Completely Anonymous ABE Scheme to manipulate Cloud Data Access Privilege and Anonymity

Syeda Zeba Fatima[1] and Steven Raj[2]

[1] PG Student, Computer Science & Engineering, Guru Nanak Dev College,
Bidar, Karnataka, India

[2] Professor, Computer Science & Engineering, Guru Nanak Dev College,
Bidar, Karnataka, India

Abstract

Cloud computing is a progressive registering worldview, that allows adaptable, on-request, and ease use usage of computing resources, but our data is stored in few cloud servers, and different protection concerns rise up out of it. To protect the storage of cloud many schemes, depending on attribute-based encryption is proposed, where most of the work is done on preserving the data contents security and access control, whereas we are given less attention to privilege control along with privacy of the identity. Here, we showed a semianonymous privilege control plot by name Anonycontrol which direct not just content preservation and also the identity of user in existing schemes. Anonycontrol decentralizes the central authority for limiting the leakage of identity that allows us to achieve the semianonymity. we also develop file access control for the purpose of privilege control, by that all privilege actions are managed on cloud in a fine-grained way.to fully preserves the identity leakage and achieve full anonymity we make use of AnonyControl-F. Thus the security analysis demonstrates that Anonycontrol and AnonyControl-F both are safe under decisional bilinear Diffie-Hellman Assumption and also our scheme is feasible.

Keywords: *cloud computing, attribute-based encryption, access control, anonymity.*

1. INTRODUCTION

Cloud computing is a progressive figuring procedure, in which the resources are provided dynamically through the internet and the storage for data along with computation are sent to somebody or some gathering in cloud. As lots of interest is gathered from both academics as well as from the industry because of its profitability, but this computing possess 3 main obstacles before come in existence.

Preserving the privacy of data is just not about the privacy of data elements only, as cloud computing most attractive part is the outsourcing of data elements for storage, the only things has to be done is controlling the access, more importantly users only need to control the privileges for manipulating the data elements over other users of the system. This is due to when the sensitive data is sent to the servers or to other users, the risk of privacy is emerged from that just because the servers might detect illegal user's data and it access that sensitive data. For that reason not just access of data but also the operations must be controlled.

Secondly, Personal data is at risk as one's id is authenticated on the basis of information for the reason of access control. Now a days people concerns more about the privacy of their identity, the identity privacy also needs to be protected just before the cloud enters our life. That means not any authority nor should any server not know any personal information of the clients.

Lastly, the distributed computing framework should be flexible on account of security break in which some piece of the framework is compromised by attackers/aggressors.

2. LITERATURE SURVEY

If the client has some properties, than only he is able to access the data elements in some dispersed frameworks. For that we make use of a cloud server that is capable enough to hold the data and provide storage to data for the purpose of access control. We adjust with the servers that hold the data which is affecting the sensitivity of data elements. Here we make use of cipher-text policy ABE for complex control of access on the scrambled information [1]. Using this technique the confidentiality of scrambled data elements is maintained even if the provided server for storage is unable to Trust. Further our model is secure for collusion attacks. Our system makes use of attributes to describe the credentials of users, and party is being used to describe to whom it should be decrypted. This means this model is almost same as traditional control access models which is Role-based (RBAC).we give the process required for implementation and gives measurement for performance.

A quality based encryption conspire fit for dealing with different specialists was as of late proposed by Chase. The plan is based upon a solitary specialist characteristic based encryption plot exhibited before by Sahai and Waters. Pursue's development utilizes a trusted focal expert that is innately equipped for unscrambling discretionary figure writings made inside the framework. We display a multi-expert quality based encryption plot in which just the arrangement of beneficiaries characterized by the encoding gathering can unscramble comparing figure content [2]. The focal specialist is seen as "genuine however inquisitive": from one viewpoint it sincerely takes after the convention, and then again it is interested to unscramble subjective figure messages hence damaging the purpose of the encoding party. The proposed conspire, which like its ancestors depends on the Bilinear Diffie-Hellman supposition, has a many-sided quality practically identical to that of Chase's plan. We demonstrate that our plan is secure in the specific ID show and can endure a legitimate yet inquisitive focal specialist. Expanding on the proposition for multi-expert based quality based encryption from [4], we built a plan where the focal specialist is not any more equipped for decoding subjective figure writings made inside the framework. Notwithstanding demonstrating security in the particular ID display, we demonstrated that the proposed framework can endure a fair yet inquisitive focal expert. Since both Chase's plan and the proposed plot depend on a similar hardness supposition, and have a tantamount multifaceted nature, the new plan appears a feasible contrasting option to Chase's development. Be that as it may, since just the proposed strategy is fit for taking care of an inquisitive yet fair focal specialist, the proposed conspire is prescribed in applications where security against such a focal expert is required.

Multiple Authorities ABE is proposed. In this model any one is able to play the role of an authority and there will be no specification for coordinating globally expects managing a set of common reference attributes. Anyone can act like ABE authority by giving those keys that should be public and issuing private keys to various system users which has attributes. User is able to scramble the data elements in any Boolean formula [3]. This model doesn’t make use of any main elements. Developing the system collusion resistant is the main technical issue. Earlier ABE systems achieved assertion resistance when the ABE structure master one of a kind portions (addressing different qualities) of a customer's private key randomizing the key. In any case, the systems each begin from a possibly exceptional master, where we acknowledge no coordination between such experts. We make new frameworks to lace key parts and turn away game plan ambushes between customers with different overall identifiers. We exhibit our system secure using the present twofold structure encryption theory where the security affirmation works by first changing over the test cipher text and private keys to a semi-utilitarian shape and thereafter fighting security. We take after a momentum variety of the twofold structure affirmation strategy due to Lewko and Waters and produce our system using bilinear social occasions of composite demand. We show security under practically identical static assumptions to the LW paper in the subjective prophet show.

As a modern component for safe proficient access control, CP-ABE serve an exceptionally encouraging answer for business applications, for example, distributed computing [4]. Be that as it may, though occur another noteworthy problem anticipated as comprehended, which means, the counteractive action of key mishandle. Vast majority of the present CP-ABE frameworks clubbed this basic usefulness, upsetting the comprehensive usage and business use of CP-ABE frameworks to today. Two handy issues regarding key mishandle of CP-ABE are: (a) Key distribution problem; and, (2) The malevolent key consignment problem of the clients.

Quality Based Encryption (ABE) is a promising open key cryptographic primitive that can be utilized for cryptographically upheld get to control in untrusted capacity. Putting away information on untrusted capacity requires information security for information proprietors as well as postures information insurance from untrusted capacity server. To address this imperative prerequisite, Anonymous Attribute Based Encryption (AABE) is a reasonable primitive that gives clients to get to information from untrusted capacity without uncovering their personalities. In the meantime client information can be put away in untrusted capacity in an encoded shape. While putting away information in a scrambled frame, watchword based question hunt (and information recovery) is a testing research issue. In this paper we display an unknown property based accessible encryption (A2SBE) conspire which encourages client to recover just a subset of archives relating to his picked keyword(s). Client can transfer reports in broad daylight cloud in a scrambled shape, look archives in light of keyword(s) and recover records without uncovering his character. The plan is demonstrated secure under the particular cipher text policy and picked plaintext assault (IND-sCP-CPA) display and specific cipher text-approach and picked watchword assault (IND-sCP-CKA) show. The plan requires little stockpiling for client's unscrambling key and decreased calculation for decoding in contrast with different plans. The mysterious ABE gives a fascinating security highlight beneficiary obscurity notwithstanding information classification and fine-grained get to control of ABE.

3. PROBLEM STATEMENT

Data confidentiality, personal information, and lastly system resilient are the 3 main fundamental challenges that must be handled before using it in our real life.

To protect the privacy of data contents through access control we have developed various techniques. Unlike the confidentiality of data we paid less effort in protecting the privacy of identities during those interactive conventions, users id that are described by their attributes are mainly disclosed to the issuers of the key, and issuers issue that keys by using their attributes. But users want to keep their identities secret while getting their private keys. For that purpose we developed AnonyControl and Anonycontol-F to permit cloud servers to control user’s access privilege without knowing their personality data.

4. PROPOSED SYSTEM

Our users are more conscious about their Identity privacy, For preserving those user Identity privacy this model is developed. The model by name Anonycontrol-F and Anonycontrol is modeled; in this the server holds the user data without knowing the contents of data elements along with privilege for access. Limited data is made available to server.This structure mainly has four entities: Data owners, Data consumers, N attribute authority, and cloud servers.

5. METHODOLOGY

When using the public cloud, many of the users outsource their information some time the large amount of general or private information. Here in public cloud the user is responsible for dynamically checking the integrity of the data by internet. If the user is individual person, and in some limited cases, he may not be position to access through his data onto cloud. Due to his unavailability of access, the company may suffer a huge business hurdles. In order to avoid such cases, user can delegate the proxy to take his stand for data processing and other related operation. The proposed scheme helps to execute this scenario. The scheme allows the user to delegate the proxy and perform the security check to prevent any unauthorized charge. The authority generates the keys for secure access and auditor is responsible for checking the authorization of users.

6. SYSTEM ARCHITECTURE

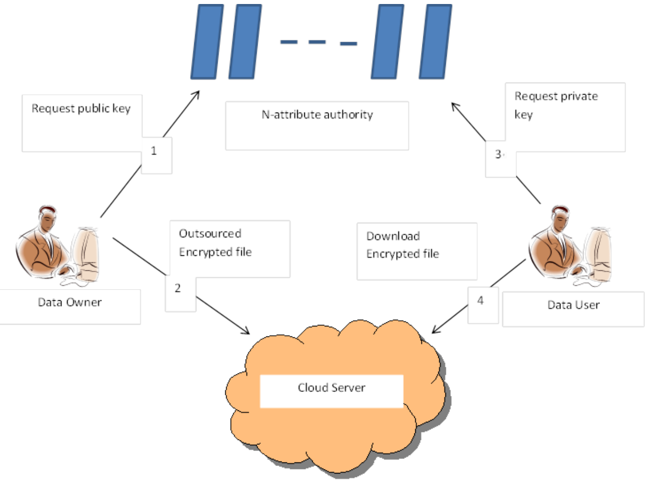

Figure.1 System Architecture

The Architecture is described as follows:

The model by name Anonycontrol-F and Anonycontrol is modeled; in this the server holds the user data without knowing the contents of data elements along with privileges for access. Limited data is made available to server for access.

This structure mainly has four entities:

i. N attribute authority,
ii. Data owners,
iii. Cloud servers and
iv. Data consumer.

N attribute authority: this entity will provide the authorities for either uploading or downloading the files.

Data Owner: once authority will accept the upload request, data owners will upload the files to the cloud server for storage.

Data consumer: Data consumer can access the stored files once the privilege is assigned for access.

Cloud Server: this entity will store all the files in highly encrypted form so that only authorized users can access it. It is assumed here that the server is

Once a data owner gets registered the password is sent to owner for uploading the file, the owner can upload encrypted file to the cloud, the files are stored in such a way that no others users nor even cloud can know any information regarding the stored files, files are stored in highly encrypted forms. The consumer of the files can access those files by make use of the file ID’s, decrypt the files and download the files. Private cloud will provide all private keys to all the clients.

7. IMPLEMENTATION

Cloud computing

This section introduces the information regarding one of the fastest growing technology named cloud computing. The name cloud is derived as it uses the cloud like image and by the type of architecture it generally follows. The cloud incorporates various soft wares and hardware that may presented like service to the customer. Cloud computing enables us to access remote services, computation and software as a service. Cloud computing resources that are existing on the Internet are handled by arbitrator services. This assistance generally provides retrieval to sophisticated networks of servers and other computing resources, advanced applications and software.

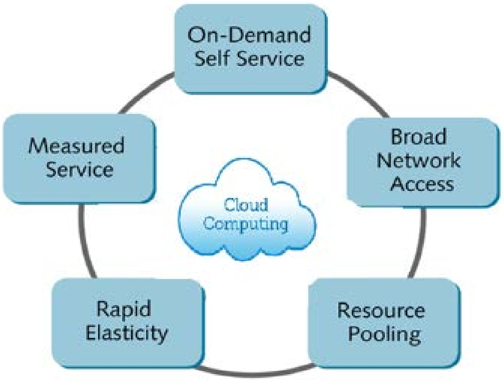

Figure 1.2 Structure of Cloud Computing

7.1 Threats Model

1. Registration -Based Social Authentication Module:

The framework gets ready trustees for a client Alice in this stage. In particular, Alice is first confirmed with her primary authenticator (i.e., password),and then a few(e.g., 5) companions, who likewise have accounts in the framework, are chosen by either Alice herself or the specialist co-op from Alice's companion list and are selected as Alice's Registration.

2. Security Module:

Validation is basic for securing your record and keeping mock messages from harming your online notoriety. Envision a phishing email being sent from your mail since somebody had manufactured your data. Irate beneficiaries and spam dissensions coming about because of it turn into your chaos to tidy up, so as to repair your notoriety. trustee-based social verification frameworks request that clients select their own trustees with no requirement. In our examinations (i.e., Section VII), we demonstrate that the specialist organization can compel trustee choices through forcing that no clients are chosen as trustees by an excessive number of different clients, which can accomplish better security ensures.

3. Attribute-based encryption module.

Attribute-based encryption module is utilizing for every last hub encode information store. After scrambled information and again the re-encoded similar information is utilizing for fine-grain idea utilizing client information transferred. the characteristic based encryption have been proposed to secure the distributed storage. Quality Based Encryption (ABE). In such encryption plot, a personality is seen as an arrangement of unmistakable qualities, and decoding is conceivable if a decoder's character has a few covers with the one indicated in the cipher text.

4. Multi-authority module.

A multi-specialist framework is displayed in which every client has an id and they can cooperate with each key generator (expert) utilizing diverse nom de plumes. We will likely accomplish a multi-expert CP-ABE which accomplishes the security characterized above; ensures the classification of Data Consumers' personality data; and endures trade off assaults on the specialists or the intrigue assaults by the experts. This is the primary execution of a multi-specialist characteristic based encryption conspire.

7.2 System Model

1. Data owner

As the name describes, it is data owner module which carry outs the actions of owner. It allows the owner to register and keep the login details. It enables the owner to encrypt the record prior to the cloud outsourcing. Once the records are uploaded on cloud the need for the owner is to effectively search over them for file utilization. The owner is able to construct a tree like structure with prefix of index for the file collection, and then encrypt the entire collection for further security. The owner places the encrypted collection to cloud, not only this but also the index. The later procedure makes the proper distribution of key to authorized users. Owner is also provided with ease of runtime addition and removal of records from the server.

2. Data consumer

In this module, the consumer login and access the file that is in encoded form. File is decoded by giving the random encryption key. If the random key is valid then the file decrypt consumer able to access the file by downloading it and provides the response and ends the session by logging out. The consumer is able to download the file in the given particular time.

3. Cloud Service Provider (CSP)

A partial trustworthy unit of the system. It honestly performs the requested task and results in right outcomes. But sometimes it may few times become curious to get the details of the uploaded data. CSP is in charge of storing the cipher text and providing the services for data transfer.

7. CONCLUSIONS

Semi-anonymous attribute-based privilege control scheme AnonyControl and a fully-anonymous attribute-based privilege control scheme AnonyControl-F is proposed in this model to solve the problem of user identities in cloud storage server. By make use of multiple Authorities in the cloud computing system our model not just achieve fine-grained privilege control but also id anonymity. Most important is our model can resist up to N-2 authority compromise, which is highly preferable mostly for Internet-based cloud computing. Our precise analysis on security and performance analysis shows Anony-Control both secure and efficient for cloud storage system. Anonycontrol is directly inheriting the security of AnonyControl and hence it is secure, but the extra overhead of communication is incurred during the 1-out-of-n transfer.

ACKNOWLEDGMENT

We are indebted to the management of Guru Nanak Dev College, Bidar for excellent support in contemplating this work at the right time. A special thanks to the authors mentioned in reference

REFERENCES

[1] Taeho Jung1, Xiang-Yang Li12, Zhiguo Wan34, Meng Wan5, “Privacy preserving data aggregation without secure channel: Multivariate polynomial evaluation,” in Proc. IEEE INFOCOM, Apr. 2013, pp 2634-2768.

[2] Vladimir Boˇzovi´c1, Daniel Socek , Rainer Steinwandt, "Multi-authority attribute based encryption with honest but-curious central authority", *Int. J. Comput, Math.*, vol 89, No. 3, 2012, pp. 268-283.

[3] Allison Lewko, "Decentralizing attribute-based encryption", *in Advances in cryptology*. Berlin, Germany: Springer-Verlag 2011, pp 568-588.

[4] Jianting Ning1 , Xiaolei Dong2 , Zhenfu Cao2 and Lifei Wei3, "Accountable Authority Ciphertext-Policy Attribute-Based Encryption with White-Box Traceability and Public Auditing in the Cloud", Springer International Publishing Switzerland 2015, LNCS, volume 9327.