International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2017 IJSRCSEIT | Volume 2 | Issue 4 | ISSN : 2456-3307

Security and Privacy Issues in Cloud Computing

Bade Ankammarao[*1], Ravu Venkata Koteswarlu[2]

[*1]Assistant Professor, Department of MCA, St. Mary's Group of Institutions, Guntur, Andhra Pradesh, India
[2]PG Student, Department of MCA, St. Mary's Group of Institutions, Guntur, Andhra Pradesh, India

ABSTRACT

Most present security arrangements depend on border security. In any case, Cloud figuring breaks the association borders. At the point when information lives in the Cloud, they dwell outside the hierarchical limits. This leads clients to loos of control over their information and raises sensible security worries that back off the reception of Cloud processing. Is the Cloud specialist co-op getting to the information? Is it honest to goodness applying the get to control strategy characterized by the client? This paper displays an information driven get to control arrangement with enhanced part based expressiveness in which security is centered around ensuring client information in any case the Cloud specialist co-op that holds it. Novel personality based and intermediary re-encryption systems are utilized to ensure the approval display. Information is scrambled and approval standards are cryptographically secured to save client information against the specialist co-op get to or bad conduct. The approval display furnishes high expressiveness with part chain of importance and asset progressive system bolster. The arrangement exploits the rationale formalism gave by Semantic Web advances, which empowers propelled govern administration like semantic clash identification. A proof of idea usage has been produced and a working prototypical organization of the proposition has been coordinated inside Google administrations.

Keywords : Authorization, Cloud computing, Encryption, Data models Authorization, Data-centric security, Cloud computing, Role-based access control.

I. INTRODUCTION

Security is one of the main user concerns for the adoption of Cloud computing. Moving data to the Cloud usually implies relying on the Cloud Service Provider (CSP) for data protection. Although this is usually managed based on legal or Service Level Agreements (SLA), the CSP could potentially access the data or even provide it to third parties. Moreover, one should trust the CSP to legitimately apply the access control rules defined by the data owner for other users.. Users may loss control on their data. This situation leads to rethink about data security. Approaches and to move to a data-centric approach where data are self-protected whenever they reside. Encryption is the most widely used method to protect data in the Cloud. There is no data-centric approach providing a Role-based Access Control (RBAC) model for access control in which data is encrypted and self-protected. The proposal in this paper supposes a first solution for a data centric RBAC approach, offering an alternative to the ABAC model. An RBAC approach would be closer to current access control methods, resulting more natural to apply for access control enforcement than ABE-based mechanisms. In terms of expressiveness, it is said that ABAC supersedes RBAC since roles can be represented as attributes. However, when it comes to data-centric approaches in which data is encrypted, ABAC solutions are constrained by the expressiveness of ABE schemes. The cryptographic operations used in ABE usually restrict the level of expressiveness for access control rules.

A data-centric approach is used for data self-protection, where novel cryptographic techniques such as Proxy Re-Encryption Encryption (PRE), Identity-Based Encryption (IBE) and Identity-Based Proxy Re-Encryption (IBPRE) are used. They allow to re-encrypt data from one key to another without getting access and to use identities in cryptographic operations. These techniques are used to protect both the data and the authorization model. Each piece of data is ciphered with its own encryption key linked to the authorization

model and rules are cryptographically protected to preserve data against the service provider access or misbehavior when evaluating the rules. It also combines a user-centric approach for authorization rules, where the data owner can define a unified access control policy for his data. The solution enables a rule-based approach for authorization in Cloud systems where rules are under control of the data owner and access control computation is delegated to the CSP, but making it unable to grant access to unauthorize parties.

To overcome the previously mentioned issues, a few recommendations [2] [3] [4] attempt to give information driven arrangements in view of novel cryptographic components applying Attribute based Encryption (ABE) [5]. These arrangements depend on Quality based Access Control (ABAC), in which benefits are conceded to clients as per an arrangement of characteristics. There is a long standing level headed discussion in the IT people group about whether Part based Access Control (RBAC) [6] or ABAC is a superior display for approval [7] [8] [9].Without going into this wrangle about, both methodologies have their own particular advantages and disadvantages.

To the best of our insight, there is no information driven approach giving a RBAC model to get to control in which information is encoded and self-ensured. The proposition in this paper assumes a first answer for an information driven RBAC approach, offering an other option to the ABAC display. A RBAC approach would be nearer to current get to control strategies, coming about more regular to apply for get to control authorization than ABE-based components. In terms of expressiveness, it is said that ABAC supersedes RBAC since parts can be spoken to as traits. In any case, with regards to information driven methodologies in which information is encoded, ABAC arrangements are compelled by the expressiveness of ABE plans. The cryptographic operations utilized as a part of ABE more often than not limit the level of expressiveness for get to control rules. For example, part progression and protest chain of command capacities can't be accomplished by current ABE plans. Additionally, they as a rule do not have some blend with a client driven approach for the get to control arrangement, where regular approval related components like meaning of clients or part assignments could be shared by distinctive bits of information from similar information proprietor.

This paper presents SecRBAC, an information driven get to control answer for self-ensured information that can keep running in untrusted CSPs and gives

broadened Role-Based Access Control expressiveness. The proposed approval arrangement gives a lead based approach taking after the RBAC conspire, where parts are utilized to facilitate the administration of get to to the assets. This approach can control and oversee security and to manage the intricacy of overseeing get to control in Cloud processing. Part and asset progressive systems are bolstered by the approval display, giving more expressiveness to the guidelines by empowering the meaning of basic however capable tenets that apply to a few clients and assets on account of benefit proliferation through parts and chains of command. Strategy manage details are in light of Semantic Web advancements that empower improved govern definitions and propelled strategy administration highlights like clash location. An information driven approach is utilized for information self- assurance, where novel criptograhpic methods for example, Proxy Re-Encryption (PRE) [10], Identity-Based Encryption (IBE) [11] and Identity-Based Proxy Re-Encryption (IBPRE) [12] are utilized. They permit to re-encode information starting with one key then onto the next without getting access and to utilize personalities in cryptographic operations. These systems are utilized to secure both the information and the approvaldemonstrate.

Every bit of information is figured with its own particular encryption key connected to the approval model and guidelines are cryptographicallysecured to protect information against the specialist organization get to or bad conduct while assessing the rules. It additionally consolidates a client driven approach for approval rules, where the information proprietor can characterize a brought together get to control arrangement for his information. The arrangement empowers a rule-based approach for approval in Cloud frameworks where guidelines are under control of the information proprietor and get to control calculation is appointed to the CSP, yet making it not able to allow access to unapproved parties.

II. Attribute Based Encryption

A Attribute based encryption conspire (ABE) was presented by Sahai and Waters in 2005. The objective of this plan is to give security and get to control.

Quality based encryption (ABE) is an open key based one to numerous encryption that permits clients to encode and decode information in view of client traits. Security and access to control is the principle objective of the Attribute Based Encryption. It is an open key (PK)based one to numerous encryption that permits clients to encode and decode information in view of client properties. In which the secret key (SK) of a client and the cipher text(CT) are reliant upon qualities (e.g. the nation she lives, or the sort of membership she has).In such a framework, the decoding of a figure content is conceivable just if the arrangement of properties of the client key matches the traits of the figure content. Decoding is just conceivable when the quantity of coordinating is no less than a limit esteem. Impact resistance (A foe that holds various keys ought to just be get to information if no less than one individual key stipends get to.) is significant security elements of Attribute-Based Encryption.

The issue with Attribute based encryption (ABE) plan is that information proprietor needs to utilize each approved client's open key to encode information. The use of this plan is limited in the genuine environment since it utilizes the entrance of monotonic ascribes to control client's entrance in the framework. Attribute based encryption conspire has different classes which are to be examined in detail encourage. It incorporates Key strategy Attribute based encryption (KP-ABE), Cipher text policy Attribute based encryption (CP-ABE), Attribute-based Encryption plot with Non-Monotonic Access Structures e.t.c.

III. Key policy ABE Scheme

It is the altered type of traditional model of ABE. Clients are doled out with a get to structure (AS) over the information traits.. To mirror the get to structure the mystery key of the client is characterized. Figure writings are marked with sets of property and private keys are connected with monotonic get to structure that control which figure messages a client can decode. Key policy Attribute Based Encryption (KP-ABE) plan is intended for one-to-numerous correspondences.

Calculation takes input K as a security parameter and returns PK as open key and the framework ace mystery key MK. PK is utilized by message senders for encryption.MK is utilized to produce client mystery keys and is known just to the power. For encryption calculation takes a message M, people in general key (PK), and an arrangement of property as info. It yields the cipher text (CT). Key era calculation takes as info a get to structure (AS) and the ace secret key MK. It yields as a mystery key SK that empowers the client to decode the message encoded under an arrangement of properties if and just if matches T[1]. Decoding is conceivable just if the quality set fulfills the client's get to structure. The KP-ABE plan can accomplish secured get to control and more adaptability to control clients than ABE conspire.

The issue with KP-ABE plan is encryptor can't choose who can unscramble the scrambled information. It can just pick clear characteristics for the information, it is inadmissible in some application on the grounds that an information proprietor needs to believe the key guarantor.

IV. Cipher texts Policy ABE Scheme

CP-ABE is the altered type of KP-ABE presented by Sahai. In a CP-ABE conspire, each figure content is connected with a get to strategy on characteristics, and each client's private key is connected with an arrangement of attributes[3]. A client can unscramble a figure message just if the arrangement of qualities connected with the client's private key fulfills the get to approach connected with the figure content. CP-ABE works in the turnaround method for KP-ABE.

The calculation takes as information a security parameter K and returns the general population key PK and additionally a framework ace mystery key MK. PK is utilized by message senders for encryption.MK is utilized to produce client mystery keys and is known just to the power. For encryption of information calculation takes as info the general population parameter PK, a message M, and a get to structure AS. it yields the figure content CT[4]. Key-Generation this calculation takes as information an arrangement of trait connected with the client and the ace key MK. It yields a mystery key SK that empowers the client to decode a message encoded under a get to tree structure T if and just if matches

Decoding of the information just if fulfills the get to structure connected with the figure content CT. It enhances the impediment of KP-ABE that the encoded information can't pick who can unscramble. It can

bolster the get to control in the genuine environment. Likewise, the client's private key is in this plan, a mix of an arrangement of traits, so a client just utilize this arrangement of credit to fulfill in the encoded information

Downsides of the most existing CP-ABE plans are still not satisfying the undertaking necessities of get to control which require significant adaptability and productivity. CP-ABE has impediment as far as indicating approaches and overseeing client properties. In a CP-ABE plot, unscrambling keys just bolster client traits that are composed consistently as a solitary set, so the client can just utilize every conceivable mix of characteristics in a solitary set issued in their keys to fulfill approaches.

V. Attribute-based Access Control (ABAC) model.

The idea of Attribute Based Access Control (ABAC) has existed for a long time. It speaks to a point on the range of consistent get to control from basic get to control records to more skilled part based get to, lastly to an exceedingly adaptable technique for giving access in view of the assessment of characteristics.

ABAC is a legitimate get to control display that is discernible on the grounds that it controls access to objects by assessing rules against the characteristics of the substances (subject and protest) activities and the earth significant to a demand. Properties might be considered attributes of anything that might be characterized and to which an esteem might be allocated. In its most essential shape, ABAC depends upon the assessment of characteristics of the subject, traits of the protest, environment conditions, and a formal relationship or get to control administer characterizing the reasonable operations for subject-question property and environment condition mixes. All ABAC arrangements contain these essential center abilities to assess traits and environment conditions, and uphold guidelines or connections between those characteristics and environment conditions.

The principles or approaches that can be executed in an ABAC model are restricted just to the degree forced by the computational dialect. This adaptability empowers the best expansiveness of subjects to get to the best broadness of items without determining singular connections between every subject and every protest. Provisioning ABAC portrays credits to subjects and protests represented by a get to control decide set that indicates what operations can happen, this ability empowers question proprietors or directors to apply get to control strategy without earlier information of the particular subject and for a boundless number of subjects that may require get to. As new subjects join the association, guidelines and items don't should be altered. For whatever length of time that the subject is appointed the ascribes fundamental for access to the required items, no adjustments to existing standards or protest traits are required. This advantage is frequently alluded to as pleasing the outer client and is one of the essential advantages of utilizing ABAC.

VI. Role based Access control model

The idea of part based get to control (RBAC) started with multi-client and multi-application on-line frameworks spearheaded in the 1970s. The focal idea of RBAC is that consents are connected with parts, and clients are allocated to fitting parts. This enormously simplifies administration of authorizations. Parts are made for the different employment works in an association and clients are appointed parts in view of their obligations and qualifications. Clients can be effectively reassigned from one part to another. Parts can be allowed new authorizations as new applications and frameworks are consolidated, and authorizations can be denied from parts as required.

A part is appropriately seen as a semantic develop around which get to control approach is figured. The specific accumulation of clients and consents united by a part is brief. The part is more steady in light of the fact that an association's exercises or works more often than not change less much of the time. A few unmistakable inspirations for developing a part are examined underneath. A part can speak to competency to do specific undertakings, for example, a doctor or a drug specialist.

A part can encapsulate power and duty, e.g., ace fiject manager. Power also, duty are unmistakable from competency. Jane Doe might be capable to head a few offices, however is relegated to head one of them. Parts can react specific obligation assignments that are turned through various clients, e.g., an obligation

doctor or move director. RBAC models and executions ought to have the capacity to helpfully suit these appearances of the part idea.

A late review by NIST [1] exhibits that RBAC addresses numerous requirements of the business and government segments. In this investigation of 28 associations, get to control prerequisites were observed to be driven by an assortment of concerns including client, stockholder and backup plan confidence, protection of individual data, counteracting unapproved dispersion of financial resources, anticipating unapproved utilization of long distance phone circuits, and adherence to proficient models. The review found that numerous associations construct get to control choices in light of \the parts that person clients go up against as a feature of the association." Many associations liked to midway control and keep up get to rights, less at the framework manager's close to home caution yet more as per the association's assurance rules.

The review additionally found that associations commonly saw their get to control needs as one of a kind and felt that accessible items needed satisfactory flexibility. Other proof of solid enthusiasm for RBAC originates from the measures field. Parts are being considered as a feature of the developing SQL3 standard for database administration frameworks, in light of their usage in Oracle 7. Parts have additionally been consolidated in the business security profile of the draft Common Criteria [2]. RBAC is moreover very much coordinated to winning innovation and business patterns. Various items bolster some type of RBAC straightforwardly, and others bolster firmly related ideas, for example, client bunches, that can be used to actualize parts.

Despite the perceived convenience of the RBAC idea, there is close to nothing concurrence on what RBAC implies. Therefore RBAC is a formless idea deciphered in different courses by different scientists and framework designers, going from easy to detailed and complex.

VII. CONCLUSION

A data-centric authorization solution has been proposed for the safe security of information in the Cloud. SecRBAC permits overseeing approval taking after a manage based approach also, gives advanced part based expressiveness including part and protest chains of command. Get to control calculations are appointed to the CSP, being this not just not able to get to the information, additionally not able to discharge it to unapproved parties. Progressed cryptographic strategies have been connected to ensure the approval display. Re-encryption keys supplement every approval lead as cryptographic token to ensure information against CSP trouble making. The arrangement is free of any PRE plan or execution as far as three particular elements are bolstered. A solid IBPRE conspire has been utilized as a part of this paper so as to give a complete and doable arrangement.

A proposition in view of Semantic Web innovations has been uncovered for the representation and assessment of the approval demonstrate. It makes utilization of the semantic components of ontologies and the computational abilities of reasoners to determine and assess the model. This likewise empowers the use of cutting edge systems, for example, strife discovery what's more, determination techniques. Rules for sending in a Cloud Service Provider have been additionally given, including an half and half approach perfect with Public Key Cryptography that empowers the use of standard PKI for key administration furthermore, conveyance. A prototypical usage of the proposition has been likewise created and uncovered in this paper, together with some trial comes about

VIII. REFERENCES

[1]. Cloud Security Alliance, "Security guidance for critical areas of focus in cloud computing v3.0," CSA, Tech. Rep., 2003.

[2]. Y. Zhang, J. Chen, R. Du, L. Deng, Y. Xiang, and Q. Zhou, "Feacs: A flexible and efficient access control scheme for cloud computing," in Trust, Security and Privacy in Computing and Communications,2014 IEEE 13th International Conference on, Sept 2014, pp. 310-319.

[3]. B. Waters, "Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization," in Public Key Cryptography - PKC 2011, 2011, vol. 6571, pp. 53-70.

[4]. B. B and V. P, "Extensive survey on usage of attribute based encryption in cloud," Journal of

Emerging Technologies in Web Intelligence, vol. 6, no. 3, 2014.

[5]. V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in Proceedings of the 13th ACM Conference on Computer and Communications Security, ser. CCS '06, New York, NY, USA, 2006, pp. 89-98.

[6]. InterNational Committee for Information Technology Standards, "INCITS 494-2012 - information technology - role based access control - policy enhanced," INCITS, Standard, Jul. 2012.

[7]. E. Coyne and T. R. Weil, "Abac and rbac: Scalable, flexible, and auditable access management," IT Professional, vol. 15, no. 3, pp. 14-16, 2013.

[8]. Empower ID, "Best practices in enterprise authorization: The RBAC/ABAC hybrid approach," Empower ID, White paper, 2013.

[9]. D. R. Kuhn, E. J. Coyne, and T. R. Weil, "Adding attributes to role based access control," Computer, vol. 43, no. 6, pp. 79-81, 2010.

[10]. G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "Improved Proxy Re-encryption schemes with applications to secure distributed storage," ACM Transactions on Information and System Security, vol. 9, no. 1, pp. 1-30, 2006.

[11]. F. Wang, Z. Liu, and C. Wang, "Full secure identity-based encryption scheme with short public key size over lattices in the standard model," Intl. Journal of Computer Mathematics, pp. 1-10, 2015.

[12]. M. Green and G. Ateniese, "Identity-based proxy re-encryption," in Proceedings of the 5th International Conference on Applied Cryptography and Network Security, ser. ACNS '07. Berlin, Heidelberg: Springer-Verlag, 2007, pp. 288-306.

[13]. Lawall, D. Reichelt, and T. Schaller, "Resourcmanagement and authorization for cloud services," in Proceedings of the 7th International Conference on Subject-Oriented Business Process Management, ser. S-BPM ONE '15, New York, NY, USA, 2015, pp. 18:1-18:8.

[14]. D. Y. Chang, M. Benantar, J. Y.-c. Chang, and V. Venkataramappa, "Authentication and authorization methods for cloud computing platform security," Jan. 1 2015, uS Patent 20,150,007,274.

[15]. R. Bobba, H. Khurana, and M. Prabhakaran, "Attribute-sets: A practically motivated enhancement to attribute-based encryption," in Computer Security

[16]. ESORICS 2009. Springer Berlin Heidelberg, 2009, vol. 5789, pp. 587-604.G. Wang, Q. Liu, and J. Wu, "Hierarchical attribute-based encryption for fine-grained access control in cloud storage services," in Proceedings of the 17th ACM Conference on Computer and Communications Security, ser. CCS '10, New York, NY, USA, 2010, pp. 735-737.

[17]. J. Liu, Z. Wan, and M. Gu, "Hierarchical attribute-set based encryption for scalable, flexible and fine-grained access control in cloud computing," in Information Security Practice and Experience. Springer Berlin Heidelberg, 2011, vol. 6672, pp. 98- 107.

[18]. W3COWL Working Group, "OWL 2 Web Ontology Language: Document overview (second edition)," World Wide Web Consortium (W3C), W3C Recommendation, Dec. 2012. J. M. A. Calero, J. M. M. Perez, J. B. Bernabe, F. J. G. Clemente, G. M. Perez, and A.

[19]. F. G. Skarmeta, "Detection of semantic conflicts in ontology and rule-based information systems," DataKnowledge Engineering, vol. 69, no. 11, pp. 1117- 1137, 2010.