BULGARIAN ACADEMY OF SCIENCES

CYBERNETICS AND INFORMATION TECHNOLOGIES • Volume **16**, No 1
Sofia • 2016 Print ISSN: 1311-9702; Online ISSN: 1314-4081
DOI: 10.1515/cait-2016-0002

# A Comprehensive Survey and Analysis on Access Control Schemes in Cloud Environment

*P. G. Shynu, K. John Singh*

*School of Information Technology & Engineering, VIT University Vellore, Tamil Nadu, India*
*Emails: pgshynu@vit.ac.in johnsingh.k@vit.ac.in*

***Abstract:*** *Cloud computing has emerged as the most dominant computational paradigm in recent times. There are tremendous benefits for enterprises adopting cloud technologies. It provides resources and services on demand, pay-as-you go basis. This includes infrastructure, platform and software services. But there are still a number of security threats and challenges associated with utilizing cloud computing. A proper access control is the fundamental security requirement in any cloud environment, to avoid unauthorized access to the cloud systems. As cloud computing supports multi-tenancy and has a various categories of users with different sets of security requirements, traditional access control models and policies cannot be used. This paper discusses on various access control models used for cloud environment and presents a detailed requirement analysis for developing an access control, specifically for the cloud. A comprehensive study on various security problems associated with outsourced data on the cloud and their existing solutions are also described, with the future research directions.*

***Keywords:*** *Cloud computing, cloud security, access control in cloud, cloud storage, data privacy.*

## 1. Introduction

Cloud computing is a new promising mode of business computing. It can be called "Computing as Utility", which enables convenient, on-demand network access to a shared pool computing configurable and scalable resources. These resources are provided in a massive and virtualized manner, managed by professional service providers called Cloud Service Providers (CSP). The cloud model simplifies installation, operation and maintenance of information systems. It reduces costs and boosts system reliability and efficiency. Rather than purchasing infrastructures, users can lease these resources and save a great deal of capital. Microsoft, IBM, Google, Amazon, CloudSafe, etc., provide cloud services. Cloud services are measured

services and are characterized as on demand self-services, with broad network access, rapid elasticity and pooled resources for sharing. The resources that are being shared can be applications, hardware and system software as various services.

Based on *who provides* these services, there are four ***cloud delivery models*** namely, *private cloud, public cloud, community cloud* and *hybrid cloud*. If cloud services are provided solely for an organization, which are managed by the organization or an authorized third party, it is known as a *private cloud*. *Public cloud* services are available to the general public and offers storage, applications and other resources, for example, Amazon cloud service. *Community cloud* services are shared by several organizations for supporting a specific community. These services may be managed by the organizations or a third party. A *hybrid cloud* is a combination of different cloud computing infrastructures (public, private or community).

Similarly, based on what all services are offered, the National Institute of Standards and Technology (NIST) [1] has identified three basic ***cloud service models***: (i) *Software as a Service* (*SaaS*) which offers renting application and functionality from a service (ii) *Platform as a Service (PaaS)* provides a development and execution environment by which applications can be developed and executed. (iii) *Infrastructure as a Service* (*IaaS*) offer computing power and storage space on demand by the vendors.

Many security and privacy vulnerabilities in accessibility, virtualization and web application are discussed in [2, pp. 1-9]. Data storage security, security of data in transmission, security of the application and security and trust related to third party resources are some of the fundamental challenges in the Cloud environment. It also identifies some obstacles in the adoption of cloud by the customers such as availability of service, confidentiality and auditability of data, unpredictability in performance, scalable storage, data lock-in, and bugs in large distributed systems and software licensing. In [3], the issues of control, latency, reliability, bandwidth costs, transparency and standards are also been discussed.

Conventional security attacks in the distributed environment are also applicable in cloud, such as malicious code (Viruses, Trojan Horses), Man-in-the Middle attack, back door, distributed Denial-Of-Service (DOS) attack [3], insecure APIs, abuse and nefarious use of cloud computing and malicious insiders [4]. Due to these attacks, cloud services could be inaccessible which generates a negative impact. Availability, integrity and reliability are also important in cloud services [2]. It is also noted that cloud computing has brought new concerns such as moving resources and storing data in the cloud which reside in another country, having different regulations. When different CSPs use various technologies, the complications may increase, like potential heterogeneity issues [5]**.** Virtualization related security issues [6] in cloud are also a major research topic.

Among the various issues and challenges, *security and privacy of outsourced data* are to be considered seriously, as they are the two main factors of user's concerns in the cloud adoption. As per a recent survey [7] conducted by IDC Enterprise Panel on cloud services, 87.5% of the participants were worried about the security and privacy of their data on the public cloud, which is owned by others and supporting many users (multi-tenancy).

Appropriate access control mechanisms should be adopted to secure data in the service oriented cloud model. The information in the cloud is being shared among different entities with varying degrees of sensitivity. Our in-depth investigations on cloud security revealed the fact that an efficient, robust, precise, flexible and fine grained access control is one of the fundamental requirements to ensure the security, confidentiality and privacy of user's data, which is quite challenging too.

Most of the traditional access control models are not suitable for cloud environment. They lack flexibility in managing the attributes and also have scalability issues. Conventional methods fail to support the dynamic and sophisticated nature of cloud environment, dealing with large number of users in the cloud [3]. Resource sharing among untrusted cloud tenants, in the multi-tenant, heterogeneous, virtualized cloud environment with an access control policy is always a challenge. Extending an existing conventional access control policy, for the cloud may not be suitable as conventional models are specific to a problem, targeted for a particular platform.

In this paper, we have performed a detailed investigation and analysed various conventional access control models and their limitations to use in the cloud. The fundamental requirements for developing an access control scheme, suitable for the cloud are also identified, which have not yet been adequately investigated.

The layout of the paper is as follows. Section 2 describes various traditional access control models and their short comings. Next Section 3 describes various requirements that are to be addressed for developing an access control model for the cloud. In Section 4, a comprehensive study on various problems associated with outsourced data on the cloud and the current proposed solutions are described. Attribute Based Encryption, a promising access control scheme for the cloud is briefly described in the Section 5. This is followed by a discussion on future research directions and conclusions, in Section 6.

## 2. Access control in cloud

A group of rules and procedures that would help and enable legitimate users authorization to various data access [8]. The cloud computing security possesses various control based compliances in order to safeguard information within the cloud computing users. The fundamental goal of any access control system is restricting a user to exactly what he should be able to do and protect information from unauthorized access. There is a wide variety of methods, models, technologies and administrative capabilities used to propose and design access control systems. Thus, each access control system has its own attributes, methods and functions, which derive from either a policy or a set of policies.

The very basic nature of cloud such as on-demand and shared services and mobility makes its access control, an area of particular concern. Thus, cloud service providers need a strengthened access control system for controlling admission to their resources with the ability to monitor precisely who accesses them. They should have the ability to deal with dynamic and random behaviour of cloud consumers, heterogeneity and diversity of services. Thus, each access control system undergoes

a varied designing and methodology developed to suit the rational behavior of the users.

This segment presents a brief overview on various traditional access control schemes. It also exposes the need for improved access control mechanism specifically for the cloud.

## 2.1. The need for an improved access control schemes for cloud

Earlier user security needs were developed to match a specific environment. As a result of this disparity, there Evolved two access control models, called Discretionary Access Control (DAC) and Mandatory Access Control (MAC) [9]. These traditional models were used in military and commercial security. They have their own advantages but they do not provide a favorable paradigmatic for cloud computing and these flaws led to the proposal of other models such as Role-Based Access Control (RBAC) specifically designed to suit the cloud environment.

### 2.1.1. Mandatory access control model

In Mandatory Access Control (MAC) model, only the administrator can determine and manage the access controls. He can decide and define the access policy which cannot be altered by any other users. In the MAC model, the administrator assigns different security labels to the subject and object. These security labels help to protect the flow of information from the higher secure level to the lowest [10]. This Model is known for its multilevel security system. The main area of focus in MAC model relates to protecting and controlling the data flows. This model overlooked many other facts which led to the development of a more improved model by [11], which aimed at focusing on the integrity of the objects.

Despite the development and improvisations done on a MAC model, both the abovementioned models could not assure complete confidentiality. Indeed MAC Models are very overpriced and complicated at the deployment stage and does not back separation of duties, minimal privilege, and delegation or inheritance principles. These models require clear cut frameworks for handling various system units that are present either externally or internally. They also lack in identifying the zone factors and also do not support vital and immediate functioning of access privileges for particulars task. Most of the credible units that MAC models uses may have to violate the MAC principles, which has made its existence as an alien in the whole system. As per [8], the creation or destruction of subjects or objects is yet not handled by the Bell-LaPadula model (BLP) specified by [10]. Most of the job execution may not be smooth due to rigid security titles and need for a pivotal control to decide on the access rights. For example, the credit card department of a bank wants to know the details about a client, but their access rights shall be limited only to certain information’s and not all the information about the customer that are confidential to the banking department. The need for use of present web applications for cloud computing has in its turn caused the MAC model to handle intricate and complex semantic models which denotes rights and restriction that are included in the access control policies.

### 2.1.2. Discretionary access control model

In Discretionary Access Control (DAS) model, the owner of the objects determine the permission rights on the objects or data that needs to be accessed based on the membership in a particular group or users identities. When compared to MAC model, the DAC model cannot be used in areas which need higher level of security. The commercial operating systems like UNIX and Window based platforms make use of DAC model, as this model is very flexible and simple to use [12]. The discretionary access control can be put into use either by using the identity-based access control or by means of access control matrix – Access Control List (ACL) or capabilities [13].

As far as the usage of DAC model in cloud computing is concerned, this model has to face a lot of challenges such as the absence of a proper methodology to handle improper rights, which the user gets from the owners, access permissions. This model also entitles the user to share vital information about objects to outsiders as certain access rights can be misused and leaked. The DAC model does not safeguard the secrecy and integrity of objects as the user can handover their rights to another parties. The DAC model does not restrict the flow of information or handle any viruses which can indirectly possess the access permission [14]. The DAC model's inability to maintain privacy and various access permission policies proves it as a non-viable model for cloud computing.

### 2.1.3. Role based access control model

The role based model is a normal way to control access as this model works on the basis such that the responsibility of the subject is more vital that what the subject is [9, 15]. Role Based Access Control (RBAC) model provides the flexibility to a subject that it can have multiple roles or membership in multiple groups. In this model the roles are predetermined to the task which is based on the access permissions. This model works on the workflow authorization model in order to combine and blend workflow with authorization flow. Further to this, RBAC model paved way for the development of another model called Task Role Based Access Control (T-RBAC) [16]. This model makes use of active access control for task and passive control to define the roles.

As whole, the RBAC model proved to be superior than DAC and MAC model [17] but in spite of the various advantages the RBAC model possess, the task of determining the definite role featuring a system and categorizing the subject based on these roles, make this model hurdle some. In order to access the system, each subject is assigned a role, as the basic functioning of the RBAC model involves categorizing the subject in to numerous categories. The RBAC model can invite violation of access policy as multiple roles (e.g., an employee in an organization can belong to groups in the same organization) can cause threat of higher rights being shared and misused, which can result in the user enjoying more privileges than actual.

The RBAC model faces many challenges such as:

a. This model fails to work on the Principle of delegation in an organization structure at times of absence of a particular employee. It does not take into account

the zone factor, i.e., the time and location factor which enable to limit access permission and hence reducing the chance of security threats.

b. This model does not consider the random and dynamic behavior of users and furthermore do not offer sensitivity to the information.

c. The RBAC model does not support dynamic activation of access rights and cannot separate task form roles.

d. Identities and roles define and decide the relationships between users.

e. The absence of various complex semantic models for communicating with privileges makes RBAC model weak for cloud computing usage.

f. The static test such as testing and verifying the access control functions are highly needed for proper functioning of cloud computing. There also exist various other dynamic compliance functions which can serve as support function [18]. Ensuring the response time and system requirements are vital in cloud computing applications and hence a prior check of the same shall be done before using RBAC model in cloud computing. (e.g., in many applications such as banking system, health care etc. the response time is very critical and important with the users).

g. RBAC model cannot be successfully implemented in cloud computing systems where in access to a sequence or series of operations cannot be ascertained. (e.g., Health care system involves a multiple stages of operations).

### 2.1.4. Attribute based access control model

The Attribute Based Access Control (ABAC) model (Fig. 1) mainly depends on group of attributes that are needed to make any access decisions [19]. In ABAC model the attributes can be characterized or used in multiple ways such as role, location or start date of any project for any user which may or may not be connected to each other [20].

Once the attributes are identified, they are treated as discrete values and are matched with the set of values that may or may not be allowed access, based on the policy decisions. These models are also named as Policy Based Access Control (PBAC) or Claims Based Access Control (CBAC).

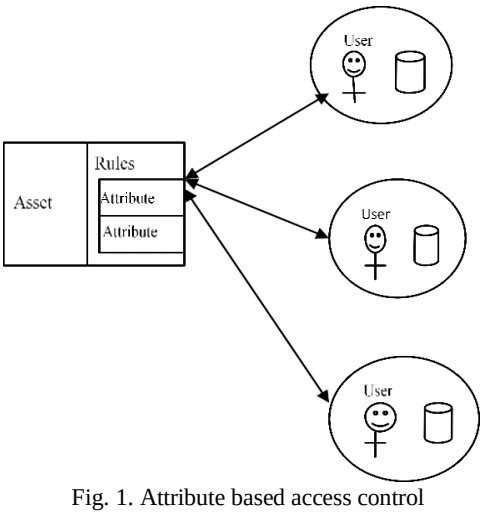


Fig. 1. Attribute based access control

In ABAC model, the system needs not know the subject beforehand. The attributes are provided only once the subjects are identified as genuine by the system. Suggesting a suitable security policy for these models can be very crucial as these policies are in charge of choosing the attributes which are needed to take corrective access decisions. A more detailed study on ABE is given in Section 5.

#### 2.1.5. Risk based access control model

This model evolved to cater to different rules, regulations and policies that tie up any giant organizations [21]. The Risk Based Access Control (RBAC) model works on various levels of risk in accordance with the prevailing situations. The various access decisions are taken on the basis of operational need principle [17]. The security policy in RBAC models are constantly evolving. The security policy in this model keeps changing on the basis of the risk levels. The RBAC models cannot or rather is insufficient for its use in cloud computing due to its vast analysis and the need to combine different number of systems in order to calculate the levels of risk. In order to make a corrective access decision, a proper regulation [17] of different security policies and environment is very vital. Another risk based access control model called, Quantified Risk Adaptive Access Control (QRAAC) was proposed in [22] and the risk is calculated as the product of information value and the unauthorized disclosure probability which denotes the trustworthiness of the cloud user. The information value identifies the level of sensitivity of the resources. These models are very complex and hence expertise person are needed to handle this model.

## 3. Basic requirements for access control schemes in cloud

A detailed analysis has been carried out, in order to identify the basic and important access control requirements for cloud systems and it is described below.

1. *Remote access and authentication with dynamic performance*. Cloud computing should support remote access to its resources and it should be dynamic and scalable. Hence any access control system should possess these characteristics [3]. The major requirement in any cloud based system is the need for a trustworthy authentication system [23]. Once the authentication is completed then only the system can perform its next level. Hence it is very important for any cloud system to build a strong authentication system with various security features. The most vital factors such as time of authentication and login should be considered as these factors also contribute to the successful functioning of the system. It is also very essential to consider various security enhancements such as identity management, mutual authentication, which is combined with authorization mechanisms in the authentication system for cloud users.
2. *Support for heterogeneity and interoperability*. Cloud systems and services are based on diverse technologies, with differences in software and hardware. This causes the heterogeneity issues in the cloud [24] and this requirement must be addressed in designing the access control systems. Different cloud service providers deliver their services with some specialties and as per customer's requirements. They may sometimes collaborate [25] by contributing their resources together. This forces

the access control system to support interoperability, which allows users moving from one service provider to another.

3. *Complexity and response time*. The complexity of the decision making algorithm used in the access control system and its response time are the major factors that influences the quality and efficiency of the service [26].

4. *Trust factor*. The concept of trust relations between the cloud service providers and the users need more improvement in terms of deciding the trusted behaviours of both of them and assessing these behaviours to be taken into consideration [3] in further access decisions.

5. *Scalability*. Another aspect that is to be considered for cloud based access control system is its scalability [27]. The number of users and evaluation of access policies are to be considered for its scalability. Various costs, such as operational, management and maintenance costs are also should be taken into consideration with scalability.

6. *Selection of attributes*. The decisions taken by the access control systems are based on various attributes in the cloud environment. But it is a complex task to arrive at a conclusion on what kind of attributes are to be selected or how many such attributes are to be considered for the decision making [28].

7. *Resource allocation and virtualization*. With regard to recourse allocation in the cloud, virtualization and hypervisors are the major factors and they make access control systems more complex to design [29]. Inferences between the users of the cloud system, improper access control policies and lack of organized user account controls etc. are some of the major challenges in developing an access control system for cloud.

8. *Single sign-on scheme*. It may require using the services from multiple clouds by a cloud user. It is to be noted that these cloud services adopt a variety of access control policies and these policies should have the ability to transfer customer's credential information across layers [29], in order for them to access various resources and services provided in these multiple clouds by a single authentication.

9. *Privileges*. The most vital aspect of cloud computing is to assign or ease privileges which helps in reducing the errors caused due to human or system. The utility of an access control system depends on the steps actually needed for addition, removal and altering privileges or capabilities to a subject [30] and that should be fulfilled in smaller number of steps to minimize the errors.

10. *Audit in access control*. Auditing forms an essential role in cloud computing. The need of audit in access control system is to observe and supervise the present state of the system, capture any unsuccessful decision making, track and note the alterations of privileges [18]. Auditing also had to keep track of any modifications made on the object and capabilities to subject.

11. *Delegation of permission and roles*. The delegation of permission and roles is highly needed [31] where the users need to interact with each other in the cloud surrounding or environment, which in turn increases the flexibility of access control systems.

12. *Flexible configuration and compatibility*. As cloud computing works on the concept of dynamic environment, there is a need for flexibility of configuration in an access control system [30].The concept of virtualization is the basis of cloud computing and the means of service delivery to its users. Thus an access control system in the cloud computing should have the compatibility and capability [18] to work with various operating systems.

13. *Managing policies*. The access control policy management should be able to handle and find suitable solutions for any unforeseen and volatile behaviors [3] Disagreement can be between various policies used in access control system or the policy rules. Hence there is need for policy management in access control system and the absence of the same may lead to violation of data privacy.

14. *Awareness of operations and workflows*. The performance of any access control system depends on a various factors like processors, memory, OS or endpoint system components. Thus there is a need for operational and situational awareness as these might affect the access decisions. The very essential component of cloud computing is the active and passive workflows [32]. Roles can be passive workflow and tasks are active workflow.

15. *Testing and verifying access policy functions*. One of the critical characteristic of access control in cloud computing is testing and verification [18]. This enables the access control system to manage any future policy changes or predict the consequences and impact of activation policies or its modifications. It verifies the impact of the combination of various access control policies and ensures that the privileges are not leaked due to syntactic and semantic errors.

## 4. Current proposed solutions

A role based access control system called RBTBAC (Role Based Time Bound Access Control) model is proposed for electronic health record datasets [33]. Every user has some role, which could be that of a doctor, patient or staff. Depending on the personal details of the user, every role has some privilege. This model is constructed using a hierarchical approach. Also, a time parameter is added with the access control policies for every user. It specifies the time constraint for accessing the records from the cloud for a user with certain role, along with selective privileges. The user can access the records with in this authorized time interval. The advantages of this model are privacy of user data is preserved, prevention of unauthorized attacks by digital signature usage. It also maintains a revocation list for credential by which it prevents the usage of expired credentials. The main difficulty of this system is with key handling as it involves key distribution for different classes which make this model inefficient.

A flexible access control algorithm for cloud environment was recommended by W a n g [3], which work on circumstantial data like security and time. This proposal was based on the role based access control model by linking the trust relationship with the customers. The trust management system revises and modifies the trust levels after each activity. This system functions on the assumption that each cloud holds a global certificate Authority Authorization Centre (AAC) which is in charge

of access control. Even though linking the access control with the calculated trust level, along with the user's behavior modification is an acceptable approach, yet this proposed system can cause certain threats such as trespassing, unawareness of the techniques of granting access and the type of mechanism, probability of single point attack on AAC and the vagueness of the use of RBAC model for granting access to users.

Another suggested model was coRBAC (Cloud optimized RBAC model) by Tianyi, Weidong and Jiaxing [34]. This model incorporates several characteristics of both RBAC and distributed RBAC like dRBAC's domain. The coRBAC model functions in such a manner that each organization has its own internal RBAC and has a single manager role known as D.Manager in it. This model joins the distributed authentication services and provides the capacity to issue certificates to the Certificate Authority. It works by allotting domains which has the competence to handle the users and their roles within their internal network. In order to augment the effectiveness of the access control system, the hierarchical caches have been affixed within the coRBAC model. The high dependence on Certificate authority for the issue of certificates may lead to problems of efficiency and scalability. These problems can affect the functioning of huge organizations with lots of users, as the users need to be issued new certificates for every access. The threat of single point attack on CA and other barriers are also some of the drawbacks of this model. Other drawbacks such as the use of third party domain , the lack of mechanism to deal with diversity created by different security domains, absence of originality in using private roles within internal networks and the lack of information regarding the security domain in the issued certificates.

Yet another scheme known as Task Role Based Access Control (TRBAC) scheme was proposed for health care system in cloud computing by Jayaprakash and Gunes [35]. The permissions in TBAC (Task Based Authorization Control) are activated or deactivated based on the current task or process. Since there is no segregation between the tasks and roles and in order to deal with the separation problem and identify the access control mechanism various factors are used like roles, tasks, workflow, users, information resources and business rules. The synchronization of workflow with authorization in this scheme is done by making uses of workflow authorization flow. This scheme made use of tasks that support active access control and roles, which support passive access control. Even though this scheme was put into use in Amazon Elastic Compute Cloud (Amazon EC2), there lacked the solution to how semantic problems were tackled, how purposeful and relevant were the information that was shared between various hospitals and how the separation problem between roles and task was fixed. Both the T-RBAC model and health care system undergo the problem of heterogeneity for which there has not been solution mentioned in this scheme. This scheme does not take into consideration the sensitivity levels of the information which is highly required in healthcare systems.

A more improvised model was proposed by Sun et al. [36] to authenticate or validate the users of health care systems using the semantic access control scheme. This system is based on ontologies.This scheme puts into use access control system in semantic web environment and makes use of ontologies for RBAC security model.

The RBAC model was lengthened by making use of semantic web technologies. In order to define the relations used in ontologies, this model applied semantic scopes of subjects, objects actions and attributes. This scheme proves a basis for crafting a semantic access control system; however this scheme needs to be put into action and assessed in a workable environment and ability to tackle vast number of users with distinct regulations. This scheme has failed to find a solution to the dynamic activation problems in the RBAC model. There are numerous users, with various types of roles and permissions in health care systems. This makes the migration to a cloud based system, more challenging where the centralization becomes unrealistic by a small group of security administrators. Also, as there are sequences of operations involved in healthcare systems, this model requires to be tested in varied scenes to make sure that right permissions are given for each activities associated with these operations.

T s a i and S h a o [37] proposed a reference Ontology framework based on the Role Based Access Control Model (O-RBAC). This scheme puts forth a suitable policy with a definite role for every tenant. It functions in a manner such that each one subject would possess multiple roles in various sessions and each role hierarchy would be based on domain ontology, which can be transferred between various ontology domains. In order to grant permissions, this scheme makes use of various policies like access policy and security policy. According to the role's characteristics, the policies can be used as components of roles like priority and business values. Despite this scheme is regarded as a good access control model that can be used for cloud computing, it lacks the presence of good ontology transformation operations algorithms for comparing the similarities between various ontology. This scheme demands a more recent back end database scheme in order to back the O-RBAC model. This scheme fails to safeguard the sensitivity levels of information, no backing of the principle of delegation and dynamic activation of access rights for particular tasks. There needs to be a guarantee for granting access decisions within an acceptable or fair time and in accordance with system requirements. Moreover the scalability of O-RBAC model needs to be measured in terms of the number of roles, permissions, hierarchy size of role and role assignment limits of the tenants.

A privacy enhancement system on academic that is based on private cloud system was proposed by M o n and N a i n g [38] which made used of Eucalyptus Open source cloud infrastructure. This was named as Attribute Role Based Access Control (ARBAC). This system is a combination of Role based access control and attribute based access control model. The model aims to ensure privacy of cloud users and security of personal information. As mentioned in the scheme the primary objective is to safeguard data privacy, but does not provide any clarity on how the same shall be achieved. This scheme only refers to the privacy manager who shall be single point, responsible for all privacy related matters and has not defined any other components in the system. Even though, this scheme works on the combination of RBAC and ABAC model, there has not been any evidence on how this combination works and what benefits are being achieved by this combination.

R a and Y u [39] proposed a technique KP-ABE scheme, for flexible, scalable and fine grained access control scheme based on Attribute Based Encryption (ABE).

It also has a re-encryption technique used for user revocation. The computational over head is delegated to the cloud servers. A symmetric Data Encryption Key (DEK) is used to encrypt the data. Corresponding to a set of attributes in KP-ABE, a public key is generated according to an access structure and it encrypts the DEK. The user is then able to decrypt encrypted DEK, if the associated attributes of the file stored in the cloud and access structure of user's key matches, which is used in turn to decrypt the file. This model is not suitable for applications, which requires more sophisticated broadcast encryption. Here users are associated with many attributes and these attributes are linked with a policy associated with the ciphertext. Another problem with this scheme is that the user who encrypt doesn't have any role in deciding who can decrypt his encrypted data. He can only choose descriptive attributes for the data, and has no option but to trust the key issuer.

Hierarchical Attribute-Based Encryption (HABE) is introduced by W a n, L i u and D e n g [40] for fine-grained access control in cloud storage. It combines the Hierarchical Identity-Based Encryption (HIBE) [41] and CP-ABE algorithms. This model delegates the computation to the CSP and ensures fine grained access control. It adopts disjunctive normal form policy and the same domain master controls all attributes in one conjunctive clause. So according to specific policies, the same attribute may be administrated by multiple domain masters. This makes it difficult to implement practically. Moreover, this method doesn't support compound attributes efficiently.

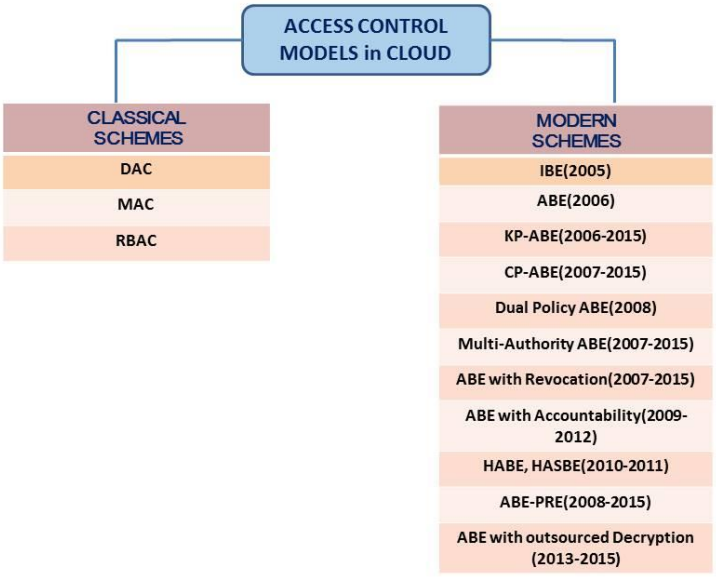


Fig. 2. Various access control models used in cloud

X i n et al. [42] 2014 proposed a privacy preserving access policy for cloud data with semantic security. This model uses the Cipher-text Policy Attribute-Based Encryption (CP-ABE) combined with Identity-Based Encryption (IBE) scheme.

Here, each data file is described by a set of meaningful attributes and it defines a public-private key pair for each of these attributes. User's secret key is computed as a combination public key and the attribute's secret key and thus each attribute presents a different key to each user. Decryption of a ciphertext is possible only if the user have the matched attributes to satisfy the cipher text so that the privacy is ensured. This model is not implemented in the real cloud environment and the computation complexity is high for the encryption as well as decryption. Also for user revocation, the ciphertext needs to be re-encrypted and the user must be online to do so and this is a major obstacle to adopting this model.

A time-based proxy re-encryption known as TimePRE scheme was proposed in 2015 by L i u, W a n g and W u b [43] for the cloud service provider to do the re-encryption, when a user is revoked. An attribute-based access structure and a time of access are associated with each data. A user is identified by a set of attributes and a set of eligible time periods. This denotes the period of validity of the user's access right. After this predetermined period of time, this scheme allows the access right of a user to expire automatically. The problem with the scheme is that we cannot revoke a user from the system at any time, as the time is predetermined.

Recently, L i u and X i o n g [44] suggested a shared authority based authentication protocol called SAPA, which is a privacy preserving access policy for the cloud. To ensure that the cloud user accesses only own data, attribute based approach is adopted and to provide data sharing among different users, a proxy re-encryption scheme is applied. This model supports various security and privacy considerations such as authentication, data anonymity, user privacy, and forward security etc. by anonymous access request matching mechanism which provides the shared access authority. This is only a theoretical model for the authentication and authorization but not tested in the real cloud environment.

A classification of basic access control models used in cloud environment is depicted in Fig. 2. Many variants of these basic schemes are being studied to overcome the limitations of these models. Also brief comparative study on various access control and privacy preserved models proposed currently in cloud environment are depicted in Table 1. The suitability and relevancy of these schemes are also specified.

Table1. Comparison of various access control and privacy preservation models in cloud

| Sr. No | Title | Model used | Advantages | Disadvantages | Application relevancy |
|---|---|---|---|---|---|
| 1 | Security and privacy issues within the cloud computing [3] | Role based access control | A global certificate Authority Authorization Centre (AAC) to enhance the trust of access control for each user. | System can cause certain threats such as trespassing, unawareness of the techniques of granting access and the type of mechanism, probability of single point attack on AAC and the vagueness of the use of RBAC model for granting access to users | Supports users with similar roles |

Table 1 (c o n t i n u e d)

| Sr. No | Title | Model used | Advantages | Disadvantages | Application relevancy |
|---|---|---|---|---|---|
| 2 | RBTBAC: secure access and management of EHR data [33] | Role based time bound access control model | User privacy preserved, prevention of unauthorized attacks by digital signature usage, revocation list for credential to prevent the usage of expired credentials | Key handling is difficult as key distribution for different classes | Roles with time bounded access |
| 3 | An efficient role based access control system for cloud computing [34] | coRBAC (cloud optimized RBAC model) | This model joins the distributed authentication services and provides the capacity to issue certificates to the Certificate Authority (CA) | High dependence on CA for the issue of certificates may lead to problems in efficiency and scalability. Single point attack on CA | With the help of a CA to issue authenti-cation |
| 4 | Ensuring access control in cloud provisioned healthcare systems [35] | Task Role Based Access Control (TRBAC) | Permissions are activated or deactivated based on the current task or process, associates the user with permission indirectly and assigns the permission according to the actual needs | As health care system undergoes the problem of heterogeneity for which there has not been solution mentioned. Lacking a solution to how semantic problems were tackled | Based on current tasks |
| 5 | Semantic access control for cloud computing based on e-healthcare [36] | RBAC security model with on-tologies (O-RBAC) | Semantic relationship of roles considered for fine grained access control | Dynamic activation problems. Fails to safeguard the sensitivity levels of information | Ontology for defining permissions of users. Suitable for large number of users |
| 6 | Towards privacy preserving access control in the cloud [45] | Cloud mask model | Generation of group key and key handling as well as rekeying approach is user-friendly | For a large number of people within a group is impractical. Also change of policies leads to re- encryption | Suitable for small group by generating a group key |
| 7 | Towards privacy-preserving access control with hidden policies, hidden credentials and hidden decisions [46] | Homo-morphic crypto-graphy supported access control model | Anonymity of users is maintained as policies and credentials defined by users are hidden | Computations within the container take a lot of time, anonymity of user makes it difficult to maintain log information | Supports anonymity of users data |

Table 1 (c o n t i n u e d)

| Sr. No | Title | Model used | Advantages | Disadvantages | Application relevancy |
|---|---|---|---|---|---|
| 8 | Privacy aware access control for data sharing in cloud computing [47] | Privacy aware access control model | Flexible access control policy types, scalable as encryption and access control policy part is different, two levels of protection of data, commutative encryption employed and is reliable and easy | Policies defined by the entities is not hidden even though data is hidden | Suitable for preserving the privacy of user data |
| 9 | Achieving an effective, scalable and privacy-preserving data sharing service in cloud computing [42] | CP-ABE combined with Identity-Based Encryp-tion (IBE) scheme | Robust data sharing security, succeeds in preserving the privacy of cloud users, efficient and dynamic user revocation | Not implemented in the real cloud environment, the computation complexity is high for the encryption and decryption, for user revocation, the ciphertext needs to be re-encrypted and the user must be online | Supports users with different attributes organized in single set |
| 10 | Shared authority based privacy-preserving authentication protocol in cloud computing [44] | SAPA – attribute based combined with proxy re-encryption scheme | Fine grained access control. Privacy preserving access policy, data anonymity, forward security | This is only a theoretical model not implemented in real cloud environment | Suitable for privacy preservation of users and data |
| 11 | HASBE: A hierarchical attribute-based solution for flexible and scalable access control in cloud computing [40] | Hierar-chical Identity-Based Encrypti-on (HIBE) and CP-ABE algorithms | Delegates the computation to the CSP and ensures fine grained access control | Difficult to implement in real cloud environments | Supports users with different attributes organized in single set, in hierarchical way |
| 12 | Multi-Authority Attribute Based Encryption (MA-ABE) scheme with revocation [48] | MA-ABE algorithm | Supports fine grained access for multiple users | Computation time and complexity are high | Suitable for users with large computational resource |

## 5. Attribute based encryption model – an efficient way for access control

From our studies on various access control schemes, the Attribute Based Encryption (ABE) is a promising technique for effective, secure and fine-grained access control for the cloud. It is a public key encryption scheme which takes attributes as the public key and ciphertext or secret key are attached to it while encrypting. When compared to other schemes, it provides both data confidentiality and expressive access control. A detailed investigation on the ABE schemes is carried out and given in this section.

In 2005 a new Identity Based Encryption called Fuzzy Identity Based Encryption (FIBE) [4] was proposed, in which identities are represented as a set of descriptive attributes. This model can be considered as the basic concept of Attribute Based Encryption. Later Nali, Adams and Miri [50] introduced a threshold ABE scheme, which can prevent collusion attacks but its threshold semantics made it to fail in designing a generic system for which expressive access control is needed.

Attributes possess a major role in ABE and encryption of data is done under a set of attributes describing the intended receivers. The secret key of these users is also associated with the attributes set for encryption. Attribute-based encryption schemes allow users to decrypt cipher-text as long as it has the attributes satisfying a threshold policy. Subsequent researches on ABE can roughly be classified based on the access policy, as Key-Policy ABE (KP-ABE) [51] and Ciphertext-Policy ABE (CP-ABE) [52].

In KP-ABE [51], the ciphertext is associated with a set of attributes and the secret key is associated with the access tree. The encrypting party has no control over who has access to the data and can only define the set of descriptive attributes necessary to decrypt the ciphertext. There is a trusted authority that generates the secret key, provided the user submits the appropriate values for the attributes that constitute the access tree. In CP-ABE [52], the ciphertext is associated with the access tree and the encrypting party determines the policy under which the data can be decrypted, while the secret key is associated with a set of attributes.

Melissa Chase [53] proposed the scheme called multi-authority ABE model for the cloud access control which addressed many problems of single authority ABE schemes. It involves several authorities coordinated by a trusted Central Authority (CA), which distributes the attribute keys to users. However, the central authority holds the master key of the system, so it can decrypt all the ciphertext in the scheme. Each user is assigned a unique global User IDentifier (UID) and each user is assigned a unique Authority IDentifier (AID). Both the UID and AID are issued by a Certificate Authority (CA) trusted by the various authority domains. To prevent two users from colluding together to gain illegal access of data, the CA-certified UID is to be used together with the secret keys issued by different authorities for data decryption. The authors propose an efficient attribute revocation method in multi-authority CP-ABE systems using proxy encryption. The utilization of a CA brings new security vulnerability and increases the computation and communication cost.

In 2010, Lin et al. [54] adopted the Distributed Key Generation (DKG) protocol [55] and the Joint Zero Secret Sharing (JZSS) protocol to construct the secure threshold Multi-Authority Fuzzy Identity-Based Encryption (threshold MA-FIBE) scheme without a central authority for the first time. To initialize the idea, the multiple authorities must cooperatively execute the DKG protocol and the JZSS protocol twice and $k$ times, respectively, where $k$ is the degree of the polynomial selected by each authority. Each authority must maintain $k + 2$ secret keys. This scheme is k-resilient; namely, the scheme is secure if and only if the number of the colluding users is no more than k, and k must be fixed in the setup algorithm.

Chase and Chow [56] proposed a multi-authority KP-ABE scheme which removes the central authority by using a distributed PRF (pseudorandom functions) technique. Notably, they also addressed the privacy of the user. In previous multi-authority ABE schemes [53], the user must submit his GID to each authority to obtain the corresponding secret key. This will increase the risk of user traced by a group of corrupted authorities. In order to avoid this risk, Chase and Chow [56] provided an anonymous key issuing protocol for the GID, where a 2-party secure computation technique is employed. This scheme is $(N - 2)$-tolerant; namely, the scheme is secure if and only if the number of the corrupted authorities is no more than $N - 2$, where $N$ is the number of the authorities. Chase and Chow also left an open problem on how to construct a privacy preserving multi-authority ABE scheme without the need of cooperation among the authorities.

Han et al. [57] answered the question left by Chase and Chow [56] affirmatively by proposing a decentralized KP-ABE scheme with the privacy-preserving key extraction protocol. In their scheme, multiple authorities can work independently without any cooperation and a central authority. The GID is used to tie all the user's secret keys together, while the corrupted authorities cannot pool the user's attributes by tracing it. The scheme is any number tolerant for the users and $(N - 1)$-tolerant for the authorities, where $N$ is the number of the authorities. Lewko and Waters [58] proposed a new multi-authority scheme. Although their scheme may become inefficient for large attribute universe, it is the first adaptively secure multi-authority CP-ABE scheme proved in the random oracle model. This scheme improves the previous multi-authority ABE schemes, because it does not require collaboration among multiple authorities in the setup and key generation phases, and there is no central authority. Note that the authority in this scheme can join or leave the system freely without reinitializing the system. Besides the low efficiency, this scheme has another drawback that the attributes of the user can be collected by tracing his GID.

## 6. Prospects of future research and conclusions

Many cloud access control schemes vary in the description of rules for the access control and many such methods are unable to meet the requirements of the application due to many deficiencies. So study and formulation of a unified, easy to use, articulate and high executive efficiency method to describe the access control rules is necessary. So there still exist many problems worth further studying. For better

service quality and security, there is a need for developing a privacy preserved access control models. Such a system is necessary to preserve the confidentiality and privacy of user's data in the public cloud from others. Also there is a need for designing a high security access control models with little costs of computation, communication and storage.

We discussed many security challenges in utilizing the benefits of cloud services. A detailed survey and analysis on various access control models for the cloud were discussed. We also highlighted the importance of Attribute Based Encryption and in recent years, attribute-based encryption is a relatively attractive research topic as it has many attracting properties. It provides a fine-grained and non-interactive access control mechanism of encrypted data and has great potential applications in many fields.

## References


1. M e l l, P., T. G r a n c e. The NIST Definition of Cloud, National Institute of Standards and Technology, 2011.
2. W a n g, C., Q. W a n g, K. R e n, W. L o u. Ensuring Data Storage inn Cloud Computing. – In: Proc. of 17th International Workshop on Quality of Service, 2009.
3. W a n g, Z. Security and Privacy Issues within the Cloud Computing. – In: Proc. of 2011 International Conference on Computational and Information Sciences, IEEE, 2011.
4. H u b b a r d, D. W., H. Z. S u t t o n. Top Threats to Cloud Computing. V1.0. 2010.
5. S u b a s h i n i, S., V. K a v i t h a. A Survey on Security Issues in Service Delivery Models of Cloud Computing. – Journal of Network and Computer Applications, Vol. **34**, January 2011, No 1, pp. 1-11.
6. R o b e r t, D., T. S t e p h e n. A Survey on Securing the Virtual Cloud. – Journal of Cloud Computing: Advances, Systems and Applications, Vol. **2**, 2013, No 1, pp. 2-17.
7. C l a v i s t e r. Security in the Cloud. 2009. **http://www.it-wire.nu/members/cla69/attachments/CLA_WP_SECURITY_IN_THE_CLOUD.pdf**
8. A n d e r s o n, R. Security Engineering: A Guide to Building Dependable Distributed Systems. John Wiley & Sons, 2010, p. 640.
9. A u s a n k a C r u e s, R. Methods for Access Control: Advances and Limitations. 2004.
10. B e l l, D., L. L a P a d u l a. Secure Computer Systems: Mathematical Foundations. Bedford, MA, 1973.
11. B i b a, K. Integrity Considerations for Secure Computer Systems. MA, Bedford, 1977.
12. H a r r i s, S. Mike Meyers' CISSP (R) Certification Passport. 1st Ed. McGraw-Hill, 2002, p. 422.
13. L a m p s o n, B. Protection. – In: Proc. of 5th Princeton Symposium on Information Sciences and Systems, Princeton University, 1971.
14. S a m a r a t i, P., S. V i m e r c a t i. Access Control: Policies, Models, and Mechanisms. Foundations of Security Analysis and Design, 2001, pp. 137-196.
15. L a u r i e, B. Access Control. V0.1. 2009.
16. O h, S., S. P a r k. Task-Role-Based Access Control Model. – Information Systems, Vol. **28**, September 2003, No 6, pp. 533-562.
17. S u h e n d r a, V. A Survey on Access Control Deployment. – Communications in Computer and Information Science, Vol. **259**, 2011, pp. 11-20.
18. H u, V. C., K. S c a r f o n e. Guidelines for Access Control Ssystem Evaluation Metrics. 2012.
29. A l-K a h t a n i, R. S a n d h u. A Model for Attribute-Based User-Role Assignment. – In: Proc. of 18th Annual Computer Security Applications Conference (ACSAC'02), IEEE Comput. Society, 2002.

20. K a r p, A., H. H a u r y, M. D a v i s. From ABAC to ZBAC: The Evolution of Access Control Models. 2009.
21. B r u c k e r, A., L. B r u g g e r, P. K e a r n e y, B. W o l f f. An Approach to Modular and Testable Security Models of Real-World Health-Care Applications. – In: Proc. of 16th ACM Symposium on Access Control Models and Technologies (SACMAT'11), 2011.
22. C h e n g, P., P. R o h a t g i. Fuzzy Multi-Level Security. – In: Proc. of IEEE Symposium on Security and Privacy, 2007, SP'07, 2007.
23. C h o u d h u r y, A., P. K u m a r, M. S a i n, H. L i m, H. J a e-L e e. A Strong User Authentication Framework for Cloud Computing. – In: 2011 IEEE Asia-Pacific Services Computing Conference, 2011.
24. C r a g o, S., K. D u n n, P. E a d s, L. H o c h s t e i n, M. K a n g. Heterogeneous Cloud Computing. – In: Proc. of 2011 IEEE International Conference on Cluster Computing, IEEE, 2011.
25. P a t i l, V., A. M e i, L. M a n c i n i. Addressing Interoperability Issues in Access Control Models. – In: Proc. of 2nd ACM Symposium on Information, Computer and Communications Security ASIACCS'07, 2007.
26. H u, V., D. K u h n, D. F e r r a i o l o. The Computational Complexity of Enforceability Validation for Generic Access Control Rule. – In: Proc. of IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing (SUTC'06), IEEE, 2006.
27. K e r o m y t i s, A., J. S m i t h. Requirements for Scalable Access Control and Security Management Architectures. – ACM Transactions on Internet Technology, Vol. **7**, 2007, No 2.
28. J i n, X., R. K r i s h n a n, R. S a n d h u. A Unified Attribute-Based Access Control Model Covering DAC, MAC and RBAC. – In: Proc. of 26th Annual Conference on Data and Applications Security and Privacy IFIP WG 11.3, 2012.
29. A l m u t a i r i, A., M. S a r f r a z, S. B a s a l a m a h. A Distributed Access Control Architecture for Cloud Computing. – In: Proc. of Softw. IEEE 2012, 2012.
30. F e r r a i o l o, D., J. B a r k l e y, D. K u h n. A Role-Based Access Control Model and Reference Implementation within a Corporate Intranet. – ACM Transactions on Information and System Security (TISSEC), Vol. **2**, 1999, No 1, pp. 34-64.
31. H a s e b e, K., M. M a b u c h i, A. M a t s u s h i t a. Capability-Based Delegation Model in RBAC. – In: Proc. of 15th ACM Symposium on Access Control Models and Technologies e SACMAT'10, New York, USA, 2010.
32. O h, S., S. P a r k. Task Role-Based Access Control Model. – Information Systems, Vol. **28**, September 2003, No 6, pp. 533-562.
33. Z h a n g, R., L. L i u, J. L i, Z. H a n. RBTBAC: Secure Access and Management of EHR Data. – In: Proc. of 3rd International Workshop on e-Healthcare Information Security (e-HISec'2011), 2011.
34. T i a n y i, Z., L. W e i d o n g, S. J i a x i n g. An Efficient Role Based Access Control System for Cloud Computing. – In: Proc. of 11th International Conference on Computer and InformationTechnology, 2011 IEEE.
35. J a y a p r a k a s h, H. A., M. H. G u n e s. Ensuring Access Control in Cloud Provisioned Healthcare Systems. – In: Proc. of Consumer Communications and Networking Conference (CCNC'11), 2011.
36. S u n, L., H. W a n g, J. Y o n g, G. W u. Semantic Access Control for Cloud Computing Based on e-Healthcare. – In Proc. of 16th International Conference on Computer Supported Cooperative Work in Design (CSCWD'12), 2012 IEEE.
37. T s a i, W., Q. S h a o. Role-Based Access Control Using Reference Ontology in Clouds. – In: Proc. of 10th International Symposium on Autonomous Decentralized Systems, 2011.
38. M o n, E., T. N a i n g. The Privacy-Aware Access Control System Using Attribute-and Role-Based Access Control in Private Cloud. – In: Proc. of 4th IEEE International Conference on Broadband Network and Multimedia Technology, 2011.
39. R a, C. W. K., W. L. S. Y u. Achieving Secure, Scalable, and Fine-Grained Data Access. – In: Proc. of 29th IEEE International Conference on Information, 2010.
40. W a n, Z., J. L i u, R. H. D e n g. HASBE: A Hierarchical Attribute-Based Solution for Flexible and Scalable Access Control in Cloud Computing. – IEEE Transactions on Information Forensics and Security, Vol. **7**, April 2012, No 2, pp. 743-754.

41. J e r e m y, H., L. B e n. Toward Hierarchical Identity-Based Encryption. – Lecture Notes in Computer Science, Advances in Cryptology – EUROCRYPT 2002, Vol. **2332**, Springer Berlin Heidelberg, 2002, pp. 466-481.
42. X i n, D., Y. J i a d i, L. Y u a n, C. Y i n g y i n g. Achieving an Effective, Scalable and Privacy-Preserving Data Sharing Service in Cloud Computing. – Computers & Security, Vol. **42**, 2014, pp. 151-164.
43. L i u, Q., G. W a n g, J. W u b. Time-Based Proxy Re-Encryption Scheme for Secure Data Sharing in a Cloud Environment. – Information Sciences, Vol. **258**, February 2014, No 10, pp. 355-370.
44. L i u, H., Q. X i o n g. Shared Authority Based Privacy-Preserving Authentication Protocol in Cloud Computing. – IEEE Transactions on Parallel and Distributed Systems, Vol. **26**, January 2015, No 1, pp. 241-251.
45. N a b e e l, M., E. B e r t i n o, B. T h u r a i s i n g h a m, M. K a n t a r c i o g l u. Towards Privacy Preserving Access Control in the Cloud. – In: Proc. of International Conference on Collaborative Computing: Networking, Aplications and Worksharing (CollaborateCom), Orlando, USA, 2011.
46. M a r i a n, H., F. S a s c h a, B. M i c h a e l, M. T h o m a s, S. M a t t h e w. Towards Privacy-Preserving Access Control with Hidden Policies, Hidden Credentials and Hidden Decisions. – In: Proc. of 10th Annual International Conference on Privacy, Security and Trust, 2012.
47. H a s s a n, T. Privacy Aware Access Control for Data Sharing in Cloud Computing Environments. – In: Proc. of 2nd International Workshop on Security in Cloud Computing, 2014.
48. H u a n g, X., Q. T a o, B. Q i n, Z. L i u. Multi-Authority Attribute Based Encryption Scheme with Revocation. – In: Proc. of 24th IEEE International Conference on Computer Communication and Networks (ICCCN'2015), 2015
49. S a h a i, A., B. W a t e r s. Fuzzy Identity-Based Encryption. – In: Advances in Cryptology – Lecture Notes in Computer Science, Springer, 2005, pp. 457-473.
50. N a l i, D., C. A d a m s, A. M i r i. Using Threshold Attribute Based Encryption for Practical Biometric-Based Access Control. – International Journal of Network Security, Vol. **1**, 2005, No 3, pp. 173-182.
51. G o y a l, V., O. P a n d e y, A. S a h a i, B. W a t e r s. Attribute Based Encryption for Fine-Grained Access Control of Encrypted Data. – In: Proc. of 13th ACM Conference on Computer and Communications Security (CCS'06), November 2006.
52. B e t h e n c o u r t, J., A. S a h a i, B. W a t e r s. Ciphertext-Policy Attribute-Based Encryption. – In: Proc. of IEEE Symposium on Security and Privacy (SP'07), May 2007, pp. 321-334.
53. C h a s e, M. Multi-Authority Attribute Based Encryption. – In: Proc. of 4th Conference on Theory of Cryptography TCC'07, 2007.
54. L i n, H., Z. C a o, X. L i a n g, J. S h a o. Secure Threshold Multi Authority Attribute Based Encryption Without a Central Authority. – Information Sciences, Vol. **180**, 2010, No 13, pp. 2618-2632.
55. G e n n a r o, R., S. J a r e c k i, H. K r a w c z y k, T. R a b i n. Secure Distributed Key Generation for Discrete-Log Based Cryptosystems. – In: Proc. of Advances in Cryptology – EUROCRYPT'99, 1999.
56. C h a s e, M., S. S. M. C h o w. Improving Privacy and Security in Multi-Authority Attribute-Based Encryption. – In: 16th ACM Conference on Computer and Communications, Chicago, Ill, USA, November 2009, pp. 121-130.
57. H a n, J., W. S u s i l o, Y. M u, J. Y a n. Privacy-Preserving Decentralized Key-Policy Attribute-Based Encryption. – IEEE Transactions on Parallel and DistributedSystems, Vol. **23**, 2012, No 2, pp. 2150-2162.
58. L e w k o, A., B. W a t e r s. Decentralizing Attribute-Based Encryption. – In: Advances in Cryptology, Lecture Notes in Computer Science, Heidelberg, Germany, Springer, 2011, pp. 568-588.
59. R a y k o v a, M., H. Z h a o, S. M. B e l l o v i n. Privacy Enhanced Access Control for Outsourced Data Sharing. – In: Proc. of Financial Cryptography and Data Security, 2012.