Journal of Advances in Science and Technology
Vol. 12, Issue No. 24, November-2016, ISSN 2230-9659

# An Analysis upon Various Security Methods for Identification of Data in Cloud Computing Environment: A Case Study of Predicate Based Encryption

**Anita Soni[1]* Dr. Kalpana[2]**

[1] Research Scholar, Pacific University, Udaipur, Rajasthan

[2] Assistant Professor, OPJS University, Churu, Rajasthan

***Abstract – Cloud computing has turned into a standout amongst the most critical data security issue lately. That is because of the breathtakingly developing applications and obliged services of cloud computing. Notwithstanding, with a specific end goal to securely use and revel in the profit of cloud computing through wired/wireless networking, sufficient confirmation of data security, for example, classified ness, verification, non repudiation, and respectability is the most basic component for reception. Data that was once housed under the security realm of the service client has now been put under the insurance of the service provider. Clients have lost control over the security of their data. Never again is our data held under our own particular watchful eyes.***

***This study demonstrates how Predicate Based Encryption (PBE) could be leveraged inside the Cloud to secure data. Five situations for utilizing Predicate Based Encryption inside the Cloud are introduced. These situations vary regarding mode of operation, predicate situation, and responsibility for Key Authority.***

***In a perfect world, a privacy-saving database-in-the-cloud environment might permit a database possessor to outsource its encrypted database to a cloud server. The possessor might hold control over what records might be questioned and by whom, by giving each one commissioned client a hunt token and a decryption key. A client might then present this token to cloud server who might utilize it to find encrypted matching records, while taking in nothing else. A client could then utilization its possessor issued decryption key to take in the actual matching records.***

---------------------------♦-----------------------------

Cloud computing is the conveyance of computing services over the Internet. Cloud services permit people and organizations to utilize software and hardware that are oversaw by unbiased gatherings at remote areas. Illustrations of cloud services incorporate online record storage, long range interpersonal communication locales, web mail, and online business applications. The cloud computing model permits access to information and computer resources from anyplace that a network connection is accessible. Cloud computing furnishes an imparted pool of resources, incorporating data storage space, networks, computer processing power, and particular corporate and client applications.

In its broadest utilization, the term cloud computing alludes to the conveyance of adaptable IT resources over the Internet, instead of facilitating and operating those resources by regional standards, for example, on a school or college network. Those resources can incorporate applications and services, and in addition the base on which they work. By sending IT framework and services over the network, an organization can buy these resources on an as-required groundwork and maintain a strategic distance from the capital expenses of software and hardware. With cloud computing, IT limit might be balanced rapidly and effectively to accommodate changes popular. While remotely hosted, oversaw services have long been a piece of the IT scene, an uplifted investment in cloud computing is constantly powered by pervasive networks, developing norms, the ascent of hardware and software virtualization, and the push to make IT expenses variable and transparent.

In accepted undertaking computing, IT sections estimate interest for applications and limit and contribute time and cash to improve those resources in-house or buy them from others and work them in-house. With cloud computing, organizations procure IT services from remote providers, and grounds constituents access these resources over the Internet. Message, for instance, since a long time ago recognized a staple of an organization's IT operations, might be obtained from a go of sources, and a developing number of grounds contract with outside suppliers for this capacity. Software is hosted by the provider and does not have to be introduced or supported on distinct computers around facilities. In a few cases, an expansive college or a consortium may turn into a provider of cloud services. Storage and processing needs can likewise be met by the cloud. Foundations pay just for the resources utilized, and clients can access the applications and documents they need from virtually any Internet- associated computer. In a develop cloud computing environment, establishments might have the capacity to include new IT services or react to changes in limit on the fly, sparing capital expenses that could be redirected to systems of vital esteem to the organization.

Cloud computing give IT organizations a fundamentally distinctive model of operation, one that exploits the development of web applications and networks and the climbing interoperability of computing systems to furnish IT services. Cloud providers spend significant time specifically applications and services, and this mastery permits them to effectively oversee redesigns and upkeep, reinforcements, fiasco recuperation, and failover functions. Accordingly, shoppers of cloud services may see expanded unwavering quality, even as expenses decrease because of economies of scale and other generation elements. With cloud computing, organizations can monitor present needs and make on-the-fly changes in accordance with expand or decline limit, pleasing spikes popular without paying for unused limit throughout slower times. Aside from the possibility to lower expenses, schools and colleges addition the flexibility of having the ability to react rapidly to demands for new services by acquiring them from the cloud. Cloud computing supports IT organizations and providers to build standardization of conventions and processes so the numerous bits of the cloud computing model can interoperate fittingly and effectively. Cloud computing's scalability is an alternate key profit to higher instruction, especially for research undertakings that oblige immeasurable measures of storage or processing limit for a constrained time. A few organizations have fabricated data focuses close wellsprings of renewable vigor, for example, wind ranches and hydroelectric offices, and cloud computing manages access to these providers of "green IT." Finally, cloud computing permits school and college IT providers to make IT expenses transparent and in this manner match utilization of IT services to the individuals who pay for such services.

In spite of the fact that the profits of cloud computing are getting to be more tangible, noteworthy policy and innovation issues must even now be dealt with for it to achieve its potential. Indeed as "public" clouds are constantly advanced, another class of "private" clouds is coming to fruition. Though public cloud providers offer moderately undifferentiated services, private clouds seek after comparative economies of scale however do so while protecting the capacity to tweak applications and services for buyers. Extensive organizations, for example, statewide business settings for higher instruction, for example, may put resources into cloud services for all the establishments in the system. As more amazing amounts of facilities consider cloud computing, services that have institutional identification or coordination needs are less inclined to be sourced from the cloud, and a heterogeneous blend of services some from the public cloud, others from private clouds, still others advanced in-house or acquired and modified is liable to describe most institutional IT portfolios.

Cloud computing construction modeling comprises of two parts "the front end" and "the back end". The front end of the cloud computing system involves the customer's unit (or it may be computer network) and a few applications are required for gaining entrance to the cloud computing system. Back end alludes to the cloud itself which may include different computer machines, data storage systems and servers. Gathering of these clouds make an entire cloud computing system. The entire system is controlled through a focal server that is likewise utilized for monitoring customer is request and traffic guaranteeing smooth working of the system. An exceptional sort of software called "Middleware" is utilized to permit computers that are associated on the network to correspond with one another. Cloud computing systems additionally must have a duplicate of all its customers! data to restore the service which may emerge because of an unit breakdown. Making duplicate of data is called excess and cloud computing service providers furnish data repetition.

Cloud Computing is the name given to a later pattern in computing service procurement. This pattern has seen the mechanical and social movement of computing service procurement from being given mainly to being given remotely and altogether, by alternate gathering service providers. These alternate gatherings offer purchasers a reasonable what's more adaptable computing service that purchasers might overall not have been receptive, left to figure things out without anyone else's input manage. This new method of service procurement has advanced from and is the finish of research stemming from (around others) conveyed and networked systems, utility computing, the web and software services research.

This ideal model transformation has accelerated computing being seen as an alternate family unit utility, otherwise known as "fifth utility", and has provoked numerous a business and individual to move parts of their IT foundation to the cloud and for this data to get oversaw and hosted by Cloud Service Providers (Csps). Be that as it may, Cloud Computing is the cause célèbre around tech intellectuals and has expedited the term `cloud Computing' as an umbrella term being connected to varying circumstances and their answers. In that capacity an expansive extend of definitions for Cloud Computing exists, each of which vary relying upon the starting creators' inclining.

Predicate Based Encryption (PBE), speaks to a group of awry encryption schemes that considers specific fine grained access control as a major aspect of the underlying cryptographic operation. The beginnings of PBE are in Identity Based Encryption (IBE). In IBE schemes a substance's encryption key is inferred from a basic string that speaks to the element's own particular public identity e.g. a message address. PBE schemes offer a wealthier plan in which an substance's `identity' might be built from a set of attributes and decryption is connected with access policies that offers a more expressive means with which to depict the connection between the attributes. Different developments of PBE schemes have been recommended that utilize general predicates (spoke to as Boolean recipe) or particular predicates, for example, equity, shrouded vector or inward item. The decision of predicate will have a regulate influence upon the plan, its qualities and the creation of the access policies. Also, the situation of the predicate (either with the figure content or the decryption key) has an incredible influence upon the workings of a PBE plan.

## SECURITY OF IDENTITY DATA IN CLOUD COMPUTING

The developing popularity, proceeding improvement and development of cloud computing services is an unquestionable actuality. Information saved generally on a computer might be saved in the cloud, incorporating word processing reports, spreadsheets, presentations, sound, photographs, movies, records, monetary information, errand schedules, and so on. A cloud service provider (SP) is an alternate gathering that keeps up information about, or for, an alternate element.

Believing an alternate gathering obliges taking the danger of expecting that the believed unbiased gathering will go about as it is normal (which may not be correct constantly). At whatever point some element stores or processes information in the cloud, privacy or privacy inquiries may emerge.

Privacy in cloud computing could be characterized as ."the capacity of a substance to control what information it uncovers about itself to the cloud (or to the cloud SP), and the capability to control who can access that information.".

Various existing privacy laws force the models for the accumulation, upkeep, utilize, and revelation of directly identifiable information (PII) that must be fulfilled even by cloud Sps. (PII is usually reputed to be identity information.) Due to the way of cloud computing, there is next to zero information accessible in a cloud to bring up where data are archived, how secure they are, who has admittance to them, or in the event that they are exchanged to an alternate have (if that have might be trusted).

A cloud can't be utilized for saving and processing data also applications provided that it is unsecure. The real issue as to in cloud is the manner by which to secure PII from being utilized by unapproved clients, how to anticipate assaults against privacy, (for example, identity burglary) actually when a cloud SP can't be trusted, and how to administer control over the divulgence of private information.

Giving touchy data to an alternate organization is a genuine concern. Are data held some place in the cloud as secure as data secured in client regulated computers and networks? Cloud computing can expand the dangers of security breaks. Knowing who has client's. close to home data, how they are, no doubt entered, and the capability to keep up control over them averts privacy ruptures of PII, and can minimize the hazard of identity robbery and duplicity.

We furnish more insights about privacy in cloud computing in. We accomplish an answer for the privacy issue that we explore in this study in through the utilization of a substance driven approach. The approach that we propose in is based on unknown recognizable proof, which is utilized to intercede cooperations between the client and cloud services. The approach uses dynamic bunch, which upholds the policies and uses a set of security instruments to ensure the delicate data.

## PREDICATE BASED ENCRYPTION

Predicate Based Encryption (PBE), speaks to a group of lopsided encryption schemes that considers specific fine-grained access control as a major aspect of the underlying cryptographic operation [ksw08]. The roots of PBE are in Identity Based Encryption (IBE). In IBE schemes an element's encryption key is inferred from a straightforward string that speaks to the substance's public identity e.g. a message address. Case in point, given an element Albert his comparing encryption key will be Enc(albert) == albert@foobar.com. Throughout encryption, the ensuing figure content will adequately be labelled with the string speaking to the encryption key, the element's public identity. An element's decryption key will be inferred from the same string utilized for the encryption key e.g. Albert's decryption key will be inferred from his message address. On recipt of a ciphertext message the beneficiary can decrypt the figure content if and just if the two personalities, held inside the decryption key and figure content, are `equal'. PBE schemes offer a wealthier plan in which an element's `identity' could be developed from a set of attributes and decryption is connected with access policies that offers a more expressive means with which to portray the connection between the attributes.

For the most part talking, inside PBE schemes elements and figure messages are each one connected with a set of attributes. These attributes are utilized to portray some part of the element, the data that is continuously encrypted, and the environment. An element can decrypt a figure content just if there is a match between the attributes of the figure content and the decrypting element. Matching is accomplished through predicates (access policies) that indicate: a) the set(s) of authorised attributes that a substance must have to decrypt and access the plain-content; and b) the relationship between the attributes.

Different developments of PBE schemes have been recommended that utilize general predicates (spoke to as boolean equation) or particular predicates, for example, balance, shrouded vector or internal item. The decision of predicate will have an administer influence upon the plan, its attributes and the sythesis of the right to gain entrance policies. Additionally, the situation of the predicate (either with the figure content or the decryption key) has an extraordinary influence upon the workings of a PBE plan. Regular to all PBE schemes are four operations taking into account encryption, decryption and key era. The exact esteem for encryption and decryption keys is needy upon both the development of the plan and arrangement of predicates.

The point when taking a gander at the diverse PBE schemes, three groupings (or family) of schemes develop based upon the predicates being utilized, the plan's point and the schemes development.

1. Identity Based -Identity Based Encryption (IBE) schemes are utilized to encrypt messages utilizing a solitary ascribe that alludes to the clients identity i.e. message address or travel permit number Shamir; Boneh and Franklin. In these schemes the right to gain entrance policy is likewise included a solitary characteristic. To add extensibility to IBE schemes these `single' attributes were stretched out utilizing string linking to encode more information.

2. Quality Based - Attribute Based Encryption (ABE) schemes [gs+06] further generalises upon IBE schemes and uses general predicates styled as boolean equation blanket operations for example, conjunction, disjunction and limits. The attributes themselves need not essentially allude to an element's identity, or even to a substance, and can allude to non-identity identified viewpoints, for example, Tcp/ip port numbers and addresses.

3. Particular Predicate Based - The last group of schemes are those that utilize particular predicates throughout their development. Despite the fact that these schemes might be alluded to by the predicate being utilized, the general term Predicate Based Encryption can likewise be utilized. Particular predicates that have been utilized incorporate that of inward item [ksw08] and shrouded vector predicates.

The perceivability of the right to gain entrance policies and attributes will contrast between schemes. By plan all PBE schemes are Payload Hiding (PH). This guarantees that the payload can't be gained entrance to by a vindictive element. A PBE plan is Attribute Hiding (AH) if the plan likewise shrouds information of the encryption key i.e. attributes/access policies, used to encrypt the figure content. Throughout decryption the point when an element endeavors to gain entrance to the plain-content they will just take in if the decryption method is great or not and won't take in all else concerning the figure content and its attributes/access policy. While all schemes as a matter of course are payload concealing, property concealing schemes are indigent upon the underlying predicates used to understand the plan. Such usefulness is accomplished when utilizing inward item and shrouded vector predicates.

Predicates are utilized to characterize the obliged sets of attributes required, regularly as far as boolean recipe, by the decrypting substance for decryption to happen. Inside PBE the term Access Policy can be utilized reciprocally with the term predicate, and inside Key-Policy schemes with decryption key. This area displays a review of access policies, their definition and restrictions. The expressiveness of a right to gain entrance policy is indigent upon both: a) the predicates utilized by the plan; and b) other scientific develops utilized inside the plan's development. That is, the admissible operations accessible when developing a right to gain entrance policy are not general and will differ.

## PBE SCHEMES

Similarly as with numerous an encryption plan, PBE schemes encrypt messages utilizing some mystery esteem. PBE schemes vary in their operation by utilizing Linear Secret Sharing Scheme (LSSS) to disperse this mystery esteem around a set of attributes as per a few right to gain entrance policy. Just those authorised to decrypt the figure content can remake the mystery esteem. While it is normal to see PBE schemes being executed utilizing blending based cryptography, the strategies used to convert the predicate/access policy into a LSSS will fluctuate. Also where this policy conversion happens is needy upon if the plan is a Key-Policy or Ciphertext- Policy plan. To outline and talk over all the contrasts between the different techniques for development for distinctive predicates just builds the extension and multifaceted nature of this examination. As being what is indicated the examination inside this section will just keep tabs on general predicate PBE schemes. It is trusted by keeping tabs on these schemes that the onlooker can increase a "feel" for how other PBE schemes work.

Developments of PBE schemes might be characterised as far as: a) how predicates are transformed into Lssss; b) how the ensuing LSSS combines with the matching based cryptography, c) the underlying blending based cryptography. Segment 8.2 offers a short prologue to pairing based cryptography and how the encryption and decryption operations could be figured it out. Area 8.3 gives a substitute and more formal definition for access policies, and how they identify with LSSS and cryptographic operations of PBE schemes. For numerous general predicate PBE schemes the means by which the LSSS and blending based cryptography are combined will contrast generously. Segment 8.5 portions how this might be attained utilizing the vast universe CP-ABE plan from Waters.

As the relationship between figure messages and substances, when decrypting, is one-to-a lot of people, one of the issues experienced when planning a PBE plan is that of element arrangement. Substance plot is a strike performed by two or more substances who separately don't have enough attributes to fulfill a right to gain entrance policy. The substances will then consolidate their attributes in an endeavor to fulfill the policy. This is a vital assault that developments of PBE must be impervious to and numerous schemes have been intended to counter such a strike.

The computational multifaceted nature of PBE schemes is indigent upon the correct development of the plan. Notwithstanding, of correct development some general perceptions over the unpredictability might be perceived. Underneath the unpredictability regarding decryption key and figure content, and encryption and decryption times are examined.

## ENCRYPTED INFORMATION IN CLOUD COMPUTING

In recent years, cloud computing is gaining much momentum in the IT industry. Especially, we have seen the dramatic growth of public clouds, in which the computing resources can be accessed by the general public. One of the biggest advantages of a public cloud is its virtually unlimited data storage capabilities and elastic resource provisioning.

Many IT enterprizes and individuals are outsourcing their databases to the cloud servers, in order to enjoy the much lower data management cost than maintaining their own data centers. It has never been easier than now that a variety of users/clients could access or share information stored in the cloud, independent of their locations. Despite enthusiasm around the cloud data service outsourcing model, its promises cannot be fulfilled until we address the serious security and privacy concerns that data owners have. The outsourced data may contain very sensitive information, such as Personal Health Records (PHRs), facebook photos, and business documents. Many people remain dubious about the levels of privacy protection of their data when stored in a server owned by a third-party cloud service provider.

Given that there have been numerous reported data breaches related to cloud servers, which could be due to malicious attacks, theft or internal software bugs and errors, it can be claimed that the servers are not fully trustworthy. This implies that there is no absolute governance about how the owners' information will be used and whether the owners actually control access to their data. To cope with the tough trust issues and to ensure owners' control over their own privacy, applying data encryption on the documents before outsourcing has been proposed as a promising solution, which is already adopted by many recent works. In this study, we focus on the "multi-owner" setting, where the encrypted data are contributed by multiple owners and can be searched by multiple users.

With encrypted data, one of the key functionalities of a database system - keyword search becomes an especially challenging issue. We will take PHR as the main motivating example. First we need to support frequently used complex query conditions efficiently. For example, a user may want to find out other patients with the same disease and symptoms from an encrypted PHR database, by submitting a query like "(20<age<30) AND (sex="female") AND (illness="diabetes")". Also, a medical researcher may query the database using the following: (age>50) AND (region=" Massachusetts") AND (illness="cancer"). This class of boolean formulas feature conjunctions among different keyword fields and we will refer to them as multi-dimensional keyword search in this study. To hide the query keywords from the server, it is apparently inefficient for a user to download the whole database and try to decrypt the records one by one. Searchable encryption (SE) has been proposed as a better solution; informally speaking, a user submits a “capability” encoding her query to the server, who searches through the encrypted keyword indexes created by the owners, and returns a subset of encrypted documents that satisfy the underlying query without ever knowing the keywords in the query and the index.

On the other hand, in many existing SE schemes, the legitimate users are often given a secret/private key that endows her unlimited capability to generate any query of her choice, which is essentially a “0” or “1” authorization. However, we note that “fine-grained search authorization” is an indispensable component for a secure data outsourcing system. Although the accesses to actual documents can be controlled by separate cryptographic enforced access control techniques such as attribute-based encryption “0-1” search authorization may still lead to leakage of data owners’ sensitive information. For example, if Alice is the only patient with a rare disease in a PHR database, by designing the query in a clever way (e.g., submitting two queries with/without the name of that disease and with Alice’s demographic info), from the results a user Bob will be certain that Alice has that disease. Thus, we argue that a user should only be allowed to search for some specific sets of keywords; in particular, the authorization shall be based on a user’s attributes. For instance, in a patient matching application in health social networks, a patient should only be matched to patients having similar symptoms as her, while shall not learn any information about those who do not.

## INFORMATION PRIVACY IN THE CLOUD

Cloud computing includes greatly accessible enormous figure and storage stages offering a wide go of services. A standout amongst the most famous and fundamental cloud computing services is storage-as-a-service (SAAS). It gives organizations reasonable storage, expert upkeep and movable space.

On one hand, because of aforementioned profits, organizations are energized by the public introduction of SAAS. On the other hand, organizations are hesitant about embracing SAAS. One of the real concerns is the privacy as cloud service is for the most part furnished by the alternate gathering. In the accompanying, we call the organization, who uses SAAS, the database holder. We call any individual who questions the organization's database, the database client. Also we call the cloud servers, which store the database, the cloud server. Right away we begin to illuminate distinctive sorts of privacy challenges throughout the sending of cloud service. From the view of the database manager, three challenges emerge.

- Challenge 1: how to secure outsourced data from robbery by programmers or malware penetrating the cloud server? Encryption by the cloud server and confirmed access by clients appears to be a clear result. In any case, cautious thought ought to be given to both encryption system and its granularity.
- Challenge 2: how to secure outsourced data from ill-use by the cloud server? An inconsequential result is for the holder to encrypt the database preceding outsourcing. Accordingly, clients (furnished with the decryption key(s)) can download the whole encrypted database, decrypt it and perform questioning in situ. Obviously, this nullifies most profits of utilizing the cloud. A more sumptuous approach is to utilize searchable encryption. Lamentably, ebb and flow searchable encryption strategies just help basic hunt (attribute=value), instead of convoluted SQL, inquiries.
- Challenge 3: how to acknowledge substance level fine-grained access control for clients? This challenge is even harder to settle as it obliges variable decryption proficiencies for distinctive clients. Indeed trifling answer for the second challenge does not settle this challenge as it gives every client equivalent decryption proficience (same decryption key). A perfect result might involve the database possessor issuing a given client a key that just permits the client to inquiry and decrypt certain records. From client's point of view, three more challenges emerge.
- Challenge 4: how to inquiry the cloud server without uncovering question parts? Taking in client's inquiry items means taking in client's conceivably touchy hunt investment. Also, by taking in client inquiries, the cloud server continuously takes in the information in the encrypted database.
- Challenge 5: how to shroud inquiry substance (e.g., values utilized as a part of "attribute=value" inquiries) from the database possessor. For the database possessor to practice access control over its outsourced data, a client might as well first acquire a support from the database possessor over its inquiry substance. On the other hand, in a few cases, the client may need to get the approbation without uncovering its question substance even to the database possessor. This is the situation when the client happens to be an abnormal amount official who is immediately qualified to pursuit any esteem and is not eager to uncover question to anybody.

- Challenge 6: how to conceal question substance while guaranteeing database possessor the hiden substance are commissioned by some authentication power (CA). Such challenge surfaces, for instance, when the client is FBI who does not have any desire to uncover the individual it is researching while database holder needs to get some certainty by verifying FBI is commissioned by the court to do this examination.

In this study, we present another plan that addresses previously stated prerequisites. It depends on characteristic based encryption and unseeing Boneh-Boyen feeble mark plan. Indeed, we change the standard trait based encryption to make it privately searchable in the cloud computing situation. Moreover, we utilize the unseeing Boneh-Boyen mark plan to let client absently recover a pursuit token and decryption key. Also, visually impaired pursuit token and decryption key extraction technique might be coupled with CA approval on client's include.

## PROTECTION TECHNIQUE FOR DATA MIGRATION IN CLOUD COMPUTING

An observation on the Data Migration : Data migration to a cloud computing environment is from numerous points of view a practice in hazard administration. Both qualitative and quantitative elements apply in a dissection. The dangers must be painstakingly adjusted against the accessible protects and wanted profits, with the comprehension that responsibility for security stays with the organization. An excess of controls might be wasteful and ineffectual, if the profits exceed the expenses and partnered dangers. A suitable equalize between the quality of controls and the relative hazard connected with specific systems and operations must be guaranteed.

Data security is an alternate vital research theme in cloud computing. Since service providers regularly don't have entry to the physical security system of data focuses, they must depend on the foundation provider to attain full data security. Actually for a virtual private cloud, the service provider can just define the security setting remotely, without knowing if it is completely executed.

The framework provider, in this connection, must attain the accompanying targets: (1) classifiedness, for secure data access and exchange, and (2) auditability, for bearing witness to if security setting of applications has been altered or not. Classifiedness is normally accomplished utilizing cryptographic conventions, inasmuch as auditability might be attained utilizing remote verification methods. Remote authentication regularly obliges a trusted stage module (TPM) to create non-forgeable system outline (i.e. system state encrypted utilizing TPM's private key) as the verification of system security. In any case, in a virtualized environment like the clouds, Vms can alertly relocate starting with one area then onto the next; thus straightforwardly utilizing remote confirmation is not sufficient.

Hence, it is discriminating to fabricate trust components at each building layer of the cloud. Firstly, the hardware layer must be trusted utilizing hardware TPM. Besides, the virtualization stage must be trusted utilizing secure virtual machine monitors. VM migration might as well just be permitted if both source and objective servers are trusted. Later work has been committed to planning proficient conventions for trust stronghold and administration.

Need for securing data migration process : Cloud Migration is one of greatly talked focus where cloud directors face great issues around then of data migration from an organization's server to a server that structures cloud somewhere else. Why they face inconveniences how about we discover. As I know, cloud carries on as an interface through which organizations can access data in a virtual environment. Accordingly, smooth working of it depends essential on how decently tidied and learned cloud providers are around there.

Also, if data migration is not completed systematically and legitimately, it can offer ascent to issues concerning data and cloud security of organization's possessions that principally contain data. Accordingly, enlisting cloud providers having sound encounter about the field with plentiful learning and aptitude sets gets fundamental for overseeing cloud all the more viably and proficiently.

## CONCLUSION

Cloud Computing embodies the as-a-Service paradigm and allows for services to be provided en masse to consumers. When combined with the cloud setting, two different sets of scenarios emerged based upon whether the service user’s or CSP’s data was to be protected. PBE schemes can be used to protect service user’s data in three different scenarios: Scenario I saw the inclusion of PBE within a service; Scenario II saw the provision of PBE asa-Service; and Scenario V saw PBE being deployed by the user themselves. In each of these three scenarios PBE can be used by service users to specify precisely with whom they wish to share their data, for what purpose, and for how long. Although Scenario V may be a privacy zealot’s ideal choice , they are in full control its practical feasibility has yet to be determined.

PBE schemes can be used to protect service user's data in three deferent scenarios: Scenario I saw the inclusion of PBE within a service; Scenario II saw the provision of PBE as-a-Service; and Scenario V saw PBE being deployed by the user themselves. In each of these three scenarios PBE can be used by service users to specify precisely with whom they wish to share their data, for what purpose, and for how long. Although Scenario V may be a privacy zealot's ideal choice| they are in full control its practical feasibility has yet to be determined; the ability for service users' to act competently as a Key Authority is still unclear. The remaining two scenarios, on the other hand, do appear to be more promising. However, these scenarios in themselves do present a dilemma between usability and the guarantees made over end-to-end security.

## REFERENCES

Gopalakrishnan (2009). .“Cloud Computing Identity Management,.” SETLabs Briefings, vol. 7.

E. Shi and B. Waters (2008). “Delegating capabilities in predicate encryption systems,” in ICALP’08.

E. Shi and B. Waters (2008). Delegating capabilities in predicate encryption systems. In ICALP ’08, pages 560–578.

Foster I, Zhao Y, Raicu I, Lu S (2008). Cloud Computing and Grid Computing 360-Degree Compared. In: Grid Computing Environments Workshop (GCE’08). oi:10.1109/GCE.2008.4738445

J. Baek, R. Safavi-Naini, and W. Susilo (2008). Public key encryption with keyword search revisited. In Proceedings of ICCSA, Part I, ICCSA ’08, pages 1249–1259.

J. Benaloh, M. Chase, E. Horvitz, and K. Lauter (2009). Patient controlled encryption: ensuring privacy of electronic medical records. In CCSW’09, pages 103–114.

J. de Muijnck-Hughes (2011). “Data protection in the cloud,” Master’s thesis, Radboud Universiteit Nijmegen, March 2011

M. Li, S. Yu, N. Cao, and W. Lou. (2011). Authorized private keyword search over encrypted data in cloud computing. Technical report, http://ece.wpi.edu/ mingli/, Mar. 2011.

S. Overby (2010). How to Negotiate a Better Cloud Computing Contract, CIO, April 21, 2010,

S. Yu, C. Wang, K. Ren, and W. Lou (2010). Achieving secure, scalable, and fine-grained data access control in cloud computing. In IEEE INFOCOM’10, 2010.

Tim Mather, Subra Kumaraswamy, Shahed Latif (2009). "Cloud Security and Privacy: An Enterprise Perspective on Risk and Compliance", Editor Mike Loukides. O’Reilly.

Y. C. Chang and M. Mitzenmacher (2005). “Privacy preserving keyword searches on remote encrypted data,” in ACNS’05, 2005.

Brian Hayes (2008). "Cloud Computing", Commun. ACM 51.7, pp. 9-11.

**Corresponding Author**

**Candidate Name***

Research Scholar, Pacific University, Udaipur, Rajasthan

**E-Mail –**