International Journal of Research and Development in Applied Science and Engineering (IJRDASE)
ISSN: 2454-6844

A Review on Access Control Schemes Application in Cloud Security Environment Modelling

Deepti Priyadarshni
Computer Network,
BBD University, Lucknow, India
deepti.priyadarshini@yahoo.com

Dileep Kumar Gupta
Computer Network.
BBD University, Lucknow, India
dileep.gupta.in@gmail.com

Abstract-- Access control is a mechanism that generates an environment that denies or restricts access to a small or large organization or system. It consists of monitoring and recording of all attempts and procedure made in a stepwise during access of a system. During the access mechanism it is to be identified the user's authentication in respect to his access of a system in an authorized or unauthorized manner. This article provides a review on various mechanisms which are of significant for protection in data storage and access in computer security. Various access control models are studied and considered which includes the most common role based access control, attribute based access control, discretionary access control and temporal Based Access Control. All these models are well known and identified in various forms in access control mechanisms.

Keyword-- Access control, RBAC,TBAC , cloud computing ,storage and security.

1. Introduction

"Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction"[8].

Cloud computing has started to be applied in industry due to the advantage of reducing capital expenditure and transforming it into operational costs [9]. Therefore, applications are directly built using Cloud service technology or existing applications are migrated to the Cloud.

As there are a hefty amount of issues and concerns around privacy and confidentiality of data, and they are a continuous subject of controversy in our society which raises questions difficult to answer. Some examples of these questions that may arise from Cloud customers:

"How secure is my data?

Can I trust my cloud provider?

Which are the risks and mitigations for any existing issue on my data in the cloud?"

Now a day's not just a single user is using cloud computing for his/her personal use, but there are many big organizations as well, that are using cloud computing facilities in large scale.

Cloud computing provides an extensible and powerful environment for growing amounts of services and data by means of on-demand self-service. It also relieves the client's burden from management and maintenance by providing a comparably low cost, scalable, location-independent platform. However, cloud computing is also facing many challenges for data security as the users outsource their sensitive data to clouds, which are generally beyond the same trusted domain as data owners. To address this problem, access control is considered as one of critical security mechanisms for data protection in cloud applications.

The three service delivery models for cloud computing are:

(1) Software as a Service (SaaS) in which cloud customers use the provider's applications over the Internet; (2) Platform as a Service (PaaS) in which customers deploy their self-created applications on a development platform that a cloud service provider provides; and (3) Infrastructure as a Service (IaaS) in which cloud customers rent processing, storage, network capacity from cloud service provider.

The cloud computing paradigm is associated with security concerns both at the providers' end and consumers' end. While providers want to ensure that their resources and services are utilized only by authorized users; consumers would like to ensure that their data is securely maintained in the cloud and that the servers are not compromised.

Access control is a fundamental aspect of information security that is directly tied to the primary characteristics such as confidentiality, integrity and availability. Cloud computing service providers should provide the following basic functionalities from the perspective of access control: (i) Control access to the service features of the cloud based on the specified policies and the level of service purchased by the customer. (ii) Control access to a consumer's data from other consumers in multi-tenant environments. (iii) Control access to both regular user functions and privileged administrative functions. (iv) Maintain accurate access control policy and up to date user profile information.

For these reasons, this thesis aims at providing a **Three-Stage Role Based Access Control Model (3-Stage RBAC)** for maintaining privacy and confidentiality of data while using cloud computing.

2. Related Work:

Innovations are necessary to ride the inevitable tide of change. Most of enterprises are striving to reduce their computing cost through the means of virtualization. This demand of reducing the computing cost has led to the

innovation of Cloud Computing. Cloud Computing offers better computing through improved utilization and reduced administration and infrastructure costs. Cloud Computing is the sum of Software as a Service (SaaS) and Utility Computing. Cloud Computing is still at its infant stage and a very new technology for the enterprises. Therefore, most of the enterprises are not very confident to adopt it. **Björn Johanssonand, Paul Pierce (2011),** [1] tackled this issue for enterprises in terms of cost and security. In this work I discuss the benefits and drawbacks an enterprise can have while they adopt Cloud Computing in terms of Cost and Security. In the end, concluding that Cloud Computing is better for medium and small sized enterprises as compared to large enterprises in terms of both cost and data security.
In this research work, they tackled the affects of Cloud Computing in the enterprises. The specific areas they researched during my study were cost and security. They have found that Cloud Computing is a very hot topic now days and many enterprises are interested in it. Most of the enterprises have idea about it but still there is confusion about the real definition of Cloud Computing. This is understandable as this technology is in its infant stage however, as it evolved from Grid Computing therefore, most of the enterprises which have used Grid Computing are better able to understand the term Cloud Computing. There is a confusion or disagreement about the boundaries of Cloud Computing as many enterprises and even cloud providers believe that private cloud is a part of Cloud Computing. However, in my research They have found that Cloud Computing is the sum of Software as a Service (SaaS) and Utility Computing, but does not include Private Clouds. The enterprises which are in the process of making a decision to adopt Cloud Computing face real dilemma as they hear different (positive and negative) views from different sources. The first characteristic that tends enterprises to think about Cloud Computing is the cost effect. I have done a thorough research about the cost effect on enterprises. There are many factors or characteristics which affect the cost of Cloud Computing for enterprises. These factors include elasticity, flexibility, data center cost, pricing models and administrative costs. The elasticity is the biggest factor to make Cloud Computing cost effective for enterprises and most of the enterprises move to cloud because of this characteristic of Cloud Computing. I have concluded that enterprises save their capital by not building their data center and not hiring employees for managing them. Along with that flexibility and different pricing models makes Cloud Computing more cost effective for enterprises. However, an important finding is that these benefits are only for medium sized or small enterprises. The large enterprises can save their cost by building big data center due their demand and capital they have. In other words, private cloud is something perfect for the large enterprises.

Access control is one of the most important security mechanisms in cloud computing. Attribute-based access control provides a flexible approach that allows data owners to integrate data access policies within the encrypted data. However, little work has been done to explore temporal attributes in specifying and enforcing the data owner's policy and the data user's privileges in cloud-based environments. In this work, **Yan Zhu, Hongxin Hu, Gail-Joon Ahn, Dijiang Huang, and Shanbiao Wang (2012),** [2] presented an efficient temporal access control encryption scheme for cloud services with the help of cryptographic integer comparisons and a proxy-based re-encryption mechanism on the current time. They also provide a dual comparative expression of integer ranges to extend the power of attribute expression for implementing various temporal constraints. We prove the security strength of the proposed scheme and our experimental results not only validate the effectiveness of our scheme, but also show that the proposed integer comparison scheme performs significantly better than previous bitwise comparison scheme.
In this work, they addressed the construction of temporal access control in cloud computing. Based on forward/ backward derivation functions, we proposed a temporal access control encryption to support time range comparisons and re-encryption mechanism. They also discussed how to handle current time controls and temporal constraints with our solution.

Abdul Raouf Khan (2012), [3] Cloud computing is one of the emerging technologies. The cloud environment is a large open distributed system. It is important to preserve the data, as well as, privacy of users. Access Control methods ensure that authorized user's access the data and the system. This work discusses various features of attribute based access control mechanism, suitable for cloud computing environment. It leads to the design of attribute based access control mechanism for cloud computing.
Access control decisions are very important for any shared system. However, for a large distributed system like a cloud system, access decision needs to be more flexible and scalable. This work presents various access control methods used in cloud computing and highlights features of attribute based access control features, which are important for designing an attribute based access control.

Santosh Bulusu et. al. (2012), [4] aimed to identify security challenges for adapting cloud computing and their solutions from real world for the challenge that do not have any proper mitigation strategies identified through literature review. For this the objective is to identify existing cloud computing security challenges and their solutions. Identify the challenges that have no mitigation strategies and gather solutions/ guidelines/practices from practitioners, for a challenge with more references but no mitigation strategies identified. This study presents a literature review and a snowball sampling to identify CC security challenges and their solutions/mitigation strategies. The literature review is based on search in electronic databases and snowball sample is based on the primary studies searched and selected from electronic databases. Using the challenges and their solutions identified form literature review, challenges with no mitigation strategies are identified. From these identified challenges with no mitigation strategies, a challenge with more references is identified. The surveys are employed in the later stages to identify the mitigation strategies for this

challenge. Finally the results from the survey are discussed in a narrative fashion.

This study identifies cloud computing security challenges and their solutions. Where these (challenges and solutions) are common to cloud computing applications and cannot be generalized to either service or deployment models (viz. SaaS, PaaS, IaaS, etc.). The study also identifies that there are methods (guidelines/practices identified from practitioners) to provide secure interoperability, migration and integration of on-premise authentication systems with cloud applications, but these methods are developed by individuals (practitioners/ organization) specific to their context. The study also identifies the non-existence of global standards for any of these operations (providing interoperability/migration/IDM integration with cloud). This identified non-existence of global standards and guidelines could be help academics to know the state of practice and formulate better methods/standards to provide secure interoperability. The identified cloud computing security challenges (43) and solutions (89), can be referred by practitioners to understand which areas of security need to be concentrated while adapting/migrating to a cloud computing environment.

Takahiko Kajiyama (2012) [5], according to him many IT professionals would agree that cloud computing is the most revolutionary information delivery model since the introduction of the Internet. For corporate management and decision makers, cloud computing brings many financial and functional benefits as well as serious security concerns that may threaten business continuity and corporate reputation. The definition of cloud computing is still blurry in a large part, because of the magnitude of the security risks and the virtually unlimited amount of information being published. The purpose of this research is to assess how cloud security risks and threats most commonly discussed today are affecting current and prospective cloud users' decisions on adoption. In this research, both practitioner and academic literature was reviewed in order to incorporate views from both sides on cloud security, as well as technology white works, government reports, and recent market and security articles. Then an online survey targeting current and prospective cloud users was conducted, and real-life driving and resisting forces of cloud adoption were assessed. The survey posed questions about a variety of security risks, and even though the respondents indicated concerns about these risks, none of them were voted as a "show stopper" in cloud adoption. Furthermore, the majority of respondents were confident with their cloud service providers' protection mechanism, while being well aware of the existence of the risk.

Because of the magnitude of both risks and benefits it brings, cloud computing continues to be one of the most actively discussed, researched, and criticized technologies in IT. One possible drawback from its popularity is the information overflow caused by researchers and practitioners, making it more difficult for organizations to obtain applicable information they require in addressing cloud security concerns. The aim of this thesis is to clearly identify the current security risks of cloud computing, and to measure how these risks are affecting organizations' decisions on cloud adoption. The results show that both current and prospective cloud users are well aware of the existing risks and threats, yet the majority of them believe cloud computing is reasonably secure for both non-critical and mission-critical application deployments. Because of the nature of the technology and architecture it is based on, cloud computing does require more preventative measures and broader security perimeter than traditional, on-premise application and data hosting. However cloud computing, if properly planned and deployed, will bring positive economic, functional, and for some organizations additional security benefits. The favorable outcome is being the primary driving force, as the recent economic fallout is forcing organizations seek more cost effective solutions, and this trend of favoring cost-saving solutions is likely to continue at a rate consistent with the growth of cloud adoption. The priority of computer security has shifted drastically in the past decade, yet both service providers and users are in agreement that cloud adoption is likely to accelerate despite of its high security concerns. The level of concern will probably remain high, as the world will continue to observe occasional cloud security incidents, as well as non-cloud breaches and hacker attacks. For some organizations, however, high security concerns are affecting decision makers in a positive and constructive manner, rather than being a show stopper, as they take more precautions and preventative measures to mitigate these risks. Added regulatory compliance requirements and privacy concerns, post-adoption security measures such as continuous monitoring and auditing will also be taken seriously and make cloud environments even less vulnerable. Unlike the era of Internet boom, when everybody immediately jumped onto the bandwagon and learned hard lessons later, it can be said that cloud computing is probably the most carefully adopted trend in IT in the recent years. For further research, as the vast majority of the survey respondents indicated that cloud computing is going to be more secure in the future as the service models become more mature and better technologies become available, close examination of cloud service providers' effort for bringing cloud security to the next level, and the advancement of SECaaS is recommended. In addition, as cloud computing is encroaching on mobile devices such as smartphones and tablets, more research could be conducted to evaluate cloud security concerns that are specific to mobile devices.

The relationship between users and resources is dynamic in the cloud, and service providers and users are typically not in the same security domain. Identity-based security (e.g., discretionary or mandatory access control models) cannot be used in an open cloud computing environment, where each resource node may not be familiar, or even do not know each other. Users are normally identified by their attributes or characteristics and not by predefined identities. There is often a need for a dynamic access control mechanism to achieve crossdomain authentication. In this work, we will focus on the following three broad categories of access control models for cloud computing: (1) Role-based models; (2) Attribute-based encryption models and (3) Multi-tenancy models. They reviewed the existing literature on each of the

above access control models and their variants (technical approaches, characteristics, applicability, pros and cons), and identify future research directions for developing access control models for cloud computing environments.

Natarajan Meghanathan (2013) [6], identified the following future research directions for access control models in cloud computing environments: (1) Develop attribute-driven role-based access control models such that the userrole and role-permission assignments be separately constructed using policies applied on the attributes of users, roles, the objects and the environment; and the attribute-based user-role and role-permission assignment rules be applied in real-time to enforce access control decisions. (2) Develop a location-aware role-based control model incorporated to the Policy Enforcement Point of a cloud (thereby, preventing the disclosure of user's identity, role, or location directly to a remote server in the cloud that may not be fully trusted), and enable/activate the role only when the user is located within the logical positions (computed from real positions by specific mapping functions) that lie within the spatial boundary of a role. (3) Explore software-hardware co-design for security such that the fine-grained access control and usage control mechanisms implemented in software are integrated with new hardware architectural and virtualization features that can help protect the confidentiality and integrity of the data and the resources, even when the powerful underlying hypervisor may be compromised. (4) Mitigate insider threats to the data and resources from the perspective of both a rogue cloud provider administrator and the employee in the victim organization that exploits cloud weaknesses for unauthorized access. (5) Incorporate the relationship between trust and reputation in the access control models for better and secure service quality within the cloud. The security challenges of cloud computing are exacerbated due to some of its characteristic features such as resource sharing, multi-tenancy and virtualization. Due to the multi-tenancy model of cloud computing, users (tenants) of a cloud computing environment prefer their traffic to be isolated from all other tenants. Though access control for cloud environments are typically provided using techniques such as VLANs and firewalls, these are more suited for enterprise environments and cannot meet the challenges in emerging cloud environments. The challenges include multi-tenancy, diversity in cloud network architectures, scalability (large scale) and the high dynamism of the cloud infrastructure. With multi-tenancy, intra cloud communication (e.g., provider-tenant and tenant-tenant) is becoming a norm and it requires fair sharing between tenants and rate-limiting tenants, which cannot be provided using VLANs and firewalls. In a distributed multi-cloud environment, collaboration between clouds can be either globally federated (consistent with global meta policy), loosely coupled (based on verification of per-cloud access control policies) or ad hoc (establish secure collaboration on a per-user basis). It is possible for all these three collaborations to coexist together in a large scale cloud and systematically update a virtual global directory service on virtualized shareable resources and services of each cloud, manifested across service-level agreements (SLAs). The new network architectures to evolve for the data centers should employ multiple paths and require specific routing algorithms and address assignments. As today's clouds scale to tens of thousands of physical machines, with a lot more virtual machines added and removed, enterprise level access control mechanisms will not be scalable enough to handle attacks (e.g., denial of service attacks between cloud tenants) that target a large number of entities, in the order of the magnitude typically seen in the public Internet. Thus, new access control mechanisms for cloud computing environments must be flexible (to support a multi-tenant environment), scalable (handle hundreds of thousands of machines and users) and network independent (decoupled from the underlying network topology, routing and addressing).

Cloud computing is an advanced emerging technology. In this world the storage of data is a big headache for all. Cloud computing is an efficient solution for the easiest and fastest storage and retrieval of data. The main issue in cloud computing is security. Here **Bibin K Onankunju, (2013)** [7], tryied to introduce a new method for providing secured access control in cloud computing. This model provides a secure access control in cloud computing. To provide more secured access control it adopt a hierarchical structure and it uses a clock. Using this we can easily upload, download , delete files from and to the cloud.

It is a highly efficient model for provide access control in cloud computing. It is in a hierarchical structure and it using a clock for providing decryption key based on time. This model ensure both security and access control in cloud computing. The main operations in this model are registration, file upload, file download and file deletion.

One of the other main method for access control is FADE which is introduced by Y.Tang and team [5]. The method in [5] provides fine-grained access control and assured deletion for outsourced data on the cloud. But this scheme is not effectively applicable . If the data owners and service providers are in the same domain, then only it act as an effective scheme. One of the other scheme for access control is HASBE which is introduced by Z.Wan, J.Liu and R.H.Deng [2]. The main drawback of the scheme in [2] is that it is not flexible compared to other schemes.

In [10], S.Yu and team introduce a method for access control in cloud computing. In this method [10], they using KP-ABE (Key Policy Attribute Based Encryption) and PRE(Proxy Re-Encryption) . Due to the overhead of encryption and decryption, this method is not scalable.

Y.Zhu and team introduce a method for temporal access in cloud computing. In [6] these schemes are only applicable to systems in which data owners and the service providers are within the same trusted domain. The other main scheme is explained in [4] ,which is introduced by M.Li and his group . But it is very costly scheme.

In an International Joint Conference of IEEE TransCom-11, M.Zhou and his colleagues introduce a method for privacy-preserved access control for cloud computing [9]. This method [9] also has some drawbacks. But here, in this scheme, lack of flexibility and scalability make it as ineffective.

Condor is a centralized workload management system suited for computation-intensive jobs executed in local closed Grid environments. Its resource management mechanism is similar to that of UNIX (discretionary access control), with some additional modes of access besides the traditional read and write permissions. Legion uses an object-oriented approach wherein all files, services and devices are considered as objects, and are accessed through functions of these objects. Each object can define its own access control policy, typically done using access control list and authentication mechanisms, in a default MayI function that is invoked before any other functions of the object may be called. The Globus Grid Toolkit (GT) proposes mechanisms to translate users' grid identities into local identities (which can in turn be verified by the resource providers using appropriate local access control policies) and also allow users' certificates be delegated across many different sites.

With the single sign-on mechanism (e.g., Open Grid Service Infrastructure, OGSI), users can login only once and have access to multiple grid sites, as well as programs can be authorized to access resources on a user's behalf and can further delegate them to other programs. The OGSI operates in conjunction with resource usage brokers (e.g. Gruber) that act as distributed policy enforcement points to enforce both local usage policies and global service level agreements (SLAs) and allow resources at individual sites to be efficiently shared across multiple sites. In, the authors propose a flexible attribute-based multi-policy access control (ABMAC) model for grid computing systems in which each autonomous domain may have its own security policy ABMAC is based on the idea of integrating the individual authorization decisions arrived at for user requests to access resources/services (all of which are identified with their characteristics or attributes) according to the security policy of each domain and arriving at a final decision using a combination algorithm that can be adapted to suit to the resource/operating constraints. The ABMAC approach is more scalable compared to developing a superset of individual domain policies and evaluating user request for resource access according to this superset.

In a role-based access control (RBAC) model, the role of a user is assigned based on the least privilege concept – i.e. the role with the least amount of permissions or functionalities that is necessary for the job to be done. Task Role-based access control model (TRBAC) has been considered a viable model for cloud computing environments wherein the traditional static access control models such as discretionary, mandatory or simple role-based models cannot be employed. TRBAC can dynamically validate access permissions for users based on the assigned roles and the task the user has to perform with the assigned role. Tasks could be classified as workflow tasks (those that need to be completed in a particular order) that require active access control and non-workflow tasks (those that can be completed in any order) that require passive access control. Workflow tasks driven active role-based access control is time sensitive and the access permissions assigned for users performing these tasks change dynamically with time, depending on the order in which the tasks are to be executed. Care should be taken to ensure that a user has the minimum required privileges to perform a task under a particular role, and that no role can be assigned to two or more tasks at the same time. Another variant of role-based access control proposed for cloud computing environments is the Attribute-role-based access control (ARBAC) model, wherein the data object to be protected are assigned certain attributes and values; a user with a specific role has to submit the appropriate values for these attributes, and are given access to the objects after proper validation by the service provider. A fine-grained key based ARBAC model has been proposed in, where users are assigned the private keys or symmetric keys that are used to encrypt/decrypt the values of the attributes defined for the data objects whose privacy needs to be protected.

Bertino et al proposed the temporal-RBAC (TRBAC) model that enables and disables a role at run-time depending on user requests. In, the authors argue that in some applications, certain roles need to be static and stay enabled all the time, while it is only the users and permissions that are dynamically assigned. In this context, they proposed a generalized TRBAC (GTRBAC) model that advocates for role activation instead of role enabling. A role is said to be activated if at least one user assumes that role. GTRBAC supports the enabling and disabling of constraints on the maximum active duration allowed to a user and the maximum number of activations of a role by a single user within a particular interval of time. In, the authors present an XML-based RBAC policy specification framework to enforce access control in dynamic XML-based web services. However, both GTRBAC and X-RBAC cannot provide trust and context-aware access control (critical for dynamic web services, characteristic of cloud computing environments), and rely solely on identity or capability-based access control. In, the authors propose an enhanced hybrid version of the X-RBAC and GTRBAC models, called the X-GTRBAC model. X-GTRBAC relies on the certification provided by trusted third parties (such as any PKI Certification Authority) to assign the roles to users. X-GTRBAC also considers the context (such as time, location, or environmental state at the time the access requests are made) to directly affect the level of trust associated with a user (as part of user profile), and incorporates it in its access control decisions. The access privileges for a user/role are based on the threshold (i.e. the trust level) established based on the requestor's access patterns; if the user appears to deviate from his/her usual profile, then the trust level for the user is automatically reduced to prevent potential abuse of privileges. Such a real-time feature of X-GTRBAC suits to the web-based cloud computing environments with diverse customer activity profiles.

3. Conclusion

In this article a review on the recent developments is performed for the improvement of access control mechanism used in data security and authentication system applied for overcoming the effects of unauthorized access due to the protocol errors of the system mechanism. We have discussed about various methodologies applied in last ten years in the research area of access control in data

system to compare the performance and efficient usage of these technologies. It has been observed that the recent methodologies are incorporating latest A.I technique like fuzzy logic, neural network, SVM etc. for full filing the growing demand of speed and accuracy. Hybrid mechanism like neuro fuzzy methods proved to be outperforming in data access and security. In future we can expect the involvement of optimization technique like GA and PSO based evolutionary algorithms in developing improved access control mechanism rules. Hence it can be concluded that in future we can realize on the methods which includes experts learning based detection consist of organizational knowledge, that may lead to various modifications.

References:

[1] Björn Johansson, and Paul Pierce, " Cloud Computing's Effect On Enterprises", School of Economic and Management, 2011.
[2] Yan Zhu, Hongxin Hu, Gail-Joon Ahn, Dijiang Huang, and Shanbiao Wang, "Towards Temporal Access Control in Cloud Computing", The 31st Annual IEEE International Conference on Computer Communications: Mini-Conference.
[3] Abdul Raouf Khan, "Access Control In Cloud Computing Environment", ARPN Journal of Engineering and Applied Sciences, Vol. 7, No. 5, May 2012.
[4] Santosh Bulusu et. al., "A Study on Cloud Computing Security Challenges", School of Computing Blekinge Institute of Technology, 2012.
[5] Takahiko Kajiyama "Cloud Computing Security: How Risks And Threats Are Affecting Cloud Adoption Decisions" San Diego State University, 2012.
[6] Natarajan Meghanathan "Review Of Access Control Models For Cloud Computing", ICCSEA, SPPR, CSIA, WimoA - 2013.
[7] Bibin K Onankunju, "Access Control in Cloud Computing", International Journal of Scientific and Research Publications, Volume 3, Issue 9, September 2013.
[8] Peter Mell and Tim Grance. The NIST definition of cloud computing. National Institute of Standards and Technology, 53(6):50, 2009
[9] Armbrust, M. et al. Above the Clouds: A Berkeley View of Cloud Computing. EECS Department, University of California, Berkeley. Technical Report UCB/EECS-2009-28,
[10] Bibin K Onankunju, Access Control in Cloud Computing. International Journal of Scientific and Research Publications, Volume 3, Issue 9, September 2013