Review Paper of Various Access Control Policy

Taniya Jain (M.Tech Scholar)
Asst. Prof. Javed Akhtar Khan
Department of Computer Science & Engineering
Takshshila Group of Institute INDIA

ABSTRACT
This review paper include the introduction part of Big data environment with its various access control policy . The main aim of this paper is to make a survey of some existing control policy and introduce the security issue in the Cloud environment for the big data.

Keywords
Cloud Computing, Big Data, control policy , security .

1. INTRODUCTION
Cloud Computing refers to manipulating, accessing and configuring the applications online. It offers online data storage, infrastructure and application. Cloud computing is an IT operation form, based on virtualization, where resources, in terms of infrastructure, appliance and data are deployed via the internet as a distributed service by one or some service providers[1]. These services are scalable on require and can be valued on a pay per use basis. Cloud infrastructure provides extensive facilities for the client such as process, storage, power, networks, space and other computational possessions, so that the customer can set and perform their convention software as well as applications and operating system. Client does not supervise or organize the cloud infrastructure yet they have been in charge of on operating systems, applications, storage space and probably their collection and components [2]. One of the main apprehension in cloud computing is the possibility of incursion of privacy. As cloud computing is achieving augmented popularity, apprehension are being voiced about the safety issues bring in through the acceptance of this new model. -description of this inventive deployment model, be different broadly from them of conventional architectures.

2.CLOUD COMPUTING IMPORTANCE
Cloud Computing has several recompense. Some of them are listed below: One can right of entry applications as utilities, over the Internet. Stage-manage and configure the relevance online at any time. It does not necessitate installing a explicit piece of software to right to use or manipulating cloud application. Cloud computing propose online progress and deployment tools, programming runtime surroundings through Platform as a Service model. Cloud resources are accessible over the network in a method that provides platform independent right of entry to any type of clients. Cloud computing forward on-demand self-service. The resources can be used lacking interaction with cloud service contributor. Cloud Computing is extremely cost effective since it operates at higher efficiencies with larger utilization. It just has need of an Internet connection. Cloud Computing offers load comparison that makes it more reliable.

3. CLOUD COMPUTING ARCHITECTURE
Cloud service models basically imply what type of services can be offered to customers. Cloud as a Service, where can be changed by any one of the following: Security, Infrastructure, Data, Software, Desktop, Platform, IT, Database, Hardware, Computing, Testing, Storage etc.

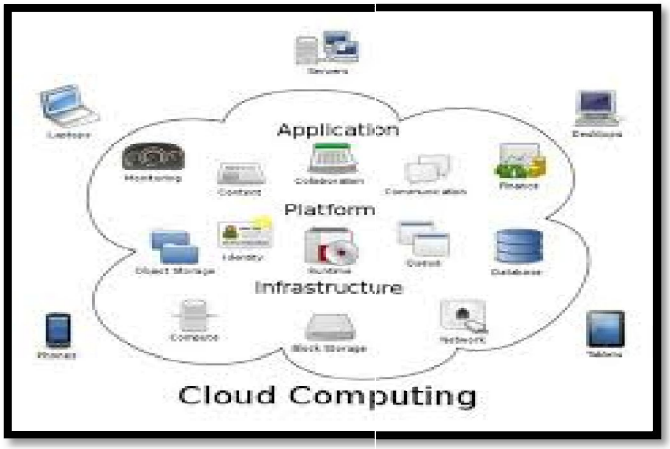

Figure 1: Cloud Computing Architecture

3.1 SAAS(Software as a Service)
SAAS is a software form provided by the merchant through an online facility. It provides network-based right of entry to commercially accessible software. User interface powered by "thin client" relevance cloud mechanism; statement via (Application Program Interfaces (APIs), loosely coupled, stateless, semantic, interoperability modular [15]. This will stay away from capital overheads on software and expansion resources; reduced Return on Investment (ROI) risk, modernized and iterative updates. On the different, Centralization of data involves new/different sanctuary measures. Examples of SaaS consist of Netflix, Intuit
Quick Books Online, Gmail, and Google Docs[16]. The four most important advantages of Saas are:-

- Lowered cost of implementation and upgrades
- Reduced support requirements
- Increased user adoption
- Increased speed of deployment

3.2 PAAS (Platform as a Service)

PaaS enables companies to develop submission more swiftly and efficiently in a cloud background using programming languages and tools supported by the contributor. The significant factor that makes PaaS unique is that it lets developers assemble and deploy web applications on a hosted communications

3.3 IAAS(Infrastructure as a Service)

This is the bottom layer of the cloud stack. It serves as a foundation for the other two layers, for their implementation. The keyword at the back this stack is virtualization. Usually platform-independent, infrastructure expenses are shared and thus abridged, service level agreements (SLAs), self-scaling, pay by usage. Keep away from capital expenditure on hardware and human resources, reduced ROI risk; low barricade to entry, streamlined and automated scaling but shortcoming are business competence and productivity mainly depends on the merchant capabilities, potentially larger long-term cost, centralization have need of new/different defense measures. With, a corporation can rent essential computing resources for deploying and storing data or running applications. IaaS enables express deployment of applications and get better the quickness of IT services by instantly adding computing processing command and storage capacity when necessary.

4. CLOUD DEPLOYMENT MODELS

In spite of the facility model utilized (SaaS, PaaS, or IaaS) there are four deployment models for cloud Server

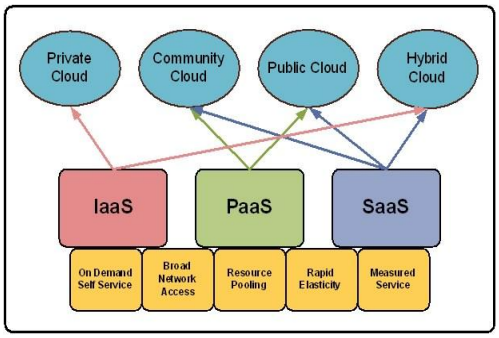

Figure 2: Cloud Computing Architecture

- Public Cloud: The cloud infrastructure is made accessible to the general community or a large business group and is owned by associations selling cloud services. Means where the infrastructure exist in totally external of the tenant enterprises.
- Private Cloud : The cloud infrastructure is operated exclusively for a single association. It may be managed by the association or a third party and could exist on premises or off location. IT services are mounted on top of large-scale build up and virtualized infrastructure within project firewall and consumed in "per transaction" basis.
- Community Cloud: The cloud infrastructure is collective by quite a few organizations and supports a precise community that has shared apprehension (e.g. security, mission, requirements, considerations, or compliance policy). It possibly will be managed by the organizations or a third party and may exist on-premises or off-premises.
- Hybrid Cloud: The cloud infrastructure is a composition of two or further clouds (private, community, or public) that stay behind unique entities but are bound together by standardized or proprietary technology that make possible data and application portability (e.g., cloud bursting for load balancing among clouds). Here, the infrastructure and business progressions reside partly surrounded by the enterprise and partly consumed from third party.

5. INTRODUCTION BIG DATA ENVIRONMENT

Big data is a broad term for data sets so large or complex that traditional data processing applications are inadequate. Challenges include analysis, capture, data curtain, search, sharing, storage, transfer, visualization, and information privacy. The term often refers simply to the use of predictive analytics or other certain advanced methods to extract value from data, and seldom to a particular size of data set. Accuracy in big data may lead to more confident decision making. And better decisions can mean greater operational efficiency, cost reduction and reduced risk.Big data refers to high volume, high velocity, and/or high variety information assets that require new forms of processing to enable enhanced decision making, insight discovery and process optimization. Due to its high volume and complexity, it becomes difficult to process big data using on-hand database management tools. An effective option is to store big data in the cloud, as the cloud has capabilities of storing big data and processing high volume of user access requests in an efficient way. When hosting big data into the cloud, the data security becomes a major concern as cloud servers cannot be fully trusted by data owners.

6. SECURITY ISSUES IN BIG DATA

The biggest challenge for big data from a security point of view is the protection of user's privacy. Big data frequently contains huge amounts of personal identifiable information and therefore privacy of users is a huge concern. When producing information for big data, organizations have to ensure that they have the right balance between utility of the data and privacy. Before the data is stored it should be adequately anonym zed, removing any unique identifier for a user. This in itself can be a security challenge as removing unique identifiers might not be enough to guarantee that the data will remain anonymous. The anonym zed data could be could be cross-referenced with other available data following de-anonymization techniques. When storing the data organizations will face the problem of encryption. Data cannot be sent encrypted by the users if the cloud needs to perform operations over the data. A solution for this is to use "Fully Homomorphism Encryption" (FHE), which allows data stored in the cloud to perform operations over the encrypted data so that new encrypted data will be created. When the data is decrypted the results will be the same as if the operations were carried out over plain text data. Therefore, the cloud will be able to perform operations over encrypted data without knowledge of the underlying plain text data. An additional problem is that software commonly used to store big data, such as Hadoop, doesn't always come with user authentication by default. This makes the problem of access control worse, as a default installation would leave the information open to unauthenticated users. Big data solutions

often rely on traditional firewalls or implementations at the application layer to restrict access to the information.

7. CONTRO ACCESS POLICY LITERATURE SUMMARY –

7.1 ATTRIBUTE-BASED ENCRYPTION (ABE) [4]

In This paper , the authors proposed a Key-Policy Attribute-Based Encryption method and discussed on how to change the policies on keys. Our access control scheme is constructed based on the **CP-ABE** method with primer group order **(CP-ABEPrimer)** in [8], which is proved to be secure under **generic bilinear group model** and **random oracle model**. At an intuitive level, this means that if there are any vulnerabilities in the scheme, then these vulnerabilities must exploit specific mathematical properties of **elliptic curve groups** or **cryptographic hash functions used when instantiating the scheme** .[8] has emerged as a promising technique to ensure the **end-to-end data security in cloud storage system**. It allows data owners to define access policies and encrypt the data under the policies, such that only users whose attributes satisfying these access policies can decrypt the data. When more and more organizations and enterprises outsource data into the cloud, the policy updating becomes a significant issue as data access policies may be changed dynamically and frequently by data owners. However, this policy updating issue has not been considered in existing attribute-based access control schemes [9]–[12]. In [10], the authors also proposed a cipher text delegation method to update the policy of cipher text. However, these methods cannot satisfy the completeness requirement, because they can only delegate key/cipher text with a new access policy which is more restrictive than the previous policy. A Author **[17] Liang –Ao Zhang et.al** are proposed the ABE based Access control with the Authentication and proposed the policy for the Cloud . In this paper Researcher are introduce the ABE that is attribute based Encryption technique and used this technique for the providing the securizaion data cloud , In this paper author are focus on the data owner's authentication in the ABE system and proposed a new scheme for the data access . In this paper author are do the work for Zero Knowledge Proof of Knowledge (ZKPK) to realize the anonymous authentication of the owner's policy updating key without increasing any secret information to the owner side. So author are propose an access control system with authenticated dynamic policy updating for the cloud storage and our ideas could also be applied to other ABE systems. Goyal et al. [18] further clarified the concept of **ABE** and proposed two complimentary forms of ABE: key-policy ABE (KP-ABE) and cipher text-policy ABE (CP-ABE) .In CP-ABE scheme, the cipher text is associated with an access policy on attributes, and the user's private key is associated with a set of attributes. A user is able to decrypt a ciphertext only if the set of attributes associated with the user's private key satisfies the access policy associated with the ciphertext. The KP-ABE scheme has the opposite situation where the access policy is correlated to the user's private key and describes the encrypted data with the user's attribute.The Attribute-Based Signature(ABS) [19] is adapted to ABE based access scheme to realize the anonymous authentication in [20, 21], but they can't directly enable the cloud to authenticate the owner's policy updating key. Furthermore, in the ABE based access control system that uses the ABS scheme to realize the authentication, the authorities have to maintain double attributes. This significantly increases the burden of authorities and the size of the user's key .a new method for the cloud to authenticate the owner's policy updating key the cloud server. We emphasize that the data owners are hypothesized to be fully trusted in Yang et al. scheme [22].

8.CONCLUSION

In this paper we are work for the Big data environment with its security issue .in this review paper we are include the introduction part of BIG Data and its Environment , we are contract the Control policy that used in the Big Data Environment for the data access we are also discus the various control policy and some security issue related to Big data and cloud domain .

REFERENCES

[1]Puya Ghazizadeh, Ravi Mukkamala & Stephan Olariu, 2013, "Data Integrity Evaluation in Cloud Database-as-a-Service", IEEE Ninth World Congress on Services, 978-0-7695-5024-4/13, DOI 10.1109/SERVICES.2013.40, pp.280-285.

[2] Ling Lang & Lin wang, 2012, "Research on cloud computing and key technologies", IEEE International Conference on Computer Science and Information Processing (CSIP), 978-1-4673-1411-4/12, pp.863-866

[3] Mohammed A. AlZain & Ben Soh and Eric Pardede, 2013, "A New Approach Using Redundancy Technique to Improve Security in Cloud Computing", pp. 230-235.

[4] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in CCS'06. ACM, 2006, pp. 89–98.

[5] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attributebased encryption," in S&P'07. IEEE, 2007, pp. 321–334.

[6] B. Waters, "Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization," in KC'11. Springer, 2011, pp. 53–70.

[7] A. B. Lewko, T. Okamoto, A. Sahai, K. Takashima, and B. Waters,"Fully secure functional encryption: Attribute-based cryption and (hierarchical) inner product encryption," in EUROCRYPT'10. Springer, 2010, pp. 62–91.

[8] A. B. Lewko and B. Waters, "Decentralizing attribute-based encryption,"in EUROCRYPT'11. Springer, 2011, pp. 568–588.

[9] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable, andvfine-grained data access control in cloud computing," in INFOCOM'10.IEEE, 2010, pp. 534–542.

[10] K. Yang, X. Jia, and K. Ren, "Attribute-based fine-grained access control with efficient revocation in cloud storage systems," in AsiaCCS'13. ACM, 2013, pp. 523–528.

[11] K. Yang, X. Jia, K. Ren, B. Zhang, and R. Xie, "DAC-MACS: Effective Data Access Control for Multiauthority Cloud Storage Systems," IEEE Trans. Info. Forensics Security, vol. 8, no. 11, pp. 1790–1801, 2013.

[12] K. Yang and X. Jia, "Expressive, efficient, and revocable data access control for multi-authority cloud storage," IEEE

Trans. Parallel Distrib. Syst., vol. 25, no. 7, pp. 1735–1744, July 2014.

[13] A. Sahai, H. Seyalioglu, and B. Waters, "Dynamic credentials and ciphertext delegation for attribute-based encryption," in CRYPTO'12. Springer, 2012, pp. 199–217.

[14]Amir Mohamed Talib, Rodziah Atan, Rusli Abdullah & Masrah Azrifah, 2011, "CloudZone: Towards an Integrity Layer of Cloud Data Storage Based on Multi Agent System Architecture", IEEE Conference on 14

[15] Basant Narayan Singh," Cloud Service Models – SaaS PaaS IaaS - Which One is for You?", posted Tuesday, June 28, 2011

