewise the assessment of security controls on physical framework and offices. Cloud shopper is in control to get confirmation from the supplier that fitting security controls are mulled over, in light of the fact that in the cloud computing, the framework and offices are normally controlled and claimed by the cloud specialist co-op.

### 6.1. Data Protection in the Cloud

Protection of information in the cloud is best expert when we have a blend of encryption, information misfortune anticipation strategies, respectability protection, validation, and approval systems. Whenever sellers and undertakings utilize cryptographic calculations, it is critical these calculations to be notable as recognized by NIST. It is additionally helpful to have re-assessment on a yearly premise of the calculations and keys that are used so as to be guaranteed about the quality of the protection. It is likewise critical associations or partnerships that are utilizing cloud innovation to comprehend the security controls that are identified with the information in the cloud multi-occupant condition. Equipment Security Modules or HSMs are prescribed to store the keys.

### 6.2. Proper Usage of Administrative Privileges

The association that incorporates cloud computing ought to limit authoritative benefits and just to use regulatory records when they are required. Computerized instruments ought to be utilized to stock every single regulatory record and approve that every client that has managerial benefits on workstations, work areas, and servers is approved by senior official. Every regulatory secret word ought to be mind boggling including numbers, letters and unique characters intermixed, without lexicon words in the watchword.

All default passwords for working frameworks, applications, firewalls, switches, remote access focuses, and different frameworks ought to be changed before sending any new gadgets in the organized frameworks. Administration accounts additionally ought to have long and hard to figure passwords changed all the time. Passwords away ought to be encoded or hashed. Hashed passwords ought to take after the direction provided in NIST SP 800-132 or comparative direction.

Access control records ought to be used to ensure that regulatory records will be utilized just for framework organization exercises. Director must utilize one of a kind and distinctive passwords for their authoritative and non-managerial records. This errand can be satisfied through policy and client mindfulness.

Working frameworks ought to be designed in a way that passwords can't be reused in the following a half year. At the point when unsuccessful login to authoritative record is attempted, the framework should issue a log section and alarm.

Multifaceted verification ought to be utilized for all authoritative access, and area regulatory access. This sort of confirmation could incorporate diverse procedures, such as utilizing savvy cards with testaments, biometrics, One Time Password (OTP) tokens and so forth. While empowering multifaceted declaration based verification, the private keys must be ensured utilizing solid passwords or put away in secure and confided in equipment tokens. Overseers ought to be required to get to the framework with utilizing non authoritative and completely logged account.

### 6.3. Wireless Access Control of the Data

Association that is utilizing cloud computing and have remote network(s) should utilize business remote devices for filtering, identification and revelation and business remote interruption discovery frameworks. The security official from the association ought to consistently catch remote movement from the fringes of an office and use business and free investigation devices to determine whether the remote activity was exchanged utilizing the encryption that the association approves or some weaker conventions. In this setting the security authorities ought to likewise utilize remote administration devices on the wired piece of the system with a specific end goal to remove data about the remote potential and gadgets associated with the frameworks that are overseen.

### 6.4. Data Recovery in Cloud Computing

It is imperative every framework that is utilizing cloud computing to has programmed go down methodology in any event once per week, and for frameworks that store delicate data significantly more much of the time than once per week. The general reinforcement methodology ought to try and incorporate the working framework, application programming and information on the machine. Various reinforcements after some time could be likewise executed and arrangements of reinforcement ought to be in consistence with any official or administrative prerequisites.

It is additionally prescribed once per quarter a testing group to make assessment of an irregular example of framework reinforcements with attempting to reestablish them on a proving ground condition. Frameworks that are reestablished ought to be affirmed to ensure that the working framework, application and information from the reinforcement are on the whole useful and in place. Consequently, if there is malware contamination, methodology of reestablish ought to use reinforcement variant which is considered to originate before the first disease.

### 6.5. Boundary Defense of the Data in the Cloud

Limit protection in one association that is utilizing cloud computing could be actualized by utilizing free or business IDS and sniffers to recognize assaults from outer sources to the inward frameworks of DMZ of the association or the other way around. It is additionally gainful to deny interchanges with known malignant IP locations or breaking point get to just to confided in destinations. Association ought to incorporate system based IPS gadgets as an expansion to IDS to piece known terrible marks or conduct of assaults. Two-factor confirmation is commitment when utilizing remote login access as VPN. Just DMZ frameworks ought to speak with private system frameworks of the association through application intermediaries or application-mindful firewalls over approved channels. Odd exercises could be effortlessly recognized if NetFlow accumulation and investigation to DMZ organize is sent.

## 7. ALGORITHMS

A cipher text policy attribute based encryption scheme consists of five fundamental algorithms: Setup, Key Generation, Encryption, Decryption and Attribute revocation.

Setup: The setup algorithm takes no input other than the implicit security parameter. It outputs the public parameters PK and a master key MK.

The setup algorithm chooses a group G of prime order p and a generator g.

Step 1: A trusted authority generates a tuple $G=[p,G,G1,g \in G,e] \leftarrow Gen(1k)$.

Step 2: For each attribute ai where $1 \leq i \leq n$, the authority generates random value $\{ai,t \in Z^* p\}\ 1 \leq t \leq ni$ and computes $\{T\ i,t = ga\ i,t\}\ 1 \leq t \leq ni$

Step 3: Compute $Y= e(g,g)\alpha$ where $\alpha \in Z^* p$

Step 4: The public key PK consists of $[Y,p,G,G1,e,\{\{T\ i,t\}1 \leq t \leq ni\}1 \leq i \leq n]$

The master key MK is $[\alpha, \{\{ai,t \in Z^* p\}1 \leq t \leq ni\}\ 1 \leq i \leq n]$

Key Generation (MK,S): The Key Generation algorithm takes master key MK and the attribute list of the user as input and do the following.

Let L=[L1,L2……Ln]={v1,t1 , v2,t2,,,,vn,tn } be the attribute list for the user who obtain the corresponding secret key.

Step 1: The trusted authority picks up random values $\lambda i \in Z^* p$ for $1 \leq i \leq n$ & $r \in Z^* p$ and computes $D0=g\ \alpha-r$.

Step 2: For $1 \leq i \leq n$ the authority also computes D i,1 , D i,2 =[ g r+λ i a i,t , gλ i ] where

Li = v i,ti The secret key is [D0 Di,1 , Di,2].

Encrypt (PK,A, M): The encryption algorithm takes as input the public parameters PK, a message M, and an access structure A over the universe of attributes. The algorithm will encrypt M and produce a ciphertext CT such that only a user that possesses a set of attributes that satisfies the access structure will be able to decrypt the message. Assume that the ciphertext implicitly contains A.

Step 1: Select s € Z* p and compute C0=gs and C~=M.Ys=M.e(g,g)αs

Step 2: Set the root node of W to be s, mark all child nodes as un-assigned, and mark the root node assigned.

## 8. CONCLUSION

The primary objective of this work was to investigate and assess the security strategies for information protection in the cloud computing. For that reason we broke down and assessed the most imperative security methods for information protection that are as of now acknowledged from the cloud computing suppliers. We grouped them in four segments as per the security instruments that they give: confirmation, secrecy, get to control and approval. In this way, we effectively replied on the key inquiries in the cloud innovation, or essentially said should cloud computing be confided in information protection. We can reason that if all suggested measures are considered giving verification, classification, get to control and approval, at that point the cloud computing can be confided in information protection. We additionally centered around the security issues that ought to be considered inside and out keeping in mind the end goal to have appropriate information security in the cloud. We prescribed critical safety efforts identifying with information protection in the cloud that must be considered. We additionally proposed a great deal of issues that ought to be considered keeping in mind the end goal to have enhanced information security in the cloud computing, as legitimate utilization of authoritative benefits, remote access control of the information in frameworks that utilization remote systems, information recuperation and limit resistance in the cloud.

## REFERENCES

[1] L. Badger, T. Grance, R. Patt-Corner and J. Voas, “Cloud computing synopsis and recommendations (draft), nist special publication 800-146”, Recommendations of the National Institute of Standards and Technology, Tech. Rep. (2011).

[2] U. Khalid, A. Ghafoor, M. Irum, and M. A. Shibli, “Cloud based secure and privacy enhanced authentication & authorization protocol”, Procedia Computer Science, 22, (2013), 680-688.

[3] T. Acar, M. Belenkiy and A. Küpçü, “Single password authentication”, Computer Networks, 57(13), (2013), 2597-2614.

[4] G. Wang, Q. Liu, J. Wu and M. Guo, “Hierarchical attribute-based encryption and scalable user revocation for sharing data in cloud servers”, Computers & Security, 30(5), (2011), 320-331.

[5] C. I. Fan and S. Y. Huang, “Controllable privacy preserving search based on symmetric predicate encryption in cloud storage”, Future Generation Computer Systems, 29(7), (2013), 1716-1724.

[6] D. W. Chadwick and K. Fatema, “A privacy preserving authorisation system for the cloud”, Journal of Computer and System Sciences, 78(5), (2012), 1359-1373.

[7] M. Hange, "Security Recommendations for Cloud Computing Providers", Federal Office for Information Security (2011).

[8] G. Brunette and R. Mogull, "Security guidance for critical areas of focus in cloud computing v2", Cloud Security Alliance, (2009), 1-76.

## Author Profile

**Shaik Khaja Mohiddin**, Working as Assoc. Prof. in CSE Department of Vasireddy Venkatadri Institute of Technology, he completed AMIE from IEI Kolkata, he completed his M.Tech from JNTUK, he is carrying out his research in the area of Cloud Computing in Acharya Nagarjuna University, he has a vast teaching experience of more than 13 years.

**Shaik Haseena** is currently pursuing her Post graduation in Master of Computer Applications (MCA) in Vasireddy Venkatadri Institute of Technology affiliated to JNTU Kakinada. She received her Bachelor degree in B.Sc (computers) from ANR College affiliated to Krishna University.