ISSN (Print): 0974-6846
Indian Journal of Science and Technology, *Vol 11(48), DOI: 10.17485/ijst/2018/v11i48/132752, December 2018* ISSN (Online): 0974-5645

Integrated Model for Open Learning Environment with Dynamic Multilayer Authentication and Hybrid Access Control using Cloud

R. Anuratha* **and M. Ganaga Durga**

Computer Science, Bharathiar University, Coimbatore – 641056, Tamil Nadu, India;
anu_ksyo@yahoo.com, mgdurga@yahoo.com

Abstract

Objective: This study mainly focuses on secure and user-friendly open learning environment using the cloud. This will improve the quality of education, individual care and global education. **Methods:** To make a deep analysis of the existing massive open online courses learning environment and build a mobile application using PHP and MySQL. The application is simulated under Veracode and the authentication attack prevention time is noted. In this paper hybrid Access Control Model is compared with other Access Control Models and the results are discussed. **Findings:** This research work recommends a mobile application using dynamic multilevel authentication with hybrid access control for open learning environment. The mobile application has the features like device identification, freedom in preparing security index, a random question from the security index instead of a textual password, cherished graphics password, limited unauthorized attempts with time bound and hybrid access control. Dynamic multilayer authentication proves prone free from authentication attacks. Hybrid access control under dynamic policy management delivers flexible and fine-grained authorization. This model supports primarily least privilege principle, flexibility, scalability, trust level, supporting heterogeneity and temporal constraints with dynamic policy management. It shows better results than the traditional Access Control Models. **Application:** The proposed system suggests a highly secured and cost-effective mechanism for the open learning environment.

Keywords: Access Control, Dynamic Multilevel Authentication, Hybrid Access Control Model, Ontology, Open Learning Environment

1. Introduction

Imminent technologies precisely Social media, Mobility, Analytics, Cloud computing (SMAC) redefine the fourth-generation enterprise model. Just visualize SMAC as human body then social media is the hands which interacts and shares the idea; mobile is the senses which taking into the external environment; analytics is the brain, and cloud is the skeleton, which holds it all together[1].

Open learning encourages supplementary learning and lifelong learning with 3A's (Anytime, Anywhere, Anyone) and 5R's (Retain, Reuse, Revise, Remix and Redistribute) with the help of the cloud storage. Interactive and flexible open learning environment attract learner participation than traditional learning. The massive growth in online courses underlines an alarm for security and privacy. This research paper highly concentrates in Access Control Models.

Access control plays crucial role in security of computing. Mostly it is used to grant or revoke access rights, to limit access rights and to prevent access rights from illegal attacks. Access Control is a security technique that has a set of controls to restrict access to certain resources.

The three traditional Access Control Models are discretionary access control, mandatory access control and role-based access control. Discretionary access control (Figure 1(a): User centric-identity based), which is most widely used; grants access in the basis of discretion of the

*Author for correspondence

user. Access Control List (ACL) is an example. In mandatory access control (Figure 1(b): admin centric - rule based) administrator manages access permission to each user/group with device/resource depending upon the secrecy level. Security label is an example. Role based access control (Figure 1(c): role centric) model simplifies by assigning role to user using job hierarchy and give access to system objects based on their role. Subject (S), Object (O) and Action (A) are the basic tuple entities in access control (S, O, A). Based on the three entities permission will be enforced to allow or deny the action to the objects by the subjects.

Due to the dynamic and distributed environment some type of constraints regarding location, time and attributes of subjects, the basic Access Control Model proves weaker in the sense. There an efficient dynamic model will be required. The objective of the research work is to develop a hybrid Access Control Model for the open learning environment, which is collaborative in nature.

2. Background

2.1 Technical Preliminaries

2.1.1 Open Learning Environment

Open learning environment is innovative, experimental and self-regulative (participatory) structure. Open learning environment denotes global open educational strategies such as the massive open online courses. It includes a set of trivial modular units supported by online resources with interactive learning activities.

2.1.2 Dynamic Multilayer Authentication

Dynamic multilayer authentication approach combines two or more authentication techniques into a unified solution that delivers the robust solution. It highly supports device-based authentication.

2.1.3 Access Control

Access control is a prevailing mechanism that limits (allow or deny) the entity, who (subject (S) may be device, user, group, role and process) may do function (action A read, write and execute) with certain resources (object (O) may be any computing resource like a file, printer and database) under constraints (rule, policy, location and time). Access Control Models can be classified into centralized model and decentralized/collaborative model.

Centralized approach is more restricted model, where administrator or central authority is responsible for granting or denying access to user. Example: Mandatory access control, role-based access control, discretionary access control, attribute-based access control, usage control, content-based access control, task-based access control, policy-based access control and organization-based access control. In the decentralized model users are responsible for their resource policies. Example: governance-based access control.

2.1.4 Personally Identifiable Information

Personally Identifiable Information: PII is any data that can be used to uniquely identify a person. PII is classified into four types (general, static, dynamic and confidential).

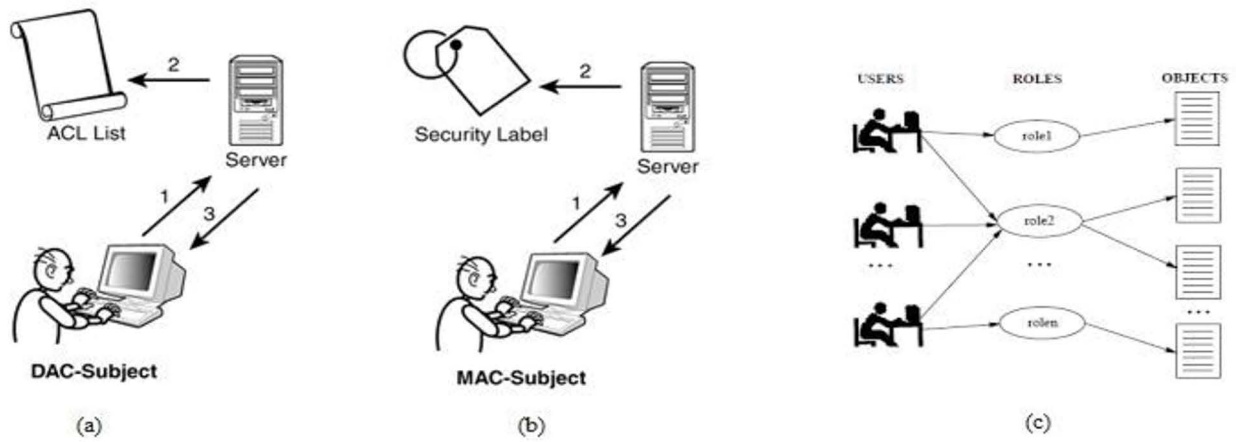

Figure 1. (a) Discretionary access control, (b) Mandatory access control and (c) Role-based access control.

- General – common attributes of the person like name, color, etc.
- Static – fixed values in nature like date of birth, birthplace, school name, etc.
- Dynamic – mutable values like address, present designation, income, last seen movie, etc.
- Confidential – private values like PAN number, bank account number, pass port number, health report, etc.

2.2 Literature Study

This study[2] has described that the discretionary model is the concept of ownership model. Mandatory Access Control Model[3] consists of two components a security level and a set of categories, which can be implemented in multilevel for ensuring information confidentiality in Defense applications.

This work[4] has proved that the Role-based Access Control (RBAC) model where object accesses are controlled by roles or job functions than the traditional discretionary and mandatory access control mechanisms. The design of attribute-based Access Control Model[5] has well suited in the cloud distributed environment.

This model[6] has proposed a scheme MA-ABE for multiple authority-based access control mechanism. The study[7] has framed C at BAC for building dedicated Access Control Models with the high-level security policies of each specific user. The previous work[8] has proved that CAACM (Context-Aware Access Control Model) to be safe, which enables dynamic activation of role permission by associating cloud management role with context.

In the context of social networks, the study[9] as reviewed Access Control Models by classifying them in relationship-based, attribute-based, community-structure-based and user activity centric based models. The proposed system suggests that Hybrid Access Control (HAC) consists of combination of Access Control Models, which can be implemented in multi-level, multi-phase and multi-factor models for the security of data in the dynamic and distributive cloud environment.

3. Proposed System

Data privacy and security are the major impact of social network and smart devices. To overcome these constraints secure authentication and access control mechanism is framed by the proposed system in the open learning environment.

Major contribution of the work is as follows:

- Provide Dynamic Multilayer Authentication (DMA).
- Create Hybrid Access Control (HAC).
- Build an intellectual hybrid mobile application for open learning environment using DMA and HAC.
- Verify the performance in terms of security, flexibility and feasibility.

The Figure 2 represents the overall contribution of the system work.

3.1 Dynamic Multilayer Authentication[10]

Authentication confirms the right person with their identity (who are you?). The proposed system recommends a dynamic multilayer authentication designed with three phases:

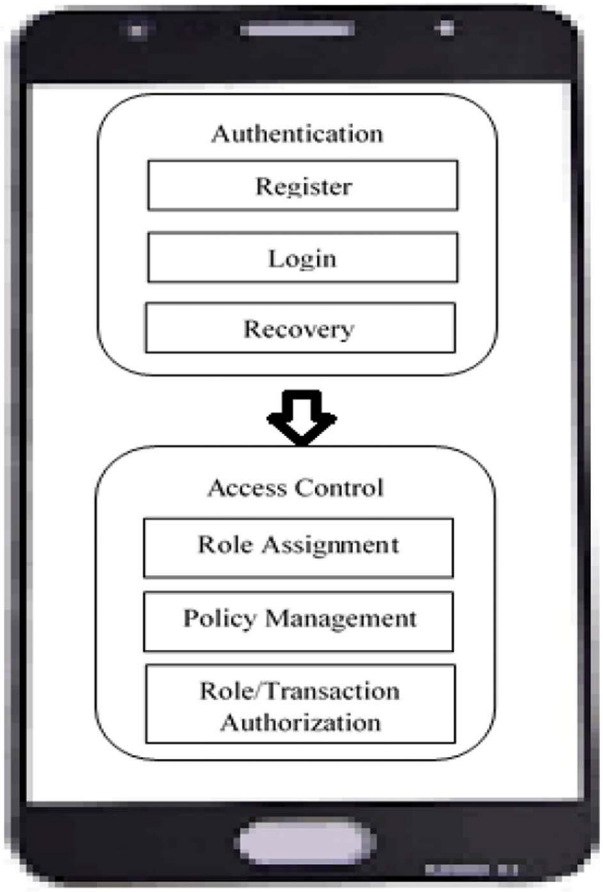

Figure 2. Proposed system model.

- Registration using Personally Identifiable Information (PII), Graphics Password (GP) and device ID with SIM number.
- Login using device ID and SIM number, security question and graphics password.
- Recovery for updating/changing dynamic PII and GP.

Device identification, a random question from the pool of PII and graphics password simply avoids guessing attack. The limited unauthorized attempts prove that the system is prone free from authentication attacks.

Authorization: Authorization governs the access privileges depending upon the user rights given in the access control matrix. The proposed system recommends a hybrid access control with dynamic policy management for authorizing the user access. Granting and revoking access policy is analysed carefully and designed for high authorization granularity.

3.2 Hybrid Access Control

3.2.1 Fundamental Conceptions in HAC Model

User (U): An entity (subject) who has the rights to access the resource (application, process and system). User is classified into four levels: Level 0 (p), Level 1 (h), Level 2 (f) and Level 3 (s).

$$U \rightarrow \{p, h, f, s\}$$

Data (D): course Subject is encompassed as Data. It may be in the content, assignment, discussion and feedback format. Data (object) are stored in raw format or un-organised format in computer. It may be in text documents (rtf, pdf), images (png, jpg), audio clips (wav, mpeg), video clips (mp4, avi) and software programs (p).

$$D \rightarrow \{rtf, pdf, png, jpg, wav, mpeg, mp4, avi, p\}$$

Function (F): Function (action) represents set of activities like read (r), write (w), change (c), delete (d), upload (up), download (dn) and execute (x).

$$F \rightarrow \{r, w, c, d, up, dn, x\}$$

Role (R): Role defines the status or job position in an organization. Role is assigned to different types of user in a same status. Role is classified into five types: super Admin (sad), admin (ad), provider (ct), consumer (l) and guest (g).

$$R \rightarrow \{ sad, ad, ct, l, g\}$$

Role mapping

$$U \Leftrightarrow R = \{(p \rightarrow sad), (h \rightarrow ad), (f \rightarrow ct), (s \rightarrow l), (h \rightarrow g), (ct \rightarrow g), (s \rightarrow g)\}$$

Rule (L): Rule streamlines the standard or policy. This will strongly regulate the user access. For example, the application is available to the particular location or particular time. Then it will be implemented as a rule for that situation.

Permission (P): Permission ensures the action to be performed to their allowed function or not (i.e. action allowed/permitted or denied/discard/prohibit).

Constraint (C): Constraint violates action in a particular situation to the rule.

Constraints will be given by the high privileged authorities dynamically. For example, during exam hours the consumers may not be allowed to access the application from anywhere, even though the user has 24 × 7 hours access to the application.

The access control development process consists of three phases: security policy, security model and security mechanism.

3.2.2 Security Policy

Security policies simply define a set of rules that has the legal permission to access what resources under which conditions. It is based on role hierarchy and relationship with subjects (S). It is also maintained by centralized authority, which is dynamic in nature. Subjects' role and their attributes are taken into consideration for granting and revoking access.

Role Hierarchy: The Figure 3 represents the role hierarchy (position) in the higher education institution. The role hierarchy is classified into four levels.

Role Assignment and Privileges of Role: The role is assigned to the hierarchy level of the institution.

- Super admin: Level 0 user has assigned with super Admin role and has the power to control all the activities of entire domains.
- Admin: Level 1 user has assigned with admin role and has the power to control their own domain.
- Provider: Level 2 user has assigned with provider role and has all rights to their allotted or handled course subjects.
- Consumer: Level 3 user has assigned with consumer role and has the limited access to their course subjects.

- Guest: Except Level 0, all the other users are treated as guest role to other domain or other subjects' activities.

Super admin, admin and course teacher are considered as highest privileged authorities. Learner has the lowest privileges and guest has the least privileges.

Relationship: Each course Subject (s) is assigned with provider and consumer. A provider can handle two or more course Subjects with in the domain or other domains. One course Subject may be handled with more than one provider also. Each provider has the rights to access their own handled course Subjects only. Each consumer has the access to their assigned course Subjects only. The Figure 4 depicts the relationship between the three subjects (provider, course Subject and consumer).

Policy Management (P): Policy management governs the access control of the entire system. Subject, object and action are the components of the tuple. Well defined policy is assigned to each role in the system according to the secrecy level and other constraints. Policy enforcement is dynamic to the environmental conditions.

P1 – Secrecy Level: Secrecy level is classified into five: top secret, secret, confidential, restricted and protected according to the five-user level.

P2 – Conflict Domain: The subjects in the particular domain is treated as their own role. But the same subjects are treated as guest role to another domain. The Figure 5 represents the details of conflict domain.

P3 – Constraints: Occasionally, the provider is assigned with a course Subject to other domains consumers and the consumers are assigned with the other domain's course Subject also. Here, the course Subject is free from domain.

P4 – Time: Generally, every institution has a semester pattern. Each semester has six-month period of time. Role assignment is continuously monitored and changed with every six months including course Subject allocation, which correlates the consumer and provider relationship.

If the consumer wants to continue accessing the course Subjects which is in the previous semester will be permitted to continue in consumer role or guest role with the permission from the admin.

P5 – Flexibility: Course Subject, consumer and provider are dynamic in nature. Provider has the power to reuse the same content or change the content of the course Subject to their wishes.

Role assignment with the level of hierarchy (i.e. subject and permission to the object) is utmost static in nature. Policy management is dynamic in nature. Role mapping and subject mapping is done with two different tables and maintained in the ACL database.

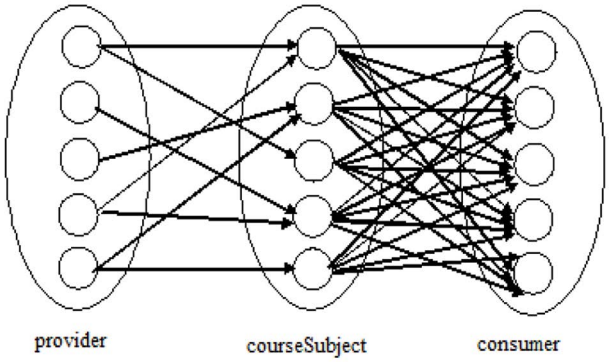

Figure 4. Relationship with provider, course Subject and consumer.

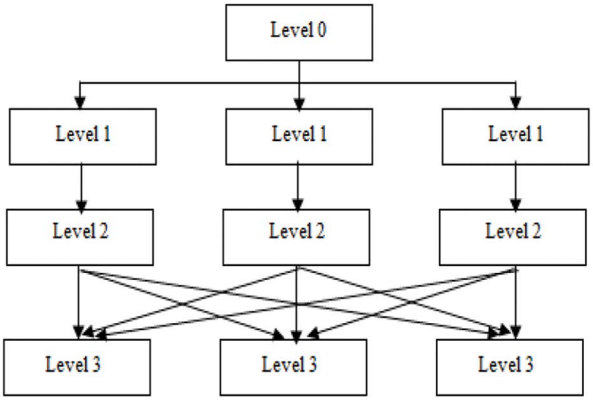

Figure 3. Role hierarchy.

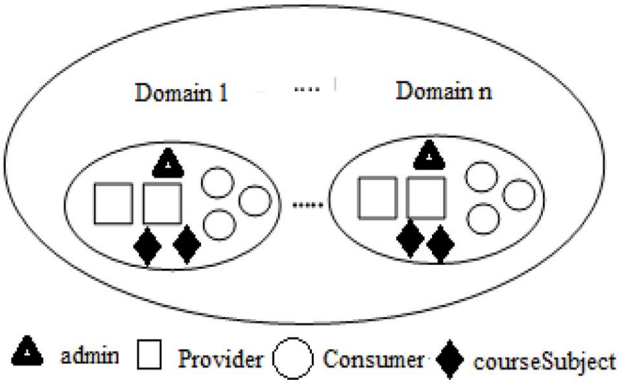

Figure 5. Conflict domain.

3.2.3 Security Model

Security model represents the implementation of security policies. Access control matrix is one of the models used to describe the user access privileges and permissions to the entire system. It has the following essential components user (subject), function (action), data (object), permission (rights) and constraints (exception). The access control matrix (Figure 6) defines the security model of the system.

An Access Control policy is (AC) implemented using set of rules (R). Rule structure is also drawn by certain terms and decisions. Decisions are often in binary format (allow (1) or deny (0)).

3.2.4 Security Mechanism

It defines the hardware and software functions that will be implemented the methodologies described by the security policy and also stated in the security model. The Figure 6 illustrates the system flow of HAC system.

3.2.5 Auditing

The user activities will be tracked and log files will be maintained to understand the behaviour of every user in order to identify any disruptions. Analysing and accounting act a major role for the security of the system.

4. Simulation

As the world becomes more associated with the networks, the impact of network security may also continuously increase. Authentication, Authorization, Access control and Encryption (3AE) proves strongest network control[11]. Due to the unbelievable increase of mobile phone users, proper training about the importance of security features is also mandatory[12]. Cloud computing may possibly have all-embracing potential in improving the infrastructure within the higher education institutions[13]. Authentication plays a substantial role for authorizing identity proof[14]. In the study, hybrid model which comprises blended mode of any two Access Control Models guarantees the data security in the Cloud environment[15]. Dynamic multilayer authentication proves prone free from authentication attacks successfully[10].

	Course content	Assignment	Feedback
sad	r,w,c,d,up, dn,x	r,w,c,d,up, dn,x	r,w,c,d,up, dn,x
ad	r,w,c,d,up, dn,x	r,w,c,d,up, dn,x	r,w,c,d,up, dn,x
p	r,w,c,d,up,dn	r,w,c,d,up,dn	r,w,c,d,up,dn
c	r,dn	r,w,up,dn	r,w,up,dn
g	r	r	r

Figure 6. Access control matrix.

An intellectual mobile application is built using PHP and MySQL. The application (apk) and the database are stored in the cloud sever. The user can be benefited by downloading the mobile application. Authentication and access control are implemented carefully in the mobile application. Due to the financial constraints, the proposed system has designed and tested the application with limited number of domains.

Login procedure is successfully implemented using Dynamic multilayer authentication[10]. For hybrid access control the following phases are designed carefully.

4.1 Role Activation and Authorization

After completion of successful login procedure, each user role is assigned with ACL database (Figure 7). Under policy management the role is enforced or authorized to do the prearranged operations. If any deceptive mischief emerged, the user activation is failed or revoked.

4.2. Transaction/Operation Authorization

The following conditions are most significant for the transaction authorization:

- User can't make transaction that their allotted role does not authorize them to do.
- User can't view or modify resources to which he/she is not authorized.

4.3. Hybrid Access Control Model

HAC has the components like subject, object, function, policy with constraints. The Figure 8 exemplifies the model of Hybrid Access Control:

ACL database has two main relations: One relation for role mapping and another relation for policy management.

4.3.1 Role Authorization

During login procedure the user is authorized and activated with their role by role mapping.

4.3.2 Transaction Authorization

When the authorized user is requested for any function/operation, policy management is triggered and the transaction is permitted or denied due to the constraints.

This policy management (Table 1) under constraints ensures that the user vasu could upload the assignment if the condition (IF(obj.dept IS sub.dept) AND (sub.secracy IS GREATERTHAN OR EQUAL TO obj.secracy) AND (cur date and time IS WITHIN due) AND (operation IS uplaod) THEN *GRANT ACCESS* ELSE *DENY ACCESS*) satisfies the constraints only.

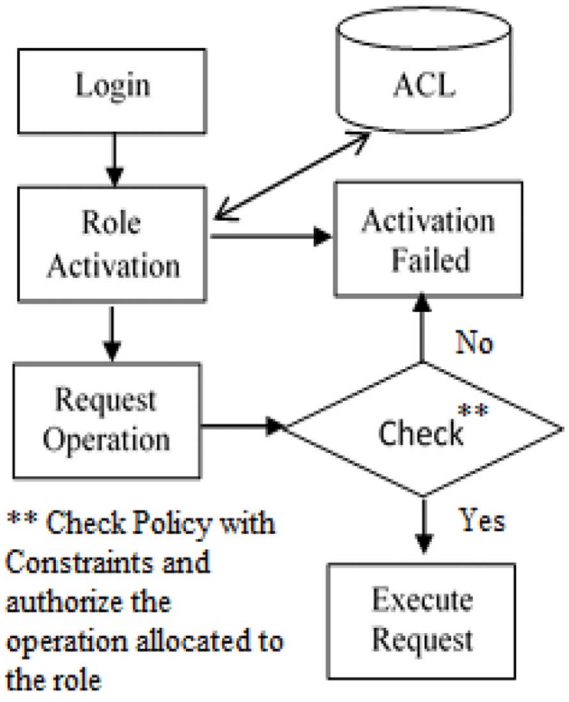

Figure 7. HAC system model.

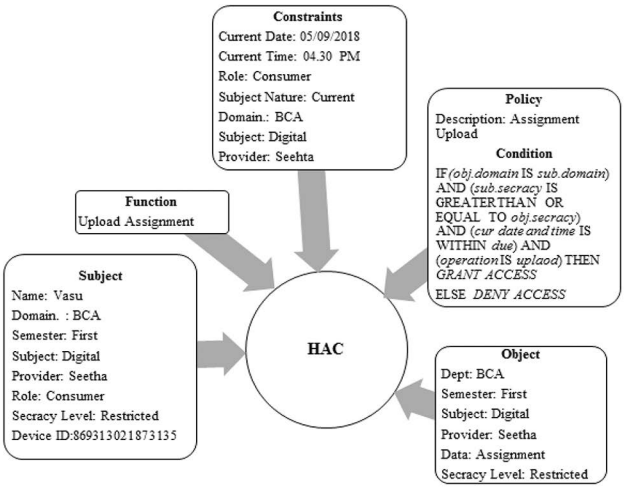

Figure 8. Model of HAC.

4.3.3 Ontology

Ontology deals with how entities can be grouped according to their similarities. It is a domain that shows the entity properties and their relationships between them. Protégé is a free open source software tool for building ontology framework in semantic network model.

The proposed hybrid Access Control Model has the primary concepts of subject (role), object (data) and action (permission). The relationship between the HAC primary concepts is shown with ontology graph using protégé.

The Figure 9 illustrates the permission between the role and object. This OWL graph will prove the role and transaction authorization.

5. Result and Discussion

Open learning environment is collaborative in nature. It is very hard to frame an Access Control Model due to shared data and dynamic access rights. When combining or extending the existing model into organization-based hybrid model, it may give a better solution. So that the proposed system recommends hybrid model integrated with authentication. The proposed model is analysed with other Access Control Models with the number of evaluation measures and the result is shown in the following Table 2.

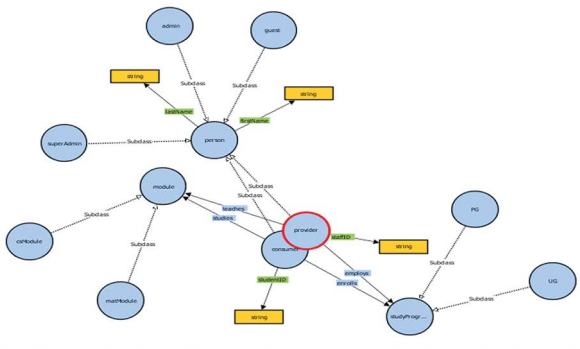

Figure 9. The general schema of OWL grap.

Table 1. An example for policy management

	Subject	Object	Function
Entity	Vasu	Assignment	Upload
Policy	Role: consumer Secrecy level: Restricted		
Constraints	Submission date: 05/09/2018, 04. 30 PM Subject nature: Current, Digital, First Semester Domain: BCA provider: Seetha		
Action	Verify the subject with policy and the constraints then similarities found Grant Permission otherwise deny permission to the user.		

Table 2. Evaluation result

Evaluation measures	DAC	MAC	RBAC	ABAC	HAC
Integrated with authentication	N	N	N	N	Y
Policy management	N	N	N	N	Y
Least privilege principle	N	N	Y	Y	Y
Auditing	Y	Y	Y	Y	Y
Flexibility	N	N	Y	N	Y
Supporting Heterogeneity	N	N	N	N	Y
Scalability	N	N	Y	N/A	Y
Delegation of capabilities	Y	N	N	N	Y
Separation of duties	N	N	Y	Y	Y
Temporal constraints	N	N	N	N	Y
Trust Level	N	N	Y	Y	Y

* N denotes not Supported, Y denotes supported and N/A denotes not applicable.

The proposed work combined admin centric model with user centric model and framed it as a hybrid one. This model supports primarily least privilege principle, flexibility, scalability, trust level, supporting heterogeneity and temporal constraints with dynamic policy management and also proves that it is a well framed one.

6. Conclusion

The study exposes that digital transformation absolutely increases the speed and availability in each field like banking, e-trade, e-governance and e-booking. Also, the digital world fully consists of learning opportunities and sharing ideas/opinions. Adapting to digital transformation in the open learning environment promises global education entirely. Security and privacy are the major issues in the short run. The intellectual mobile application has Dynamic Multilayer Authentication with Hybrid Access Control mechanism for flexible, efficacy, secure and cost-effective service in the open learning environment. A hybrid mobile application is built with limited domains and the simulator results also prove the same. The proposed work is extended to our institution in the future.

7. References

1. Insight into the Transformation of Business in the Cyber-Age. 2018. https:// datafloq.com/ read/smac-is-reshaping-the enterprise/17
2. Downs D. Discretionary access control guideline. Aerospace Report, Aerospace Corporation; 1985. p. 1–29.
3. Bokefode J, Swapnaja A, Ubale S, Apte Dattatray G, Modani. Analysis of DAC MAC RBAC access control based models for security. International Journal of Computer Applications. 2014; 104(5):6–13.

4. Ravi S, Ferraiolo D, Kuhn D. NIST model for role-based Access Control: Towards a unified standard. Proceedings of the ACM Workshop on Role-Based Access Control; 2000. p. 47–63.
5. Abdul RK. Access control in cloud computing Environment. ARPN Journal of Engineering and Applied Science. 2012; 7(5):1–3.
6. Parameshwari A, Rasina B. Fine grained data access control in cloud computing. International Journal of Computer Science and Information Technologies. 2014; 5(3):3126–31.
7. Salim K, Kamel A, Luigi L. Designing flexible Access Control Models for the cloud. Proceedings of the 6th International Conference on Security of Information and Networks. 2013. p. 225–32.
8. Zhenji Z, Lifa W, Zheng H. Context-aware Access Control Model. International Journal of Grid and Distributed Computing. 2013; 6(6):1–12. https://doi.org/10.14257/ijgdc.2013.6.6.01
9. Asim Y, Malik A. A survey on Access Control Techniques for Social Networks. Universidad of Islambad; 2016. p. 1–32.
10. Anuratha R, Ganaga D. Dynamic multi layer authentication for open learning environment. IEEE Digital Library (In Print). 2018. p. 1–773.
11. Anuratha R, Ganaga D. A comprehensive study on networking issues. International Journal of Research in Computer Applications and Management. 2014; 4(11):54–6.
12. Anuratha R, Ganaga D. A Survey on security features on BYOD (Bring your own device). National Conference on Innovative Trends in Computing and Technology; 2012. p. 122–8.
13. Anuratha R, Ganaga D. Cloud computing in educational institutions", "ROOTS". International Journal of Multidisciplinary Researches, (Special Issue on Innovation in Big Data Search, Mining and Management). 2016; 2:131–5.
14. Anuratha R, Ganaga D. Authentication – A part of identification in the cloud environment. International Journal of Advance Research in Science and Engineering. 2018; 7(1):25–34.
15. Anuratha R, Ganaga D. Analysis of data security in cloud computing using access control technique. International Conference on Global Talent Management in the Digital Era; 2017. p. 514–9.