Received: December, 2018

INASS

International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

Providing Ontology-Based Access Control for Cloud Data by Exploiting Subsumption Property among Domains of Access Control

Auxilia Michael[1]* **Raja Kothandaraman[2]** **Kannan Kaliyan[3]**

[1]Department of Computer Science and Engineering,
Sathyabama Institute of Science and Technology, Chennai, India
[2]Department of Computer Science and Engineering,
Dhaanish Ahmed College of Engineering, Chennai, India
[3]Department of Information Technology, AdhiParasakthi College of Engineering, Kalavai, India
* Corresponding author's Email: auxiliamphd@gmail.com

Abstract: Cloud computing has pulled in numerous business organizations and users because of its simplified administration effort, minimal maintenance cost and pervasive access to out-sourced resources, which can be hardware or software. Users share these resources in large-scale environments over the Internet. Stringent access control must be implemented in a cloud storage system for protecting sensitive information. Access control models in the current literature such as Discretionary Access control (DAC), Mandatory Access Control model (MAC), Role-Based Access Model (RBAC) or Attribute Access Control Model (ABAC) consider the entities of access control in isolation and thus leading to incorrect access control decisions. In this paper, Ontology-Based Access Control is proposed. This proposal uses an ontology to model the entities associated with access control and their interrelationships among them, which could be effortlessly adjusted to Cloud environments. Ontology promises to streamline knowledge sharing among the entities. Subsumption property is exploited over concepts, properties and individuals. The experimental results show that the number of rules to be stored in Policy Base is reduced and reasoning time is also considerably reduced because of applying subsumption property and hence access decision is made faster. Also, our work is compared with the existing works against the state of art models with the help of access control metrics provided by the National Institute of Standards and Technology (NIST). Our work answers the queries related to metric effectively than the existing works. Hence the performance of the system is increased and suitable for securing cloud data.

Keywords: Access control, Ontology, Security issues, Privacy, Subsumption.

1. Introduction

Nowadays users can share a large amount of information and resources (which includes hardware, web services, and so forth) through the Internet. This background provides a shared platform for heterogeneous clients (e.g., corporate, end user and so on.) by facilitating reformed client applications and frameworks [1], giving pervasive access to the mutual resources and requiring less regulatory endeavours; thus, they empower clients and organizations to expand their profitability. Lamentably, sharing of assets in open situations has altogether expanded the security dangers to the clients to whom the information belongs to. An approach to mitigating this issue consists of rights to control access over the sensitive resources. In particular, access management directs the access to the mutual resources as indicated by the user credentials, the resource type and the privacy choices of the resource owner. The vast majority of solutions to access control namely DAC, MAC, RBAC, and ABAC are chiefly based on priori and manually administered policies/rules over the resources. In any case, manually handling security guidelines and access limitations in open condition, for example, OSNs or the cloud is not functional because of the accompanying reasons: (i) An extensive number of entities should be handled. For instance, Google Drive has billions of clients and every client deals with multifarious assets. (ii) The heterogeneous objects associated with these environments would almost certainly have different protection prerequisites. For instance, for a cloud supplier offering storage, an organization including workers, faculties and assets would expect unique security necessities than individual users. (iii) The dynamicity and receptivity of such environments make the security necessities to change quickly based on the service type requested and end users [2]. Besides, a considerable percentage of the access control arrangements are proposed in the state of art. They are ineffectual for end users willing to deal with the access to sensitive data because of the accompanying issues: inflexible nature of access control models and numerous users lack specialized knowledge about information security and access control. Moreover, in many access control mechanisms, there is a relative decrease in performance as the number of entities engaged with the processing raises, which is risky in a distributed environment as a result of the number of elements to be managed [3-5]. In this manner, there is a need to create novel and strict access control arrangements suitable for open environments and overcome the previously mentioned difficulties [6].

The formulated goals are;

(i) The to think of an access control mechanism, with distinctive attention on the extensive and dynamic open state of affairs. Besides, we will think about components to formally demonstrate the entities associated with access control with intend to ease the managerial endeavours of manual administration.

(ii) To propose a common access control mechanism modelling the entities involved in access control and their interrelationships, thereby adapted to open environments.

(iii) To propose an access control model for dispersed open situations that consequently performs designation, denial and check of access rights in a proficient way.

Ontologies have picked up a considerable extent of concern as of late because of their potential as tools to arrange data and to constrain the difficulty of knowledge management. Ontologies are useful to determine the conceptualization and interrelations of an area of information [7-9] from which explicit domain objects (e.g., clients and assets) are characterized. According to our work, ontologies can be helpful for controlling access to resources. The modelled entities and their interrelations can be utilized to monitor the resource owners, their kind of relations with the resource requesters and with the resources. Through ontology, the access control on the resources can be effectively handled and authorized by following the interrelations of the ontological elements engaged with access control. Modelling the entities in the ontology can enormously expand the execution of the framework since it can undoubtedly recover target policy from the workflow by following the interrelationship of the objective elements as opposed to seeking from the database. Also, ontology reduces times of agreement between heterogeneous environments.

This paper is organized as follows: Section 2 entails the related work. Section 3 defines our proposed work, its architecture, and components. Section 4 includes security analysis; Section 5 includes experimental analysis, results, and discussion. Section 6 completes the paper with future work.

2. Related works

Fratila et al., [10] inferring that security and administrative laws are significant worries for bank areas. Banks can accomplish full security through a private cloud. New Banks have the objective of chopping down IT expenses and they can grasp private cloud. In any case, they should utilize compelling systems to anchor their own information notwithstanding security devices received by CSPs. Hamidi et al., [11] acquainted another model with actualizing security for E-Managing an account over the cloud. The model used RBAC for bearing the expected dimension of security. Be that as it may, allocating jobs and returning is done physically and every one of the drawbacks of RBAC influences the model.

Nedelcu et al., [12] discussed the points of interest and burdens of cloud in bank framework. They likewise proposed that security mechanism using access methods with high-security insight are required. A combination of ABAC and RBAC was suggested by Nai. This model discovers tenant accesses by the user. Matrix calculation is exploited for access delegation. XACML Compile time is reduced and invader cannot guess access information easily. The policy search cost is relational to the size of the database. Hence resulting in delayed access decision and ABAC is not yet consistent [13]. Tebaa et al., [14] suggested a way out for providing security and privacy using hybrid homomorphic encryption. Sensitive data are encrypted and operations are made on them without decrypting. But the shortcoming is that encrypting keys must be backed up, which is space and retrieval time overhead.

Choi et al., [15] proposed an ontology-based access control, including context for dynamic access control stating that conventional RBAC and improvement to it doesn't provide a complete solution. The reason in RBAC fails to consider security levels between objects. They created an ontology for modelling context. But the work fails to state how policies are updated and it does not concentrate on resolving policy conflicts.

Chi-Lun Liu proposed cloud access control dependent on ontologies. This work proposed a new-fangled access control mechanism called cloud service access control (CSAC). Two essential characteristics called payment status and service level are considered. Unreliable access control policies are identified by policy conflict analysis rules. In any case, the work doesn't utilize the standard ontology tool, which would not be flexible to adopt at all [16].

Ontology-based RBAC for utilizing information in cloud storage was proposed by Sun et al., [17]. Ontology is created for role assignment thereby simplifying the task. But the work fails to handle concept explosion problem and policy conflicts.

A work by Perez et al., [18] offers access control that protects user data irrespective of the Cloud service provider holding it. Unique identity-based and proxy re-encryption methods are exploited for protecting authorization model. The authorization model is highly expressive with role hierarchy modelled using an ontology, which enables advanced rule management like semantic conflict detection. The drawbacks the model provides a way to modify and update data which is not that much secure and authorization model is too complicated for privacy reasons and hence flexibility is not achieved.

Kalaiprasath et al., [19] offered an ontology-based approach for providing end-to-end security. They created cloud security ontology which captures all cloud-related threats. But the drawback is that it is not dynamic to capture new threats and it takes more time to analyse compliance models applicable to the cloud.

An enhanced technique for cloud storage was offered by Duraisamy et al., [20]. This work offers an automatic cloud data backup model. The backup mechanisms are not under the control of local jurisdiction. Thus they proposed end-to-end security for protecting cloud data using Inside Data Ownership Country Access (IDOCA) and Outside Data Ownership Country Access (ODOCA). This seems to be a novel and promising solution. But the time taken to upload file and server response time is not considered. So there is more space and time overhead.

Choudhary et al., [21] proposed a scheme for enabling access control through dynamic policy updating for cloud data. It enables data owners to check cypher text corrections. They also provide outsourcing policy updating facility to cloud service provider to minimize communication and computation overhead. They didn't discuss any means to resolve policy conflicts.

A work by Geetha et al., [22] presented an architecture called the E-RBAC model for enhancing and access control over the cloud services by calculating the trust of the roles assigned. They also gave a comparative analysis of SaaS provisioning with and without E-RBAC security model. Despite all these points, RBAC generally fails to consider security level among objects.

The access control researches specified in [23] discuss cypher-text based and inter-domain access control in cloud storage. Ciphertext-Policy Attribute-Based Encryption algorithm (CP-ABE), ontology-based attributes mapping, algebra-based policies integration, solutions for identification, access authorization and identity federation are the key technologies in current research. Secure access control for cloud storage, considering its environment heterogeneity is still lacking. Ontology proves to be an effective solution.

A multi-level policy-based schema was proposed in the work [24] for organizing and managing cloud data based on their sensitivity and confidentiality. The significance of this model is a syntactic and semantic analysis of requested policies by validity engine. Besides, Policy Match Gate and police checkpoint have been presented for ensuring policy application for data based on challenged policies in Security Level Certificate.

A work by Verginadis et al., [25] summarized important security challenges while moving to a cloud and proposed PaaSword – a novel holistic framework for lessening these challenges. Precisely, the proposed framework includes a context-aware security model, the required policy administration mechanism along with physical distribution, encryption and query middleware. But the model still fails to cope up with the needs of multifarious environments.

The suggested approach is called Proactive Dynamic Secure Data Scheme (P2DS), aiming to promise that the illegitimate access cannot be provided for sensitive data. They proposed two algorithms namely Attribute-based Semantic Access Control (A-SAC) Algorithm and Proactive

Determinative Access (PDA) Algorithm. The major aspects are: a semantic approach was provided for preventing access control. Second, the user-centric approach is followed to prevent users' data from unexpected use on the cloud side. Lastly, it can handle dynamic threats, including future hazards [26].

In this article, an innovative access control mechanism has been proposed. This mechanism reduces the searching cost and accessing time while providing access to the user [27].

Another work presents a new social network access control model by exploiting a new rule language RuleSN. This model provides efficient authorization expressiveness and flexibility to describe relations of User to User (U2U), User to Resource (U2R), Resource to Resource (R2R) and attributes of users and resources [28].

All these existing works offer different access control methods for controlling access to cloud resources. They have not thought about the interrelationship among the access control primitives, thereby leading to security violations. And the time taken for access decision and space required for storing the rules is more. Hence our research objectives are: To model the domains of access control using ontology; to exploit subsumption property among all levels and properties thereby dealing with smaller ontologies. Hence, the reasoning time is reduced and the access decision is made faster. Also, the number of rules to be saved in the policy base is reduced and the number of statements to express the rule also gets reduced.

3. Proposed work architecture

Fig. 1 shows the architecture of the efficient access control on the cloud data. This architecture involves the following components, outer components, and authorization components.

3.1 Outer components

Outer components are the subjects, reputation system and administrative tools. Subject requests for access rights. The reputation system checks the validity of credentials. Administrative tools are used for adding or removing authorization rules from the policy base.

3.2 Authorization components

Ontology Base includes ontologies of domains of access control say subject, object and action ontologies. Policy Base includes the explicit access control rules defined by the system data owner through security administrates. Inference Engine receives ontology as input and applies the subsumption algorithm on those ontologies and produces reduced ontologies.

Policy Engine receives the inferred access request and checks against the rule from the Policy Base. If the active entity in inferred access request matches with the rule, then access is granted otherwise not.

The formal definitions of each and every component are given as follows.

$$AC = (OB, PB, Oprs) \tag{1}$$

$$OB = \{ONT \mid ONT = SO \lor OO \lor AO\} \tag{2}$$

$$AB = \{(s, o, \pm a) \mid s \in SO \land o \in OO \land a \in AO\} \tag{3}$$

$$Oprs = (CA, grant, revoke) \tag{4}$$

$$CA(s,o,a) = \left\{ \begin{array}{l} True \mid (s,o,a) \in PB \lor (\exists (s_i, o_j, +a_k) \\ \in PB : (s_i, o_j, +a_k) \rightarrow (s,o,a)) \\ False, Otherwise \end{array} \right\} \tag{5}$$

The algorithm for checking the access request is given below:

```
function AccessRequest(s, o, a) returns ACCESS_DECISION

Inputs
    s is a concept/individual/property in SO
    o is a concept/individual/property in OO
    a is a concept/individual/property in AO

Static
ONTBASE ← repository of ontologies of each access control elements(SO, OO, AO)
POLBASE ← repository of authorization rules
REDONT ← Reduced Set of Ontologies
1. ACCESS_RESPONSE = false;
2. ACCESS_DECISION = no;
3. REDONT ← REDUCE (ONTBASE);
4. While there are entities to parse in REDONT and
   ACCESS_RESPONSE is false to do
5.  if the policy is valid then
6.  rule ← read the rule from POLBASE;
7.  if rule matches act then
8.  ACCESS_RESPONSE = true;
```

```
9.  else
10. ACCESS_RESPONSE = false;
11. end if
12. end if
13. End while
14. if  ACCESS_RESPONSE = true then
15. ACCESS_DECISION = yes;
16. else
17. ACCESS_DECISION = no;
18. endif
19. return ACCESS_DECISON;
```

The workflow of our model depicted in Fig. 2 is explained by this algorithm. The algorithm takes three inputs namely s, o, a. s is an entity from subject ontology(SO), o is an entity from object ontology(OO), and a is an entity from action ontology(OO). These ontologies are stored in Ontology base(ONTBASE). Line 3 tells that each ontology is reduced by applying another algorithm to REDUCE(ONTBASE). Subsumption property is implemented through this algorithm and it is the key factor in our work. From line 4-13 ACCESS_RESPONSE is computed. Retrieve the rule from the policy base (POLBASE) [line 6]. If action entity (a) in inferred access request matches the rule (Line 7), then ACCESS_RESPONSE is true (Line 8), else it is false. If ACCESS_RESPONSE is true then ACESS_DECISON is yes which means that access is granted, else access is denied. And the function returns ACESS_DECISON.

Algorithm for reduce function is given below:

```
Function REDUCE(ONTBASE) returns REDONT
{A,B,C,D,…} ← Concepts of Ontologies
{p1,p2,…pn} ← Properties of Ontologies
1. REDONT ← empty;
2. For all the concepts, properties and individuals
   do
    3. if B is a subclass of A then
    4. REDONT ← B reduces to A
    5. elseif A is equivalent to B then
6. REDONT ← A reduces to B and B reduces
       to A
7. else if A is the union of A1,  A2, … An,
       then
8. REDONT ← A1, A2, … An, Reduces to A
9. else if and B is an individual then
10. REDONT ← A is the same as B
11. else
12. REDONT ← empty
13. endif
14. endfor
15. return REDONT
```

The reduction algorithm is applied to all concepts, individuals and properties. If A and B are concepts and if B is a subclass of A, then it’s enough to handle concept A alone, thereby concepts get reduced (line 3-4). If there is an axiom stating that A is equivalent to B, then we can use either concept A or concept B (line 5-6). If concept A is a union of A1, A2, ... An, then A1, A2, … An gets reduced to A(Line 7-8). If A and B are individuals, the A is the same as B and hence ontology is reduced (Line 9-10). If nothing exists, then reduced ontology is empty.

4. Security analysis

The proposed system ensures efficient and better access control over data stored in the cloud. Each user can access the data if and only if their request matches with the access policy stored in the policy base. Since OWL language is used to model the security domains of access control, the inference process is automated and it considers strong semantic interrelationship among concepts, properties and individuals.

4.1 Theorem 1

If A and B are concepts, then it results in a new concept with implicit authorization.

Proof:

Let A and B be concepts. By reducing to the problem of subsumption, if A and B are concepts and A subsumes B, then the rule applied to concept A is also applicable for concept B without any additional rule.

The concept of credit card is defined as the union of the master card and visa card. The access rights such as eligibility of owner to check account details will be publicized to both owners of the master and owner of a visa card. Without adding an explicit rule for the visa card, this can be enforced on master card.

4.2 Theorem 2

If A is an individual and B is a concept, then rule on B is also enforced on A.

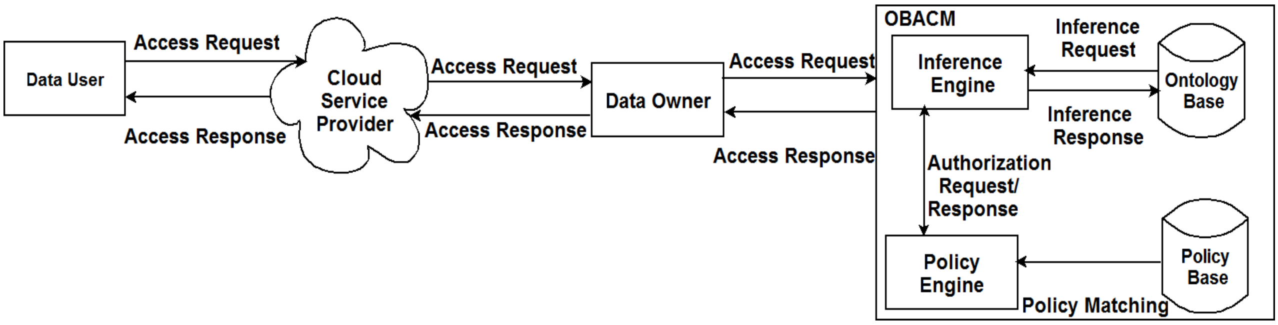

Figure. 1 Our proposed architecture of ontology-based access control model (OBACM)

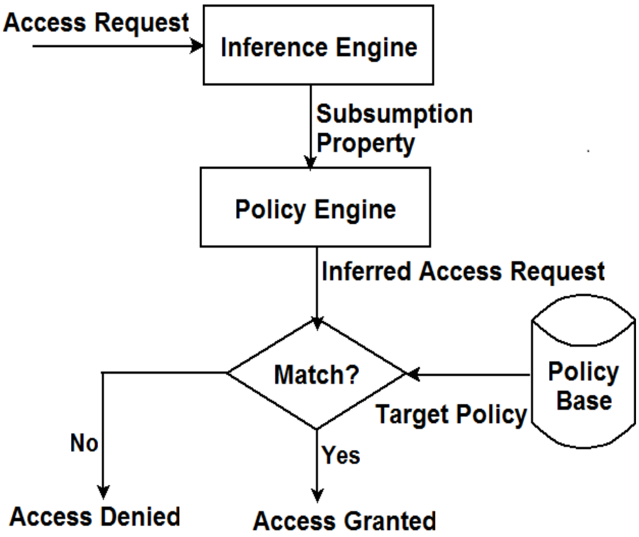

Figure. 2 Workflow of the model

Proof:

Let B be a concept and A be an individual. By reducing the problem to subsumption, there exists a relationship between A and B, i.e., A is an individual that belongs to a concept B. Since every individual derives the access rights on the concept they are belonging to, the rules enforced on B can also be enforced on A. The propagation of access rights is from subsume to subsume in the domains of subjects and objects.

Example:

Consider the subject domain, if s_i and s_j are concepts and let s_j subsumes s_i, then a new rule can be derived from s_i to s_j denoted by

$$(s_i, o, \pm a) \rightarrow (s_j, o, +a) \tag{6}$$

Consider the object domain, if o_i and o_j are concepts and let o_j subsume o_i. then a new rule can be derived from o_i to o_j denoted by

$$(s, o_{i,} \pm a) \rightarrow (s, o_j, +a) \tag{7}$$

The Propagation of access rights in the action domain is different. The subsumee cannot have a positive right when the subsumer doesn't have it.
Consider the action domain, If a_i and a_j are concepts and let a_j subsumes a_i, then a new rule is derived from a_j to a_i denoted by

$$(s, o, -a_j) \rightarrow (s, o, -a_i) \tag{8}$$

If the subsumee has the positive right, then the subsumer should also have it.
If a_i and a_j are the entities of the activation domain and let a_j subsumes a_i, then a new rule is derived from a_i to a_j denoted by

$$(s, o, +a_i) \rightarrow (s, o, +a_j) \tag{9}$$

4.3 Theorem 3

If there exists a semantic relationship between various properties, then new properties which are not explicitly mentioned in an ontology can be derived.

Proof:

The subject ontology inference is considered. Two properties namely Register_in and Issued_in are defined. Using these two properties, we can derive a new property supported by

Example:

When the authority of a bank needs to prevent the master cards supported by Banks of the USA from resolving money in a special account. It can do this by having knowledge of two properties Issued_in and Registerd_in.

$$Registered\_in(Bank_X, USA) \wedge Issued\_in(Mastercard, Bank_X) \rightarrow Supported\_by(Mastercard, USA) \tag{10}$$

This results in a new implicit authorization rule as given below in Eq. (11).

$$(USA, Mastercards, Account_X, -Settlement) \tag{11}$$

Here - indicates negative access right.

4.4 Theorem 4

If A and B are individuals, the rules defined for A is also applicable for B.

Proof:

Let A and B be individuals. The subsumption property “same as” axioms states that the two individuals are equal semantically and hence rule on anyone is applicable to another.

Thus we try to ensure that reducing inference problem to subsumption problem makes it possible to derive new rules and properties implicitly. This enables the data owner to have the strongest access control over the data stored in the cloud in addition to the mechanism provided by cloud service providers.

5. Experimental analysis

We carried our experiments using windows 8(32 bit) OS with I-5 CPU, 4GB RAM and 500GB hard disk drive. We implemented the algorithms using Java and used protégé tool to create ontology and OWL API to handle the ontologies. The comparison is done between our work and existing systems [15-19].

Generality: Starting with the creation of ontologies, we have chosen the domain of knowledge as banking [29]. Subject ontology is created in terms of credentials which are universally accepted for user authentication. Object ontology is expressed in terms of services and is identified by their URI in Access control rules. Action ontology is expressed in terms of general actions on the bank web services. Thus, it provides generality and is encouraged by the heterogeneous users of cloud. The existing systems which use ontology concept lack in their generality.

Space Efficiency: We used a parameter namely concept count indicating a number of atomic concepts. The following Table 1 and Fig. 3 show the number of statements in reduced and standard ontologies. The existing works using ontologies for access control have not utilized the reduction to subsumption algorithm; hence the number of statements to express the rule and no of rules stored in Policy Base is more than our proposed work. In our work, after applying the reduction algorithm, the number of statements gets reduced. It is enough to work with smaller ontologies and hence it requires lower space complexity. It is not necessary to store all the access control rules explicitly because of implicit authorization. Refer to the example given in Theorem 3 in section 4.3. Thereby the time taken to retrieve the target policy is also reduced.

Fig. 3 exhibits a comparison of a number of statements needed to express a rule in standard ontologies of existing works [15-19] and our proposed system. The number of concepts is ranged from 100 to 5000 in the x-axis and the number of statements is ranged from 2000 to 18000 in the y-axis. As the number of concepts increases, the number of statements also increases. However, the increase is considerably less in our proposed work.

Table 1. Comparison on Number of Statements in Standard And Reduced Ontologies

Concept count	**Statements of standard ontology**	**Statements of reduced ontology**
100	390	239
500	3158	1825
1000	3600	2300
5000	16194	10593

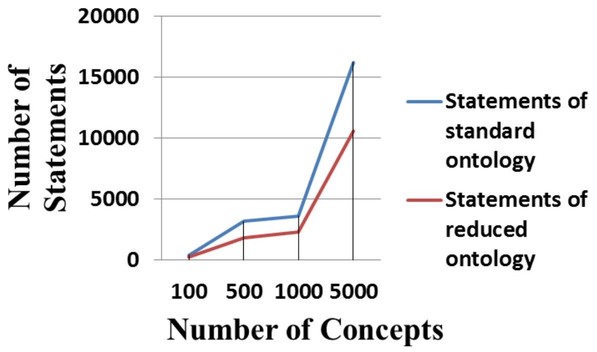

Figure. 3 Comparison of the number of statements in standard and reduced ontologies

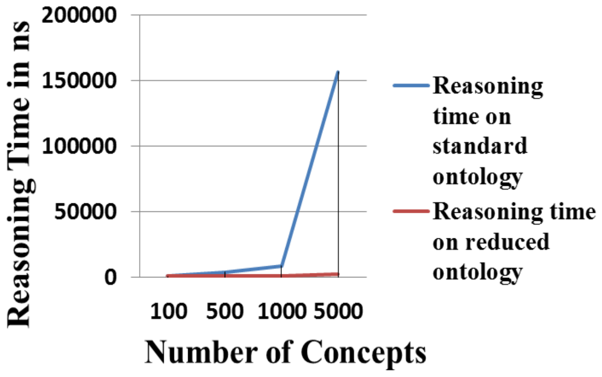

Figure. 4 Comparisons of reasoning time on standard and reduced ontologies

Table 2. Comparison of reasoning time on standard and reduced ontologies

Concept count	Reasoning time on standard ontology	Reasoning time on reduced ontology
100	969	843
500	3938	1141
1000	8751	1219
5000	186687	2204

Response Time: Time complexity of the decision-making system using ontology depends on the reasoning part. Since we have exploited subsumption property, the reasoning problem is reduced to the subsumption problem. Because of the highly efficient subsumption reasoner, the response time of our work is very much promising. For computing the reasoning time we have done an experiment using FACT++ reasoner for reasoning standard ontologies. Since reduced ontologies include only the subsumption relation between concepts, individuals and properties, we used our own reasoning engine that can only handle subsumption relation in a better period of time compared with reasoner such as PELLET, FACT++, etc.

Table 2 and Fig. 4 show a comparison of reasoning time on standard ontology and reduced ontology. As we refer to Table 2, decision making is done in a shorter period which is the most mandatory factor in the cloud.

National Institute of Standards and Technology (NIST) has facilitated many access control evaluation metrics [30]. We have chosen some among them namely ease of privilege assignments, least privilege support, separation of duty, Delegation of administrative capabilities, Flexibility of configuration into existing systems, the horizontal scope, vertical scope, conflict resolution, and evaluated our system with state of art [15-19].

Ease of Privilege Assignments: The steps vital for assigning, altering, and clearing subjects, privileges, or capacities inside the framework is essential to the ease of use of an AC framework. More the number of steps are prerequisite then, more mix-ups that can be made because of either human or framework blunders. Fewer steps require less turnaround time for man-machine communication. To evaluate the metric, the following queries must be answered. How many steps are required for assigning, changing and removing a privilege? How many steps are required for assigning, changing, and removing capability for a subject? How many steps are needed for assigning subject group and group relations? How many steps are needed for assigning object group and group relations? Thus there are 9 questions to be answered. Fig. 5 exhibits a comparison of our proposed work and existing works based on the answers given for these queries. The metric value ranges from 0 to 100 in the y-axis. If a question is answered by any of the works, then we award 10 points. If it answers partially 5 points are awarded, else 0. The system got 80 points since it answers 8 questions out of 9. And the rest is shown in Fig. 3.

Least privilege principle support: Each subject and process ought to have a minimal set of benefits expected to perform the task needing to be done. The usage of this standard has the impact of constraining harm that can result from system blunder or malicious events. The model provides a promising result to this metric and is shown in Fig. 6. Is the access control mechanism capable of imposing the least privilege principle? Does the access control system let agreeing least privilege via restrictions? Does the access control system allow us to specify the least privilege via other specifications? Our work gets 30 points since it

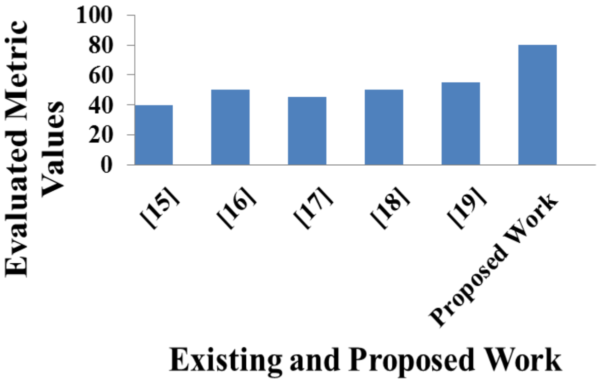

Figure. 5 Comparison of the evaluated metric values between proposed and existing works

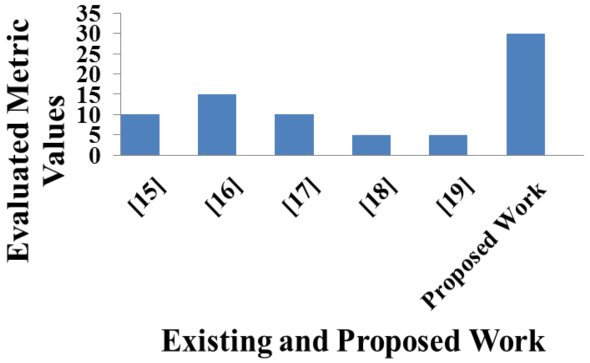

Figure. 6 Comparison of the evaluated metric values between proposed and existing works

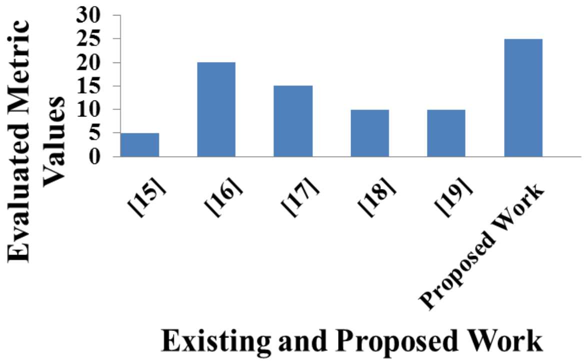

Figure. 7 Comparison of the evaluated metric values between proposed and existing works

answers all the questions which are more than the other existing works.

Separation of Duty (SoD): The following metric items are to be evaluated for this metric. Is the AC framework fit for indicating Static SoD rules? Is the AC framework fit for indicating Dynamic SoD rules? Is the AC framework equipped for determining Historical SoD rules? Our work answers the first two questions fully and the third question partially and got 25 points and the rest is shown in Fig. 7.

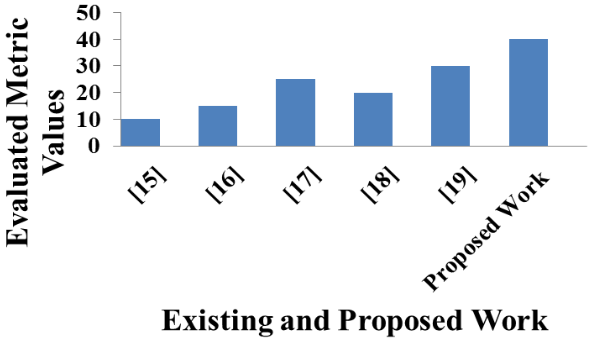

Figure. 8 Comparison of the evaluated metric values between proposed and existing works

The flexibility of configuration into existing systems: Following are the metric items to be evaluated for this metric: Is the AC component authorized by the working system? Is the AC instrument upheld by a microkernel? Is the AC implemented by applications? Is the AC implemented by a customer/server correspondence convention? Our work answers all these evaluation questions and gets 40 points which are promising than the existing works. This is shown in Fig. 8.

Horizontal and vertical scope: Does the AC framework encourage just a solitary host? Does the AC framework encourage numerous hosts by means of the network? Does the AC framework encourage virtual communities? Does the scope of information control cover applications? Does the scope of information control cover files? Does the scope of information control cover database records? Does the scope of information control cover the fields of database records? Does the scope of data control cover network devices? These are the metric items to be evaluated and our work answers 6 questions and got 60 points which are shown in Fig. 9.

Conflict Resolution: Is the AC framework equipped for forestalling policy conflicts? Is the AC framework fit for settling struggle strategy rules? Is the AC framework fit for averting clashes? Is the AC framework fit for settling? Our works provide comparatively good answers but not the best and they are shown in Fig. 10. Hence we decided to do improve the mechanism in future work. Comparing to the state-of-art, our model reduces the times of agreement, achieves heterogeneity, reduces reasoning time and rules to be stored in Policy Base and thus providing 85-90% efficient privacy-preserving access control for cloud data.

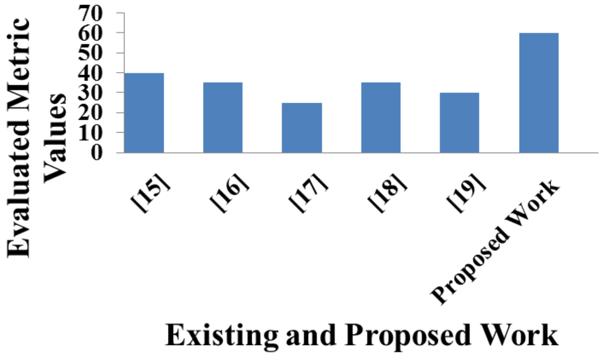

Figure. 9 Comparison of the evaluated metric values between proposed and existing works

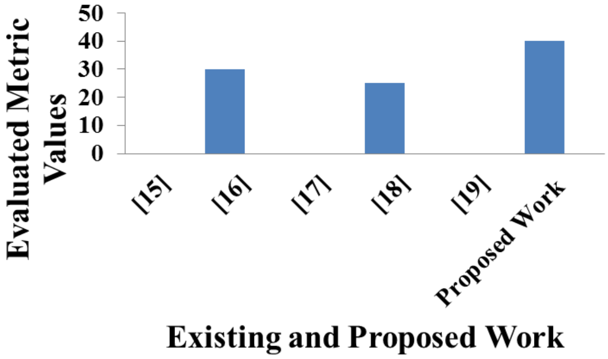

Figure.10 Comparison of the evaluated metric values between proposed and existing works

6. Conclusion

In this paper, an efficient access control model for protecting cloud data has been proposed. This model considers semantic interrelationships among domains of access control. Subsumption property is exploited among concepts, properties and individuals of ontology, resulting in the reduced ontology. Reduced ontology yields many advantages. The reasoning time in reduced ontology is much lesser when compared with the reasoning time in standard ontologies. This is experimented by doing reasoning using our reasoner and comparing it with reasoning time with FACT++ and PELLET reasoner. Moreover, the space required to store the rules is also reduced as implicit authorization rules and properties are derived using reduced ontology. Thus there is no need to save all the rules explicitly on the policy base. Our work answers many access control evaluations query facilitated by National Institute of Standards and Technology and hence proven to be 85-90% more efficient than the other works in state-of-art.

The security and experimental analysis show that the improved performance of this model makes it efficient for the cloud. We have planned to evaluate our work with more access control metrics in our future work and try to make it more dynamic by including ontology for capturing contexts and use it for even more effective access control.

References

[1] N. Khan and A. Al-Yasiri, “Identifying Cloud Security Threats to Strengthen Cloud Computing Adoption Framework”, In: *Proc. of the 2nd International Workshop on Internet of Thing: Networking Applications and Technologies*, Vol.94, pp.485–490, 2016.

[2] CSA: “CSA Releases Top Threats to Cloud Computing: Deep Dive”, *https://www.prnewswire.com/news-releases/csa-releases-top-threats-to-cloud-computing-deep-dive-300693803.html*, 2018.

[3] G. Priya, B. R. Kavitha, G. Ramya, P. Kumaresan, and F. A. Mon, “An Access Control Models In Cloud Computing: A Review”, *International Journal of Pure and Applied Mathematics*, Vol. 116, No. 24, pp.539-548, 2017.

[4] D. A. B. Fernandes, L. F. B. Soares, J. V. Gomes, M. M. Freire, and P. R. M. Inacio, “Security Issues in Cloud Environments—A Survey”, *International Journal of Information Security*, Vol. 13, No. 2, pp.113-170, 2014.

[5] K. Hashizume, D. G. Rosado, E. Fernández-Medina, and E. B. Fernandez, “An analysis of security issues for cloud computing”, *Springer Open Journal of Internet Services and Applications*, Vol. 4, No. 5, 2013.

[6] M. E. Rana, M. Kubbo, and M. Jayabalan, “Privacy and Security challenges Towards Cloud-Based Access Control in Electronic Health Records”, *Asian Journal of Information Technology*, Vol. 16, No. 2, pp.274–281, 2017.

[7] L. Hu, S. Ying, X. Jia, and K. Zhao, “Towards an Approach of Semantic Access Control for Cloud Computing”, *LNCS, Springer-Verlag Berlin Heidelberg*, Vol. 5931, pp.145–156, 2009.

[8] S. Khamadja, K. Adi, and L. Logrippo, “Designing Flexible Access Control Models for the Cloud”, In: *Proc. of 6th International Conf. on Security of Information and Networks*, pp.225-232, 2013.

[9] Y. J. Hu, W. N. Wu, and J. J. Yang, “Semantics-enabled Policies for Super-Peer

Data Integration and Protection”, *International Journal of Computer Science and Applications*, Vol. 9, No. 1, pp.23–49, 2012.

[10] L. A. Fratila, R. D. Zota, and R. Constantinescu, “An Analysis of the Romanian Internet Banking Market from the Perspective of Cloud Computing Services”, In: *Proc. of International Economic Conf. of Sibiu 2013 Post Crisis Economy: Challenges and Opportunities, Science Direct*, Vol. 6, pp.770–775, 2013.

[11] N. A. Hamidi, G. K. M. Rahimi, A. Nafarieh, A. Hamidi, and B. Robertson, “Personalized Security Approaches in E-Banking Employing Flask Architecture over Cloud Environment”, In: *Proceedia of Computer Science, 4th International Conf. on Emerging Ubiquitous Systems and Pervasive Networks, Science Direct*, Vol. 21, pp.18-24, 2013.

[12] B. Nedelcu, M. E. Stefanet, I. F. Tamasescu, S. E. Tintoiu, and A. Vezeanu, “Cloud Computing and its Challenges and Benefits in the Bank System”, *Database Systems Journal*, Vol. 6, No. 1, pp.44-58, 2015.

[13] N. W. Lo, T. C. Yang, and M. H. Guo, “An Attribute-Role Based Access Control Mechanism for Multi-tenancy Cloud Environment”, *Wireless Personal Communic ations: An International Journal*, Vol. 84, No. 3, pp.2119-2134, 2015.

[14] M. Tebaa, K. Zkik, and S. E. Hajji, “Hybrid Homomorphic Encryption Method for Protecting the Privacy of Banking Data in the Cloud”, *International Journal of Security and its Applications*, Vol. 9, No. 6, pp.61-70, 2015.

[15] C. Choi, J. Choi, and P. Kim, “Ontology-based access control model for security policy reasoning in cloud computing”, *The Journal of Super Computing*, Vol. 67, No. 3, pp.711-722, 2014

[16] C. L. Liu, “Cloud Service Access Control System Based on Ontologies”, *Advances in Engineering Software, Elsevier*, Vol. 69, pp.26-36, 2014.

[17] H. Sun, X. Zhang, and C. Gu, “Role-based Access Control Using Ontology in Cloud Storage”, *International Journal of Grid and Distribution Computing*, Vol. 7, No. 3, pp.1-12, 2014.

[18] J. M. M. P´erez, G. M. P´erez, and A. F. S. G´omez, “SecRBAC: Secure data in the Clouds”, *IEEE Transactions on Services Computing*, Vol. 10, No. 5, pp.726-740, 2016.

[19] R. Kalaiprasath, R. Elankavi, and R. Udayakumar”, Cloud Security and Compliance –A Semantic Approach in End to End Security”, *International Journal of Mechanical Engineering and Technology*, Vol. 8, No. 5, pp. 987–994, 2017.

[20] B. Duraisamy and S. Muthukrishnan, “IDOCA and ODOCA - Enhanced Technique for Secured Cloud Data Storage”, *International Journal of Intelligent Engineering and Systems*, Vol. 10, No. 6, pp.49-59, 2017.

[21] P. Choudhary and J. Natarajan, “Secure Access Control with Dynamic Policy Updating for the Data in Cloud System”, *International Journal of Intelligent Engineering and System*, Vol. 10, No. 3, pp.136-145, 2017.

[22] N. Geetha and M. S. Anbarasi, “Enhanced-Role Based Access Control (E-RBAC) with Trust Factor for Cloud Software-as-a-Service Paradigm”, *International Journal of Computer Sciences and Engineering*, Vol. 6, No. 5, pp.616-621, 2018.

[23] Z. Fan, Y. Xiao, C. Wang, and B. Liu, “Research on Access Control in Cloud Storage System: From Single to Multi-Clouds”, *American Journal of Software Engineering and Applications*”, Vol. 7, No. 1, pp.1-14, 2018.

[24] F. F. Moghaddam, P. Wieder, and R.Yahyapour, “Policy Management Engine (PME): A Policy-Based Schema to Classify and Manage Sensitive Data in Cloud Storages”, *Journal of Information Security and Applications*, Vol. 36, pp.11-19, 2017.

[25] Y. Verginadis, A. Michalas, P. Gouvas, G. Schiefer, G. Hubsch, and I. Paraskakis, “PaaSword: A Holistic Data Privacy and Security by Design Framework for Cloud Services”, *Journal of Grid Computing*, Vol. 15, No. 2, pp.219–234, 2017.

[26] M. Qiu, K. Gai, B. Thuraisingham, L. Tao, and H. Zhao, “Proactive user-centric secure data scheme using attribute-based semantic access controls for mobile clouds in the financial industry”, *Future Generation Computer Systems*, Vol. 80, pp.421-429, 2018.

[27] S. Namasudra and P. Roy, “PpBAC: Popularity Based Access Control Model for Cloud Computing”, *Journal of Organizational and End User Computing*, Vol. 30, No. 4, pp.14-31, 2018.

[28] L. Ma, L. Tao, K. Gai, and Y. Zhong, “A novel social network access control model using logical authorization language in cloud computing”, *Concurrency and Computation Practice and Experience: Special issue on Big data security and intelligent data in clouds*, Vol. 29, No. 14, 2017.

[29] M. Auxilia and K. Raja, “Ontology Centric Access Control Mechanism for Enabling Data Protection in Cloud”, *Indian Journal of Science and Technology*, Vol. 9, No. 23, pp.1-7, 2016.

[30] V. C. Hu and K. Scarfone, “Guidelines for Access Control System Evaluation Metrics”, *NISTIR 7874, National Institute of Standards and Technology, US Department of Commerce,* http://dx.doi.org/10.6028/NIST.IR.7874, 2012.