A Critical Comparative Study and Characterisation of Access Control Model

Oyeyinka, F.J[#1], Idowu, S.A[*2], Kuyoro, A[#3], Joshua, J.V[*4], Akinsanya, A.O[#5], Eze, M.O[*6], Ebiesuwa Seun[#7]

[1,2,3,4,5,6,7] *Computer Science Department, Babcock University, Ilishan-Remo. Ogun State, Nigeria*

Abstract *This paper reviews access control methods as they relate to cloud computing. Although advantages of cloud computing over traditional computing techniques cannot be overemphasised; cloud computing presents new security challenges which traditional access control method may not be able to handle, hence proposed access control methods for cloud computing were reviewed and the drawback of each method highlighted. A characterisation of the access control methods was attempted using the various features discussed in literature and comparison of the characteristics was done. From the analysis, features of RBAC and ABAC are the best among the Access Control methods but both has weaknesses in confidentiality and integrity. ABAC was also shown to be very complex. Hence it was suggested that research efforts should be concentrated in building ABAC model that is more secure and easy to implement.*

Keywords—*Cloud computing, Access Control, Role Based, Rule Based, Attribute, policy.*

I. INTRODUCTION

Cloud computing is a general term that is used to describe a class of network-based services that takes place over the Internet. In cloud computing, the resources are made available with little cost. Cloud is perceived in different ways by different group of people; it is an on-demand model that enables access to computer resources over a network (Zhenji et al, 2013). The cloud in this case refers to the Internet based resources. Hence cloud computing means a real time Internet based information technology services that satisfy users' needs without the users having to pay high maintenance and infrastructure cost. Cloud computing offers a wide range of services to organisations and businesses over a large network like the internet (Habib et al, 2010). There are cloud platform technologies that have been built that allow large number of businesses and employees to run their computing jobs online (Halton et al, 2009). Cloud computing has great advantages over data centre based services. One of them is the reduction in IT-related operational costs and complexities.

Despites the advantages of cloud computing, various security challenges associated with this emerging technology include the security issues in a wide form. These problems include trusting the data warehoused in the cloud, the cloud computing technology and the providers themselves. Cloud computing is an unsecured platform due to the fact that the client do not have control over data integrity, confidentiality, authenticity or availability. The complete control of the cloud computing infrastructure that renders the cloud services is in custody of the cloud provider (Ali A., 2011).

Hence, to guard against the issue of insecurity in the cloud for any organisation, that is to keep the data and resources intact against unauthorised access, the access control must be strong enough to detect any form of impersonation. It must only be the rightful user that will be granted access at any point in time. A lot of policy control and regulation must be carried out (Bokefode et al, 2013).

The remaining part of this paper is organised as follows: section two reviews the relevant literature; section three presents some popular Access Control methods, their characteristics and their comparison with an evaluation of these characteristics while section four concludes the paper.

II. REVIEW OF RELEVANT LITERATURE

Access control is a security measure that is devised to checkmate human interaction (e.g. who or what can have access) with the use of resources in a computing environment. There are majorly two types of access control; the physical access control and logical access control. The physical access control restricted access to campuses, buildings, rooms and physical IT assets while the logical access control on the other hand limits connections to computer networks, system files and data. Access control systems carried out the following activities authorization, identification, authentication, access approval, and accountability of entities through login

credentials including passwords, personal identification numbers (PINs), biometric scans, and physical or electronic keys.

The privilege a user has to the system resource or object are contain in an access control log which is in form of a table called access control list (ACL). The list is an indicator that shows the operating system the permission right of the user. An object can be a server, file database or other online resources. Each object has a means of identifying them such attributes to be able to know the users attached to particular resources on the access control log. There is an indicator on the access list for each user that possesses the access privileges. Some of the easiest access right is right to read, write and to execute a file. If a user cannot be identified on the access control list the request to the resources can be turned down. The followings UNIX-based systems, Digital's OpenVMS, Microsoft Windows NT/2000, Novell's NetWare, and so on are some of the example of operating systems that made up access control lists. The access control lists work differently from the operating system activity. For instance, access control list (ACL) in Windows NT/2000 is related one on one with system object. An ACL may have single or many access control entries (ACEs) which contain the name of a user or group of users. A user can be a role name, like a programmer, or a tester. For each of these categories of users, groups, or roles, the access privileges are indicated in a string of bits called an access mask. Generally, the access control lists for an object are created by the system administrator or the object owner (Margaret R., 2013).

A. Taxonomy and classification of computer security Models

Access control has become a major issue in information security as at today's technology. The demand for data consumption seems to be overwhelmed that the traditional security tools need overhauling. Hence, there is need to study the trend of information security tools in this research work though the concerns of this work is majorly of access control as information security tool. The chart in Figure 1shows the diagrammatic representation of the taxonomy of existing computer security tools under which we have forensic, Trust, Risk Assessment, Security policy, Access control, Privacy control, Cryptography and encoding and others. The interest of this research work is on Access control; it is one of the popular security techniques in literature. Access control models have been popular at dealing with security issues in the cloud. Many models had been proposed for controlling access in cloud computing. Access control has five traditional models that form the basis for other categories which are: Matrix Based, Rule-Based Access Control, Discretionary Access Control, Mandatory Access Control and Role Based Access Control. Among the existing traditional model, Role Based Access control over time stand the test of time and have received attention from various researchers. The following sub-divisions are some of the access control models as discovered through research as an off shoot of role based access control of the model: Context-Based Access Control, Attribute Based Access control, Provenance Based Access Control, Gateway Based Access Control, Policy Based Access Control, History Based Access Control, Intranet Based Access Control, Relationship Based Assess Control, Certificated Based Access Control, Usage Control, Workflow Access Control, Hypertext-Based Access Control, Tasks Based Access Control, Agent Based Access control and so on. Each of the models will be explained in the next section.

Access control is one of the ways of solving security challenges faced in today's cloud. It's an aspect that handles assessment of privilege right users has on the resources requested. The access control is enables each time a user make attempt to use or access resources to be sure is the authorized person. The security administrations setup the credentials of the users that must have access to a particular resource in a list called access control list. Anyone user whose credentials is not in the list will be denied access.

The aim of access control is to preserve the confidentiality and integrity of the data in cloud or other medium. The confidentiality can be seen in terms of securing users data and its privacy; information in cloud provider custody must be kept private to the owner. And integrity can be view as a means of maintaining data originality. The content of the data must not be distorted either through modification or alteration. The world generally is in quest of data in large number, every of our day-to-day activities require data there is need to protect the data from been misused or mishandled. Thus, adequate security measure must be put in place to forestall any future security challenge (Le X., 2005 & Abhishek et al, 2014).

B. Categories of Access Control Model

The various access control models both the tradition models and the offshoot will be discussed in this section. These include Matrix Based Access Control (MBAC), Discretionary Access Control (DAC), Mandatory Access Control (MAC), Role Based Access Control (RBAC) and Rule Based Access Control (ReBAC). These earlier versions of the traditional access control model are inadequate to

handle the security challenges in the cloud with huge resources, and numerous users; the access control must be dynamic and flexible. The Access control models (ACM) are meant for securing resources or data by controlling access to the system and the resources itself. This is a very relevant issue to be addressed compared with the alarming rate of quest for data and information as a result of the technology improvement. The data and other resources in the cloud must be properly secured and monitored to ensure that privacy of the customer is not violated (Majunder et al, 2012). The first three of these models are the basis for other models in literature.

1) ***Matrix Access Control (MATAC)***

MATAC is a mathematical model of Lampson established in the late 1960s. The models used formal mathematical notations of subject and object and an access matrix to represent the access of subjects to objects. The access matrix [i,j] represented subject and object which indicate the right that subject i has to object j (Lampson, 1969)].

2) ***Rule-Based Access Control (RuBAC)***

This model was introduced as a complement to the research work on matrix model. A mathematical notation was used to define access control rules. The predefined rules are the only criteria to permit users access to the systems. The RUBAC is used by organization with defined rules that guides their operation although there is no standard that support the model (Bell et al, 1973).

3) ***Discretionary Access Based Control (DAC)***

It is one of the traditional models where users take total control of the resources and decides who can have access to the resources. Access is granted based on the identification and authorization policies set by DAC (Punithasurya et al, 2012).

In DAC, authorisation rules that guide the access right of the subject and object are clearly stated in the system. Subject also means customer, user, system or process or group. The groups or processes can take the place of other subjects. It should also be noted that the subject as the original owner of an object or resources has the sole responsibility to decide whom to grant permission to its resource or can also decide whom to deny access at his discretion. The flexible rules help DAC to maintain authorisation database which is made up of the authorized users. Although the policies have a weakness in that it does not possess high security assurance (James et al, 2001). Though DAC is good but it can easily be exposed to attack and the original message of the owner can be duplicated without the owner's permission.

4) ***Mandatory Access Control (MAC)***

MAC model ensure confidentiality and integrity of data by controlling information flow, this does not feature in DAC model. It has a policy that is centrally controlled by security policy administrator and cannot be violated by the users ((Punithasurya et al, 2012). The classification of all subject and object in a MAC model for the process of access decision are based on predefined sensitivity levels. To achieve information integrity in MAC model one of the rules is that there is a restriction to the flow of information. It ensures that information in higher sensitivity level is restricted to that level alone. There is no cross link of information from higher sensitivity level to lower sensitivity level (Sandh, 2000). For a cloud based applications multilevel classification of information is required by the cloud service provider in other to differentiate between the users and the resources being accessed. It is easy to monitor the current access state of the object in MAC model because each object to be accessed has an attached security code (Ferraiolo et al, 1999 &2000). It is used in military and government application where the security is very strict and tight. MAC model are more robust than DAC model for data protection, however enforcement of MAC policies is difficult for cloud based application. Also the security code once identified to a particular subject in the hierarchy will not be modified. These entire shortcomings are addressed by RBAC.

5) ***Role Based Access Control Model (RBAC)***

This model has been described as a generalised access control model because they provide well recognised advantages. This model based its operation on the assignment of roles, duty or task to the user. The decision to allow users access to resources in RBAC is based on its roles in the organization. Roles are therefore, a set of policies related to the subject or object. The policies are pre-defined rules that help to prevent or permit users access to information. Without granting the permission on the object, the user cannot be activated. RBAC have been widely accepted by research community and organisation that used them for the day to day protection of their business transactions. It provides security for a web based application. Multiple roles can be assigned to a user at the same time (Punithasurya et al, 2012). Several models of RBAC have been discovered by researchers which includes introducing a form of hierarchy to role assignment. The assignment of duty in organisation can also be based on priority or seniority (Majunder et al, 2012). RBAC model is good for the security requirement of cloud applications. As part of its Advantages, RBAC allows roles-user classification,

reduced information distortion by intruders and it limit access to the authorised users alone. However, in literature the challenge has been how to develop a RBAC framework that will be able to keep track of the volume of data accumulated over a period of time as reported and implemented for the web (Ferraiolo et al., 1999& 2010) and difficulty of maintaining information about the roles as numbers of role increases (Tari et al, 1997). Also the request to access resources can be changed or deleted due to change of roles or duties

The following three fundamental rules are specified for RBAC (see fig 1):

Role assignment: A subject can only be permitted an access to object once a role is assigned.

Role authorization: An active role must be authorized for the subject. From rule 1 above, users can only take roles on which they are authorized.

Permission authorization: A subject can only be granted access only if the permission is authorized for the subject's active role (Parminder et al, 2013)& (Oyeyinka et al, 2015). The diagram for RBAC is presented in figure 1 & figure 2.

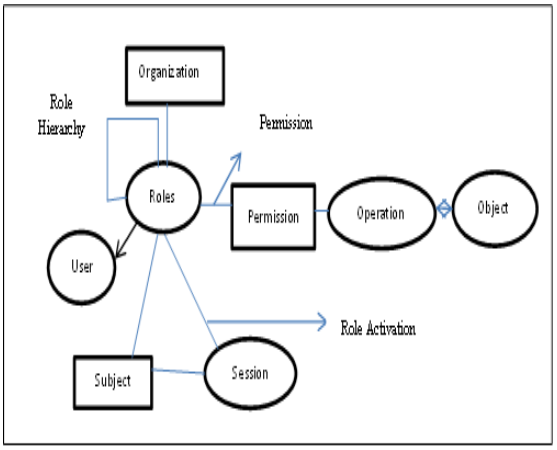

Figure 1: RBAC Model. Adapted from: (Parminder et al, 2013)

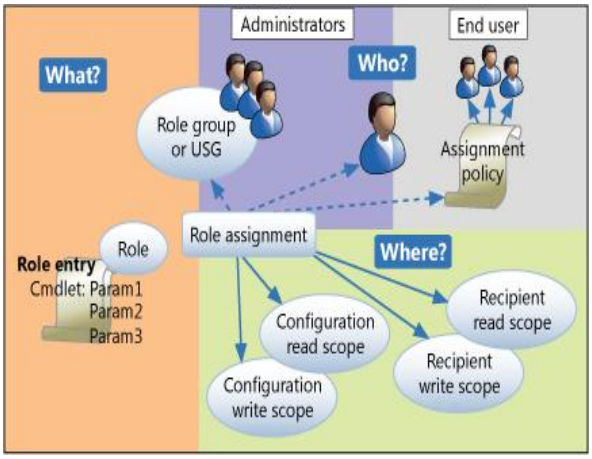

Figure 2: RBAC Architecture

6) *Attribute-Based Access Control (ABAC)*

In recent years, Attribute-Based Access Control has gained recognition in the academic and industrial community (Oasis, 2005)); (Vincet et al, 2014), (Xin et al, 2012), & (Xin et al, 2013). The decisions are made on the basis of the values of attributes, resources and other entities of interest within a system assigned to the users. ABAC uses attributes of users or object rather than assigning roles. The model works with authentication, authorization, identification and accountability. ABAC is more secure, flexible, scalable and hierarchical in structure ((Punithasurya et al, 2012).

Attribute Based Access control is made up of two main parts; a set of static-attribute-based rules, and a collection of dynamic-attribute-based rules (Malek B., & Kuhn, 2010). The static attributes have some relatively fixed nature in an access control system for instance: company-address, employee-id, employee-name, and so on. The dynamic attributes are those attributes that change over time i.e. with greater variation in an access control system like: time-of-day, employee-age, and so on (Ting, 2015).

Attribute based access control (ABAC), is an improvement over RBAC due to its flexibility and form of access control due to its policy-neutral nature (that is, ability to express different kinds of access control policies including DAC, MAC and RBAC) and dynamic decision making capabilities. Despite all these advantages, ABAC is difficult to manage compare with other access control models. In making authorization request entails assigning some attributes to the entities required for the access. It must ensure that the right attributes to entities are assigned to the right people in other to protect the system or object to unauthorized access. Hence, configuring constraints specification and enforcement mechanism require an organization to come up with attributes assignment policies.

The ABAC is more complex in constraint specification compare with other access control models such as RBAC because of the many attributes. Constraints can involve between various values of a set-valued attribute (e.g. mutual exclusion on group memberships) and also on values across different attributes. Let take this example for an organization that want only their vice-president to be carried along with the top-secret clearance and membership in their board-members email group. To specify the constraints for the requirements of this organization in ABAC system; there will be three attributes namely role, clearance and group for each user in other to establish this concept. If the user's role attribute is not 'vice-president', hence, the user's clearance and group attributes cannot be assigned the value of 'top-secret' and 'board-member-emails' respectively. It should be seen in these constraints that their priority is on users' access to objects directly rather the attention is on high-level details a security expert would specify to enable or disable a user access to the information.

In a nutshell, if a model contains too much detail it will be very difficult to execute different security indices. From this research it is very glaring that the safety problem of an ABAC system with infinite value domain of attributes cannot be ascertained (Xinwen et al, 2015 & Khalid, 2015). It was also discovered in the course of the literature reviewed that what attributes should be are not stated in any policy whether they should be static or dynamic attributes.

Despite the shortcoming identified in ABAC model, it overcomes all the weakness in DAC (Ravi et al, 1994), MAC (Ravi, 1993) and RBAC (Xin et al, 2012). NIST stated that out of the entire existing access control models. ABAC system is suitable for large enterprises because it has to some extent a form of flexibility and security robustness (Vincent et al, 2013). In spite of the complexity of ABAC to analyze constraints specification on attribute values; it was discovered that in utilizing ABAC model it enhances high-level access control requirements in the system. The diagram for Attribute Based Access Control (ABAC) is presented in figure 3.

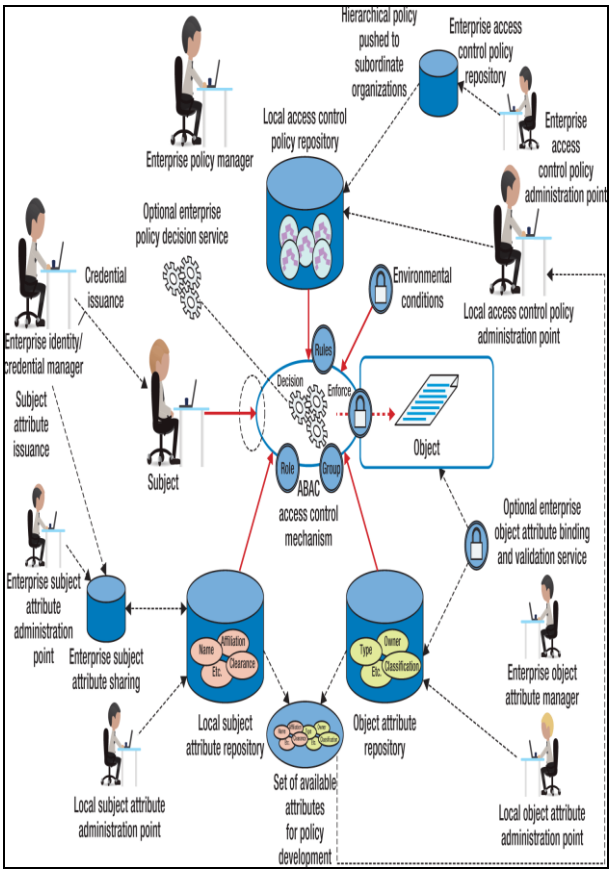

Figure 3: ABAC Database Architecture (adapted from Vincent et al, 2015)

7) History-Based Access Control (HBAC)

It is a subject to object model, the data object are granted access based on the action and request history of the subjects. In HBAC policies, a subject's request is decided based on what actions and action-requests the subject had performed before. In this context, the main motivation is to differentiate the "goodness" of subjects based on their past behaviours. This can be captured in the transactions data of the model (Anindya et al, 2005).

8) Relationship-Based Access Control (ReBAC)

ReBAC has policies that made used of regular expression-based path patterns of relationship types between graph entities such as subjects and objects for finer-grained and more expressive access control on online social networks (Anindya, 2014). The relationship pattern can be based on regular expression-based path patterns to capture the causality dependency relations between graph entities or the type of co-existence between subject-to-subject, subject-to-object, or object-to-object (Yuan et al, 2012 & Jaehong et al, 2011).

9) ***Usage Control (UCON)***

This is another approach that can have great benefit from provenance information (Jaehong et al, 2004). UCON performance is affected by the knowledge of all influencing activities of the involved party on a particular resource which can provide additional utility in pre, on-going, and post obligations and authorizations models. Data dissemination in a distributed-systems environment is another study that focuses on usage control that benefit from the information provided by provenance data (Florian et al, 2012).

10) ***Intranet Role Based Access Control (I-RBAC)***

In RBAC, the software agent in internet model differentiates between the local role and the global role hierarchies of the Intranet. This demarcation was done in such a way that the local severs hosted only the local network objects. And the global network objects are made public that is it known throughout the Intranet. There is database that stores the mapping information existing between the global and local roles which will be used when a global network object needs to access an object on another server. There is information inconsistency in I-RBAC as the number of roles increases (Martin et al, 2003).

11) ***Context-Based Access Control (CBAC)***

CBAC is a diversification of RBAC in access are allowed by taking into consideration the context of the person making request, the object requested for, the systems and the environment. The context entails user context which includes time, Location, schedule and so on, system context has to do with system state, network bandwidth, hardware, software and environmental context take care of the temperature, humidity, GIS and so on. CBAC limited user request to the present access time in context (Le X., 2005).

12) ***Trust-Based Access Control (TBAC)***

TBAC is a model used in a dynamic environment like ubiquitous computing where trust is very important because of the sensitivity of the information involved. It necessary a pre-defined knowledge of who should access such data is kept in an access control list (ACL). Once a request is made by the user the list will be checked as a form of authenticating the user. A good example can be found in electronic medical record (EMR) where the record of patient will be shared with users like licenced doctors, nurse and other medical personal based on trust and also to give good medical attention to the patient. Due to the sensitive nature of the medical information the trust level must be based on the extent to which the user can go before the disclosure of the patient's record (Le X., 2005).

Other types of access control models that have been proposed in history include Workflow Model (WFMs), Agent-Based Approach (ABA), Certificate Based Approach (CBA), and Hypertext Based Authorizations (HBA). One common characteristic among these models is that they use one parameter or the other to control access using different algorithms.

C. Related Work

Le Xuan Hung, (2005), was a PhD Fellow in u-Security Research Group, his research was based on Research Taxonomy he carried out in ubiquitous computing security. Various security tools were identified but his research was focused on access control most especially the trust and risk assessment. In the paper his research description and research milestone was covered.

Leonard, (2005), the chief scientist of the Advanced Research Project Agency (ARPA), conducted a research on 'A Vision for the Internet'. He foresaw the great advantage computer networks would have in the future and this will make computing to be used as a utility. He also concluded that the future computing will be available to all, visible, ubiquitous, cheap and so on. The rapid discovery in chip technology and networked computing environments have transformed computing to a model consisting of services that can be commoditized and delivered in a manner similar to utilities such as water, electricity, gas, and telephony (Buyya et al, 2001). Many computing paradigms such as the Web, Data Centers, Web Services, Grid Computing, P2P Computing and Cloud Computing have emerged to support IT service (Buyya et al, 2009) as referenced by (Saurabh, 2010).

Another researcher Shefail, (2005), 'A fine grain Role Based Access Control Framework'; The research was able to include a feature that can securely handle large number of users, able to provide a secured authorization and authentication to users and also managed database easily with Eucalyptus paradigm of role and access management among the domain which is used to generate an agreed simple and understandable language for information exchange and role specification. The challenge here is that space required and utilization may double and challenges of maintaining generations of backed up data may be overwhelming.

Kuyoro et al (2011), in their paper 'Cloud Computing Security and Challenges'; was able to review the cloud technology in general term and also presented a detailed analysis of the cloud computing

security issues and challenges focusing on the cloud computing types and the service delivery types. The current challenges associated with the cloud computing was identified. However most of the security issues raised in this paper had been addressed adequately but not yet resolved. The paper reviewed the key security issues faced in the cloud computing and the potential of becoming the best secure, virtual and economically viable IT solution in the future.

Also Safwan, (2013) in the dissertation Decentralizing Trust: New Security Paradigms for Cloud computing stated that, data computation integrity and security are one of the major challenges to be combated for cloud users. The study enables us to see the high level of data mistrust which has caused loss of confidence in today's cloud centralization and universal trust in all cloud's nodes rendering the clouds vulnerable to attacks. In order to resolve this anomaly the dissertation used five new paradigm (Hatman, Hadoop, Anonymous Cloud, Penny and Cloud cover) for decentralizing cloud trust relationship to ensure a robust cloud security, computation integrity, confidentiality labeling of data, ownership privacy, efficient validation, enforcement of security policy and data integrity. There was a future consideration for a congestion control mechanism to reduce the computational overhead of long tor circuits and cover traffic defense against end-to-end timing attacks. Also a greater transparency of internal cloud resources is recommended as a means of generating greater consumer confidence in cloud systems like smartphones.

However, in the same year, Parminder et al, (2013) in their paper Cross Bread Role based Access Control For Extended Security At Azure in Cloud Computing, introduced "A New Advanced RBAC Architecture" system which is a form of ontological concept that can keep record of backup of the data send to the cloud server and to put a restriction on the user per role. The ordinary RBAC model do not place any restriction on the number of users per role which their work addressed, the existing system send data directly to the cloud without any backup which can lead to data security threat in case the data got lost. Hence, the new ontology based RBAC is a conceptualization of structure in terms of relationship and the advantage of these new features is to enhance the security on cloud computing and to also prevent data loss. The new architecture discussed in this work has a limitation because of the restriction place on the number of roles per user.

Xin Jin, (2014), conducted a thorough research on attribute based access control and the implementation in cloud Infrastructure as a Service models which was based on the existing traditional model and the flaw of RBAC not able to keep the roles as it increases on the cloud. This weakness was the strength behind ABAC model. The research was carried out in three stages, to harmonize the features of DAC, MAC and RBAC for ABAC (1) to configure them naturally. Secondly, a new model was developed based on ABAC (1) to be able to handle the advanced feature of the existing RBAC and the Extension of RBAC where roles are replaced with attribute and constraints. Lastly, an administrative model was design to manage user attribute using administrative roles. The administrative model design is called generalized use-role assignment model (GURA). The model is weak in the sense that there should be an automatic update for Attribute selection when the membership rules for activated roles are not satisfied but such provision is not available in the existing ABAC. Also another problem envisaged is the integrity of the values of the attribute assigned by the users and third party.

In the same vein, Alshehri Suhair(2014), in his work on 'Toward Effective Access Control using Attributes and Pseudo roles. The dissertation was designed and developed to handle a secure access system using Cipher text Policy Based encryption (CP-ABE). This was design and validated in two-step access control approach, the Bilayer Access Control (BLAC) model. The first layer in BLAC checks whether subjects making access requests have the right BLAC pseudo-roles. If requesting subjects hold the right pseudo-roles, the second layer check rules(s) within associated BLAC policies for further constraints on access. BLAC thus makes use of attributes effectively while preserving RBAC's advantages. The critical issue noted in this research is the privacy preservation right; since various attributes are used in making access requests and policies may reveal private information of the user. In BLAC model, attributes of requested object and the requester are sent to the Access Decision Engine which is hosted by a provider in a remote server. Also the access policies are equally stored in a remote server. Therefore, the BLAC model is vulnerable to threats.

1) Research Gap

From the reviewed works, the research gaps that exist and the various approaches that have been used by many researchers to develop efficient access control models in literatures include the following;

Parminder et al (2013), tried to solve the role explosion problem in RBAC but the new architecture has a limitation because of the restriction placed on the number of roles per user in which scalability may be difficult to achieve.

Xin Jin(2014), opined that the ABAC models are weak because there should be an automatic update for Attribute selection when the membership rules for activated roles are not satisfied but such provision is not available in the existing ABAC; hence the integrity of the values of the attribute assigned by the users and third party might be tampered with.

In Alshehri Suhair(2014), critical issue noted in this research is that the privacy of the users cannot be guaranteed. The attributes of the object requested and the users are sent directly to the remote server. Also the access policies are equally stored in a remote server. Therefore, the model is vulnerable to threats.

III. COMPARISON OF SOME ACCESS CONROL MODELS

Table 1 shows some of the characteristics that exist among the access control models. This is based on some access control factors that indicate the functionality and economic values in a model used in access control as security requirement to test the performance of any model based on the features. The factors can be categorised as general confidentiality, Integrity, availability, flexibility, granularity and scalability. While others fall into the categories of non-general features but has been used by other researchers in literature.

Confidentiality: the security of a model is measured by its level of supports for privacy of data and users;

information must be made available to only the authorised users. It must avoid improper access to information. Only the authorised users have the right to read information.

Integrity: as one of the security requirement, a good model must be able to protect information from being altered by unauthorised users. Only the authorised users have the permission right to write a data or information.

Availability: one of the determinants of good access control is that the information must be available when the need arises

Flexibility: a good access control must permit a little modification such as deletion and insertion of the values or complete update on the application environment. The access control model must be able to synchronise with any change in security conditions, continuous change of users and other environmental challenges and must able to change access control policies.

Granularity: in access control, granularity is of two types; fines-grained and coarse-grained. The fine-grained granularity allows access control to have different roles for a specified data accesses and provide a fine-grained reference to the subjects and objects. While coarse-grained allow group of users and collections of objects to share the access control resources.

Scalability: has to do with increment in the number of users. Therefore if the number of users granted permission to access resources or data increase, the storage server must still work effectively. The performance of good access control model must not diminish with increase in
the number of users (Romuald, 2008, Ghani et al, 2012, Mohammed et al, 2001, Sahafizadeh et al 2010).

From table one, the comparison of the characteristics is done using reviews from literature. DAC was seen to be very poor in scalability, role assignment and granularity. It can also been seen that when considering confidentiality and integrity, MAC will serve a good purpose. RBAC and its' variants has a good strength in all the characteristics except that it has weakness in confidentiality, integrity and efficiency. ABAC has been evaluated to be very good in many of the characteristics but it is weak in confidentiality, integrity and it is also very complex.

TABLE 1: COMPARISON OF ACCESS CONTROL MODELS ADAPTED FROM (CHIRAG ET AL, 2015).

F- Fair, C- Complex, P- Poor, G- Good, V.G- Very Good, N.M- Not Mentioned, N- None

Access control	Availability	Confidentiality	Scalability	Integrity	User conveniences	Performance	Re-Usability	Role Assignment	Granularity	Authentication	Efficiency
DAC	F	F	P	F	F	F	F	P	P	F	F
MAC	F	G	F	G	F	F	F	F	F	F	F
RBAC	G	F	G	F	G	G	G	G	G	G	F
ABAC	V.G	F	V.G	F	C	V.G	V.G	V.G	V.G	G	G
MaTAC	F	P	P	P	F	F	F	N	F	F	F
RUBAC	P	P	F	P	F	F	P	F	F	F	F
CBAC	F	F	G	F	G	F	G	N.M	F	F	F
ReBAC	F	F	F	G	F	F	F	F	F	G	F
HBAC	P	P	F	G	F	F	F	F	F	G	F
IBAC	F	F	G	F	F	F	G	F	F	F	F
TBAC	F	F	G	F	F	F	F	F	F	G	F

From the foregoing, it can be seen that both RBAC and ABAC are very weak in confidentiality and integrity. Specifically, more research effort is required in the area of integrity and confidentiality in ABAC. In addition the problem of complexity in ABAC needed to be given adequate research effort by the research community in order to find an easy to implement ABAC model.

In view of these, it has been observed that the existing models have flaws and based on the analysis of these problems, a Symbolic Attribute Based Access Control (SABAC) is proposed as an improvement to ABAC. In SABAC, symbols shall be used to represent attributes at remote servers thereby solving the problem of confidentiality and integrity as observed in ABAC.

IV. CONCLUSION

The importance of developments in cloud computing cannot be overemphasized. It is the future of internet applications. Cloud computing though in its early development, will advance and become a common place infrastructure while other related technology that will make life more easier will spring up. Security issues that come with wide usage and acceptability of cloud computing is enormous while traditional and legacy access control methods may not work. The access control methods reviewed in this work need modification to be suitable for future cloud computing. Both RBAC and ABAC need a reengineering to be able to secure access to future cloud resources. Hence further works shall be done to modify ABAC to improve its confidentiality and integrity for cloud computing as it gains wider acceptance and usage. To this end we propose Symbolic Attribute Based Access Control (SABAC). This is a work in progress; other results shall be published later.

REFERENCES

[1] Zhenji Zhou1, Lifa Wu2 and Zheng Hong3 Institute of Command Information System, PLA University of science and technology Nanjing, Jiangsu, China 1zhou_zhenji@163.com, 2wulifa@vip.163.com, 3hongzhengjs@139.com, International Journal of Grid and Distributed Computing, Vol.6, No.6 (2013).

[2] Habib, S.M. Ries and S. Muhlhauser,"Cloud Computing Landscape and Research Challenges Regarding Trust and Reputation" in Ubiquitous Intelligence & Computing and 7th International Conference on Autonomic & Trusted Computing (UIC/ATC), Oct. 2010, pp. 410-444.

[3] Halton G., Deepak S., (2009), "Cloud Computing Essay", [Accessed 12-04-2010]: http://www.scribd.com/doc/23743963/Cloud-Computing-Essay

[4] Ali Asghary Karahroudy, Security Analysis and Framework of Cloud Computing with Parity-Based Partially Distributed File System, July 2011.

[5] Bokefode Jayant. D., Ubale Swapnaja A., Modani Dattatray G. and Lavel Chiplun Mumbai. Analysis of DAC MAC RBAC Access Control based Models for Security, Sinhgad College of Engineering, korti, Pandharpur, Solapur University,INDIA. International Journal of Computer Applications (0975 – 8887) Volume 104 – No.5, October 2014.

[6] Margaret Rouse, March 2013; http://searchsecurity.techtarget.com/definition/access-control Le Xuan Hung, (2005), Research Taxonomy, u-Security Research Group, lxhung@oslab.khu.ac.kr

[7] Abhishek Majumder, Suyel Namasudra and Samir Nath, (2014), Taxonomy and Classification of Access Control Models for Cloud Environemnts, Depatrment of computer

Science & Engineering , Tripura Univeristy, suryamaninagar, Tripura West, India.

[8] Majumder Abhishek, Suyel Namasudra and Samir Nathl, (2012), Taxonomy and Classification of Access Control Models for Cloud Environments. Department of Computer Science & Engineering, Tripura University, Suryamaninagar, TripuraWest, Tripura, India.

[9] Lampson, B.W., "Dynamic Protection Structures," AFIPS Conference Proceedings, 35, 1969, pp.27-38

[10] Bell, D.E., and L.J.LaPadula, Secure Computer Systems: Mathematical Foundations and Models, Bedford, MA: The Mitre Corproration, 1973future Computer and communication , Wuhan, China.

[11] Punithasurya K., Jeba Priya S.;"Analysis of diffenrent Access Control Mechanism in cloud" International Journal of applied Information systems, Vol. 4, September 2012

[12] James B. D. Joshi, Walid G. Aref, and Eugene H. Spafford, Security Models Web-Based Application. Proceeding of Communication of ACN, February 2001/Vol. 44 no.2.

[13]Sandhu, R. Lattice-based Access Control models. IEEE Computer 26. 11 (1993).Proceeding of the Fifth ACM Workshop on Role-based Access Control, Berlin, Germany, July, 2000.

[14] Ferraiolo, D.F., Barkley, J.F., and Kuhn, D.R., A role-based Access Control model and reference implementation within a corporate intranet. ACM Trans. Info Syst. Security 2,1(Feb. 1999), 34-64Gil P., (2010), "What is Cloud Computing", [Accessed 01-22-2011]: http://netforbeginners.about.com/od/c/f/cloudcomputing.htm

[15] Tari, Z., and Chan, S. A role-based access control for intranet security. IEEE Internet Computing (Sept-Oct. 1997)

[16] Parminder Singh1, Sarpreet Singh2, Cross Bread Role based Access Control for Extended Security At Azure in Cloud Computing, International Journal of Application or Innovation in Engineering & Management (IJAIEM) Volume 2, Issue 2, February 2013 ISSN 2319 - 4847 Volume 2, Issue 2, February 2013 Page 206. Web Site: www.ijaiem.org Email: editor@ijaiem.org, editorijaiem@gmail.com OASIS, Extensible access control markup language (XACML), v2.0 (2005).

[17] Vincent C. Hu, David F. Ferraiolo, and et al. Guide to Attribute Based Access Control (ABAC) Definitions and Considerations. NIST Special Publications 800-162, Jan. 2014.

[18] Xin Jin, Ram Krishnan, and Ravi Sandhu. A unified attribute-based access control model covering dac, mac and rbac. In Proceedings of the 26th Annual IFIP WG 11.3 conference on Data and Applications Security and Privacy, DBSec'12, pages 41–55, Berlin, Heidelberg, 2012. Springer-Verlag.

[19] Xin Jin, Ram Krishnan, and Ravi Sandhu. Reachability Analysis for Role-based Administration of Attributes. In Proceedings of the 2013 ACM Workshop on Digital dentity Management, DIM '13, pages 73–84, New York, NY, USA, 2013. ACM. of Texas At San Antonio, College of Sciences, Department Computer Science.

[20] B. Malek and A. Miri, "Combining Attribute-Based and Access System", Proceedings of the 12th IEEE International Conference on Computational Science and Engineering, (2009), pp. 305-312.

[21] D. R. Kuhn, E. J. Coyne and T. R. Weil, "Adding attributes to role-based access control", Computer, vol. 6, (2010), pp. 79-81

[22] Ting Cai, Jian Zheng and Xing Du(2015) , A Hybrid Attribute based RBAC Model College of Mobile Telecommunications, Chongqing University of Posts and Telecommunications, Chongqing, China, International Journal of Security and Its Applications Vol.9, No.7, pp.317-328

[23] Xinwen Zhang, Ravi Sandhu, and Francesco Parisi-Presicce. Safety analysis of usage control authorization models. In Proc. of the ASIACCS, 2006 [17] Martin Abadi and Cedric Fournet. Access control based on execution history. In Proceedings of the 10th Annual Network and Distributed System Security Symposium, pages 107–121,2003.

[24] Khalid Zaman Bijon(2015), Constraints For Attribute Based Access Control With Application Incloud Iaas, College of Sciences , Department of Computer Science, The University of Texas at San Antonio.

[25] Ravi S Sandhu and Pierangela Samarati. Access control: Principle and practice. Communications Magazine, IEEE, 32(9):40–48, 1994.

[26] Ravi S. Sandhu. Lattice-based access control models. IEEE Computer, 26(11), 1993.

[27] Xin Jin, Ram Krishnan, and Ravi Sandhu. A Unified Attribute-Based Access ControlModelCovering DAC, MAC and RBAC. In DBSec, 2012.

[28] Vincent C. Hu et al. Guide to attribute based access control (ABAC) definition and considerations(draft). NIST Special Publication, 2013.

[29] Anindya Banerjee and David A. Naumann. History-based access control and secure information flow. In Construction and Analysis of Safe, Secure, and Interoperable Smart Devices, 117 International Workshop (CASSIS 2004), Revised Selected Papers, volume 3362 of Lecture Notes in Computer Science, pages 27–48. ((Springer-Verlag, Anindya 2005

[30] Anindya. Access Control for Online Social Networks Using Relationship Type Patterns. PhD thesis, University of Texas at San Antonio, San Antonio, TX, USA, 2014.

[31] Chirag Langaliya and Rajanikanth Aluvalu,(2015), Enhancing Cloud Security through Access Control Models: A Survey, Department of C.E School of Engineering, R.K. University, Rajkot. International Journal of Computer Applications (0975 – 8887) Volume 112 – No. 7.

[32] Yuan Cheng, Jaehong Park, and Ravi Sandhu. Relationship-based access control for online social networks: Beyond user-to-user relationships. In PASSAT 2012, pages 646–655. IEEE, 2012. Amazon Web Services. http://aws.amazon.com

[33] Jaehong Park, Ravi Sandhu, and Yuan Cheng. ACON: Activity-centric access control for social computing. In 2011 Sixth International Conference on Availability, Reliability and Security (ARES), pages 242–247. IEEE, 2011.

[34] Jaehong Park and Ravi Sandhu. The UCONABC usage control model. ACM Trans. Inf. Syst. Secur., 7(1):128–174, Feb. 2004.

[35] Florian Kelbert and Alexander Pretschner. Towards a Policy Enforcement Infrastructure for Distributed Usage Control. In Proceedings of the 17th ACM Symposium on Access Control Models and Technologies, SACMAT '12, pages 119–122, New York, NY, USA, 2012. ACM.

[36] Martin Abadi and Cedric Fournet. Access control based on execution history. In Proceedings of the 10th Annual Network and Distributed System Security Symposium, pages 107–121,2003.

[37] Romuald Thion(2008), Access Control Models, University of Lyon, France.

[38] Ghani, N.A.; Selamat, H.; Sidek, Z.M. (2012, Analysis of Existing Privacy-Aware control Access for e-commerce application. Glob. J. Comput. Sci. Technology Vol 12, page 1-5.

[39] Mohammad, A.; Khdour, T.; Kanaan G.; Kanaan, R.; Ahmad, S.B.(2011), Analysis of existing Access Control Models from Web services Applications Perspective. J. Computing Vol 3 pg 10-16.

[40] Oyeyinka, F.I., Prof., Omotosho O.J., Dr.Oyeyinka I.K.(2015), A Modified Things Role Based Access Control Model for Securing Utilities in Cloud Computing, International Journal of Innovative Research in Information Security (IJIRIS) ISSN: 2349-7017, Issue 2, Volume 5 (May 2015).

[41] Sahafizadeh, E.; Parsa, S. (2010), Survey on Access Control Models. In Proceedings of 2nd International Conference
[42] Xin Jin, (2014), Attribute-Based Access Control Models and implementation in Cloud Infrastructure as a Service, The University.
[43] Vincent C. Hu , D. Richard Kuhn and David F. Ferraiolo(2015), Attribute-Based Access Control, National Institute of Standards and Technology, CSDL 2015 vol. 48 Issue No. 02 - Feb. ISSN: 0018-9162, pp: 85-88. http://doi.ieeecomputersociety.org/10.1109/MC.2015.33.