Attribute Based Access Control with Trust Calculation (ABAC-T) for Decision Policies of Health Care in Pervasive Environment

Abirami G, Revathi Venkataraman

Abstract: Attribute Based Access Control (ABAC) provides a high degree of security in access control mechanisms. Since ABAC is a fine-grained access control, it is being used wider in network security. In this paper, we have proposed an ABAC to emphasis access mechanism in pervasive computing for providing authorization to access resources which is in dynamic. The pervasive computing provides contextual information that is used as one of the attributes in ABAC to improve protection in a specific context. Moreover, ABAC is working based on the rich set of attributes to make an authorization decision more effective. To improve more on secured access privilege of users, the trust is included as one of the attributes in a subject that, provides access control in the dynamic environment. Due to the inclusion of trust, it provides flexibility and scalability in enforcing security policy. To provide access privilege to the user in a time-critical situation the trust value is calculated.

Index Terms: Attribute Based Access Control, Pervasive computing, Trust, Ubiquitous.

I. INTRODUCTION

To provide security in traditional network user authentication and access control are sufficient. But in the pervasive computing environment, this traditional technique is not suitable to provide complete security to the network resources. Since mobile users in a pervasive environment may need access to local services and resources anytime and anywhere. Therefore, we have proposed Attribute-based access control with trust to assign policy for access objects or resources in such a context.The pervasive computing environment may be ad-hoc, wireless, mobile computing and artificial intelligent and this policy make all devices to cooperate, coordinate and interacts with each other and integrated with its service [1]. In these areas' confidentiality, integrity and availability and access control of data must be ensured. Confidentiality provides that the protected data is shared only with the right users. The integrity of data ensures that only authorized user can modify it and availability supports that the requirement of data is available only to the authorized user. Access control provides authorization to the user by limiting the access rights to the resources.

Also, pervasive computing system consists of an intelligent interacting component in the smart environment. Hence, it requires the devices in this environment by facilitating with dynamic rights such as access control to resources anytime and allow to modify the access rights to the third party or delegator. The delegation of access rights is based on some principles that trust. The access rights can be unified with any devices, as well as users. The delegation of access rights is strongly computed on trust level or degree of the user or any devices. The authorization of users is provided through access control mechanism; there are various access control mechanisms such as mandatory access control which gives access according to the manager or administrator that is applicable for only government and military service and not extensible. Discretionary access control is based on an identity of the users, and applicable only for commercial, and Role-based access control, is based on role of an organization but not obtain any context information. Also, these traditional models are working only for the static and centralized system. In context based access control model, the access is provided to resource owners and administrators according to resources location. They have defined access policies completely based on context [2]. Context is one of the attributes in ABAC for access privilege. Hence Attribute-based access control (ABAC) reduces the gap such that it works for dynamic and distributed computing. Moreover, it is flexible and adapts to context information as the attribute for decision making. Hence in this paper, we have proposed an ABAC access control with trust to provide dynamic rights. The paper is structured as follows. We have explored a related work in section II. Section III includes about attribute based access control. Section IV consists of incorporating trust in ABAC and implemented in healthcare applications. Finally, in section V we have given conclusion by adding trust as an attribute in ABAC.

II. RELATED WORK

The concepts of attribute transformation for ABAC are proposed in [3], the attribute values were reduced to a smaller set of values. For that, they have introduced new authorization policies. But some issues such as conflicts due to multiple mapping had been encountered. A semantic-aware attribute-based access control model (SABAC) [4] used web ontology language to represent the attribute of resources and used XACML as the policy language to provide privacy of the data they used shibboleth. The ABAC had used in Fast health interoperability service (FHIS) for an authorization decision using attributes [5].

Revised Manuscript Received on May 06, 2019

Abirami G, Department of Computer Science and Engineering, SRM Institute of Science and Technology, Chennai, India.

Revathi Venkataraman, Department of Computer Science and Engineering, SRM Institute of Science and Technology, Chennai, India.

The working principles and benefits of the ABAC model [6] have explored and provided how the information is shared among different organizations. The trust-based access control in pervasive computing is proposed and TrustAC[7][8] could be deployed on any devices. They have used XACML for policies generation and implemented in all PDAs. In pervasive computing, trust management is implemented using a support vector machine (SVM) and fuzzy logic system, with SVM, optimal trust values had been calculated. Trust management schemes [9] in a decentralized network consists of various ranges of recommended trust values and reputation trust values. An access control mechanism [10] in a ubiquitous environment was designed and introducing trust in finer-grained access control to provide control of sensitive resources. Based on the trust value calculation, the access to protected resources is provided. To improve the security performance, trust management is used for the cross domain access control model. This model [11] expanded the XACML with inside trust management pointer (ITMP) and outside trust management pointer (OTMP). Also, it provided finer grained and dynamic authorization in an easy way.

Trust is an important factor in internet services [12]. This is calculated by means of reputation and dynamic trust values are incremented and decremented with mathematical formulae. The trust theory and community are formulated and proposed a novel trust based system like trust computation and management system (TOMS) [13]. TOMS established the trust relationship between distributed nodes. This system is used in a dynamic environment like a mobile and wireless sensor. The characteristics of reputation and trust computational model had discussed [14], also the probabilistic mechanism of trust calculation and relationship between trusts, reputation and reciprocity have been devised on eBay. In [15] the formal definition of trust had been postulated for pervasive and distributed environment. Trust description, trust evaluations are established and included. Thereby, the trust provides a way of security in ABAC model and it is being more beneficial methods to implement in a various research area.

III. ATTRIBUTE BASED ACCESS CONTROL (ABAC)

The traditional access control model such as Discretionary Access Control (DAC), Mandatory Access Control (MAC) and Role Based Access Control (RBAC) [16] are restricted due to its less security measure in the flexible and dynamic environment like pervasive computing. Also, these access control models are working based on identity, role or group assigned to users which has insufficient details to express the real world access control policies. Hence the access request of user or system is granted or denied based on arbitrary attributes of the users, objects and environments and so-called Attribute Based Access Control (ABAC).ABAC model provides secured information sharing between any enterprises because of its fine-grained policy. ABAC provides grant permission on the evaluation of attributes for a environment. Attributes are characteristics or properties of any entity, such as subject, object, and environment.• Subject: The entity that requests permission to access specific resources. It may be human or any devices. Subject attributes: Name of the person, id number, any type of devices, address etc. Attributes are represented by ATTRI.

$$ATTRIs = \{As1, As2, As3 \dots, Asi - 1, Asi\} \quad (1)$$

- Object: Any resource type that would be protected from unauthorized access and the subject is able to perform an operation on it. Example of any device or files etc. Object attributes: Any type of e-files, any type of devices etc.

$$ATTRIo = \{Ao1, Ao2, Ao3 \dots Aoi - 1, Aoi\} \quad (2)$$

- Environment: Context with which the operation can be done on an object by the subject. Environment attributes: Location, time, duration etc. Attributes of an environment are represented the same as the subject.

$$ATTRIe = \{Ae1, Ae2, Ae3 \dots Aei - 1, Aei\} \quad (3)$$

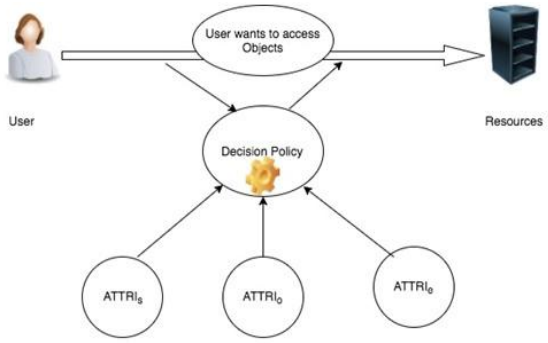

Fig. 1. ABAC policy model

In ABAC, access decision can be made by simply altering the attribute values without changing subject and object relationships. Also, ABAC provides object administrator to use access control policy without the advance knowledge of the subjects. The benefits of ABAC is when the new subject is joining the organization the rules of object accessed do not require to be modified. Here the authorization is the act of verifying the subject behavior and policy can be a rule or access privileges of a subject. The access control mechanism should be composed of authorization information that has the object being protected, the subject seeking access and the policies provide control over to access the resources and any contextual information required to build a decision. Fig. 1 shows access control decision policy based on subject, object and environment attribute. The user request for accessing resources is to be granted or denied according to the policy decision. The user is granted access only after their credential verified and fulfilled the decision policy. The decision policy engine is checking with attributes of users, the resources they required to access, context information, and policy repository for providing rights to access resources or any objects.

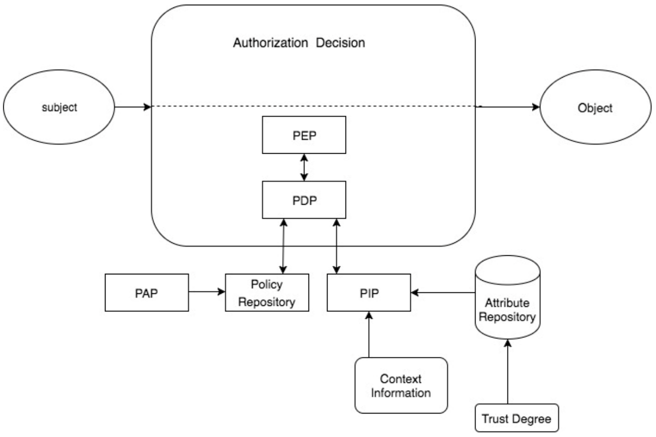

Fig. 2. Access control mechanism using ABAC and Trust Value

In this ABAC model, the decision is made in access control mechanism by the task of four functional components such as Policy Enforcement Point (PEP), Policy Decision Point (PDP), Policy Information Point (PIP), and Policy Administration Point (PAP). The PIP consists of attributes of all entities such as subject, object, and environment. The PIP provides attribute information to PDP for computing access decision. The policy administrator is used to debug Digital Policy (DP) which is an access control rules that directly executed by a machine. The Meta policies (MP) is the policy about policies to manage the DP. PEP enforces policy decision according to the request of a subject for accessing secured objects. We have provided how ABAC mechanism is working in pervasive computing with trust as attributes. In Fig. 2 the policy enforcement is based on attributes of the subject, object, context and trust, hence, to provide access rights in the dynamic environment. Trust degree of the subject is reserved in repository and PIP has confirmed the attributes for each policy according to a policy decision point.

IV. INCORPORATING TRUST IN ABAC

The pervasive or ubiquitous computing provides services to the user "anywhere", "anytime". So, in this environment, much of the sensitive information is to be protected and give restricted access to private resources. Therefore, it requires a suitable access control mechanism for providing security in the ubiquitous environment. Furthermore, the user, access privileges change dynamically with respect to the data requirement. We have introduced trust in ABAC to provide fine-grained access to restricted resources or services. The access request is being granted based on the subject trust level. Trust means the truth, strengthen, belief and goodness of a person or non-person according to their behavior in a context. The trust level can be evaluated from the past history and peer recommendation of the trustee. Hence, the requester is being permitted or blocked to get access to the services according to their trust level.

A. Calculating Trust level

We have taken, Trust value as,

$$[Trust(1,0)\in\{ATTRIs\}] \wedge ATTRIe \wedge ATTRIo \Rightarrow \text{Decision policy} \quad (4)$$

Trust decisions are made by recommender who is more reliable and assurance person like a higher authority or according to their role and task assigned to them can render a positive recommendation about on trustees and '1' is fully trusted and value '0' is complete distrust. The representation of trust calculation is given as, where 'P_Re' is a positive recommendation value and 'P_Rp' is the positive reputation value of 'i' entity and Ni is trust toward negative recommendation and reputation value Therefore, trust values have calculated based on the reputation of the trustee and recommendation by the peer devices or entity. Fig. 3 shows the threshold values, which is taken as an average of initial trust value (ITV) and reputation value (Rp) of the subject that is 0.5, based on weight index sigma (σ). The value that is greater than threshold should be considered as trusted value for an entity, and less than the threshold is taken as distrust value. The trusted and distrusted value can be calculated based on a positive and negative recommendation of trustor and reputation of trustees. The equation (4) gives the value '1' or '0' as trust value for user (U) attributes, object (O) attributes, and environment (E) attributes are included to write decision policies. The equation (5) provides threshold value by calculating the average weight of initial trust value and reputation value by the way the threshold value (Thr) is being computed in equation (6). The equation (7), provides 'α' value which is a positive recommendation about the entity given by recommender and, the reputation is being calculated according to the behavior of trustees. The 'β' refers to (8) is positive reputation and it is a direct observation compare with history, so it would be increased or decreased according to context and the 'γ' refer to (9) represents the negative approach about the entity. The equation (10) shows the trust value according to the positive approach and negative approach that is greater than the threshold value 0.5. Also, if the conditions are satisfied which means if it is beyond the threshold value is 0.5 then the entity is in trust degree if not, it is distrust.

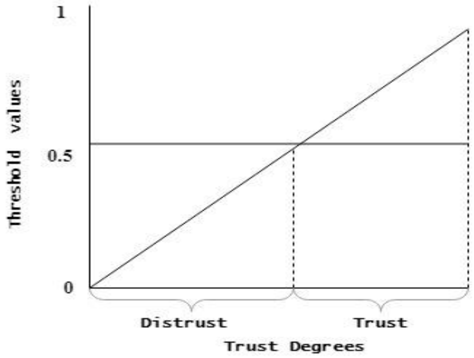

Fig. 3. Trust degree

$$Thr = Avg[\sigma.ITL(S) + (1-\sigma).Rp(S)] \quad (5)$$

$$0 \leq Thr \leq 1 \quad (6)$$

$$\alpha = \sum_{i=1}^{n} P\_Re_i \quad (7)$$

$$\beta = \sum_{j=1}^{n} P\_Rp_j \quad (8)$$

$$\gamma = \sum_{k=1}^{n} N(Re + Rp)_k \quad (9)$$

$$\alpha + \beta - \gamma \geq \text{Threshold value} \quad (10)$$

In the distributed environment, the positive recommendation of peers, the reputation of past history and direct observation of subjects with respect to context and negative values of each factor are taken to find trust values. The Algorithm 1, compute the trust value for an entity such as subject, based on this value it would be trusted by the trustor. It will be included in the policy for given applications.

```
Algorithm FindTrustValue (x)
 // x is a an entity, its trust value is to be calculated
Input: $P\_Re_{i,}$  $P\_Rp_j$, Thr = 0.5
Output: 1) Trust 2) Distrust
Begin:
Set $\alpha=\beta=\gamma=\phi$;
Set x=0.0;
for i= 1 to n do
      $\alpha = \sum_{i=1}^{n} P\_Re_i$;
end for
for j=1 to n do
      $\beta = \sum_{j=1}^{n} P\_Rp_j$;
end for
for k=1 to n do
      $\gamma = \sum_{k=1}^{n} N(Re + Rp)_k$;
end for
$x = \alpha + \beta - \gamma$
if $x \geq$ Thr then
     return (trust)
else
   return (distrust)
end if
End
```

Fig. 4. Algorithm for finding Trust value for entity x.

B. ABAC in healthcare Application

Scenario: In health care, the patient blindly trusts the doctors for taking treatment. Therefore, the direct observation of the doctor may give trust degree that could be increased or decreased because of their liable work.

The attribute of each entity is considered to write a policy for decision making. The healthcare center for the pervasive environment could be protected by providing policy decision. Since every device is connected to the smart environment and the files of patient record could be accessible in a secure manner. Also, it provides who has rights to access these data or devices can be decided in accord with decision policy.

To provide accessible rights we propose a policy that includes the trust as one of the attributes that are calculated based on direct and indirect factors such as recommendation and reputations of peer entity. It has been implemented by using XACML policies that has flexible management and for dynamic policies decision. In table 1, some of the policies have given as for sample and the rights to grant or deny permissions are provided, also trust degree as one of the attributes for security. The trust value of subject has been calculated based on the algorithm in fig 4. the trust value '1' and distrust value '0' of the subject have provided using 'α', 'β', and 'γ' values. These policies show the subject's role and an object to be accessed in specific context is given, based on these rules if any person or entity satisfies the constraints. Then they will be granted or denied access the resources. The subjects are Doctors, Nurse, Administrator, Practitioner and Technician, also the resources to be accessed are patient_medical_report, patient_billing_information, patient_diagnosis_report and environment attribute is a hospital and the trust value be '0' or '1'. The scalability is improved by providing trust degree in an emergency case in a healthcare environment.

TABLE I
SAMPLE POLICIES FOR HEALTH CARE CENTER

Policies	Actions			
	R	W	U	D
Doctor A Є {Specialist ∧ patient_medical_report ∧ trust=1 ∧ hospital}	✓	✓	✓	✕
Doctor B Є {Specialist ∧ patient_medical_report ∧ trust=0 ∧ hospital}	✕	✕	✕	✕
Nurse Є {General ∧ patient_medical_report ∧ trust=1 ∧ hospital}	✓	✕	✕	✕
Practitioner Є {GeneralDoctor ∧ patient_medical_report ∧ trust=1 ∧ context=hospital}	✓	✓	✓	✕
Administrator Є {Manager A ∧ patient_billing_infor ∧ trust=1 ∧ context=hospital}	✓	✓	✓	✓
Administrator Є {Manager A ∧ patient_billing_infor ∧ trust=0 ∧ context=hospital}	✕	✕	✕	✕
Technician Є {Medical technician ∧ patient_billing_info ∧ trust=0 ∧ context=hospital}	✕	✕	✕	✕
Technician Є {Medical_technician ∧ patient_medical_report ∧ trust=0 ∧ context=hospital}	✕	✕	✕	✕
Technician Є {Medical_technician ∧ patient_diagnosis_report ∧ trust=1 ∧ context=hospital}	✓	✓	✓	✕

*R - Read, W - Write, U – Update, D – Delete

V. CONCLUSION

In this paper, we have introduced the trust incorporated ABAC policy model in pervasive computing. Evaluating the trust degree requires past history of information and direct observation of trustee. Also, it included the recommendation given by peer entities. Thus, the degree of trust level would be increased or decreased with respect to evaluated information. After evaluating the trust of each entity this is included as one of the attributes of the subject, and thus it addresses the challenges encountered in an access control mechanism. However, authorization of any subjects is guaranteed fully with their trust degree. Hence trust plays a vital role in the smart environment like pervasive computing. The access controls have applied to healthcare center for secure data sharing and accessing. We have given about policies on healthcare and implemented in XACML. Also, we can apply trust degree with ABAC mechanism in

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

research area such as Artificial Intelligence (AI). To diagnose a particular disease, the doctor has to trust the AI based on the tested values and frequency of diagnosis the disease accurately. By the way, trust has been incorporated in many such areas to provide flexibly accessing the resources.

ACKNOWLEDGEMENT

We would express our immense thanks to SRM Institute of Science and Technology for providing enough facilities for our requirement to do research work.

REFERENCES

1. HaukeVagts, Erik Krempel, "Yvonne Fischer. Access Controls for Privacy Protection in Pervasive Environments," *ACM.*, 2011.
2. Filho, J.B., Martin, H, "A generalized context-based access control model for pervasive environments", ACM Workshop on Security and Privacy in GIS and LBS, 2009.
3. Prosunjit Biswas, Ravi Sandhu, Ram Krishnan, "Attribute Transformation for Attribute Based Access Control," ACM., pp. 1-8, 2017.
4. Habit Shen, "A Semantic-Aware Attribute-Based Access Control Model for Web Services," *Springer.*, vol. 5574, pp. 693–703, 2009.
5. Subhojeet Mukherjee, Indrakshi Ray, Indrajit Ray, "Attribute Based Access Control for Healthcare Resources", ACM., pp. 29-40, 2017.
6. Vincent C. Hu, *et al.*, "Guide to Attribute Based Access Control (ABAC) Definition and considerations, NIST," pp.1-33, 2014.
7. Abubakar Sirageldin, Baharum Baharudin, Low Tang Jung, "Hybrid Scheme for Trust Management in Pervasive Computing", *IEEE.*, May 2012.
8. Florina Almenarez, *et al.*, "TrustAC: Trust-Based Access Control for Pervasive Devices", Springer., vol. 3450, pp. 225–238, 2005.
9. Huaizhi Li, MukeshSinghal, "Trust Management in Distributed Systems", *IEEE Computer Society.*, 2007.
10. Pho DucGiang, *et al.*, "A Flexible Trust-Based Access Control Mechanism for Security and Privacy Enhancement in Ubiquitous Systems", *IEEE.*, 2007.
11. YangXiaohui, Wang Hong, "A Cross-Domain Access Control Model Based on Trust Measurement", *Springer*, vol. 21, pp. 21-28,2016.
12. Bo Tian, Kecheng Liu, Yuanzhong Chen,"Dynamic Trust and Reputation Computation Model for B2C E-Commerce", *Future Internet.*, vol.7, pp.405-428,2015.
13. AzzedineBoukerche,Yonglin Ren, "A trust-based security system for ubiquitous and pervasive computing environment", *Elsevier.*,vol.31,pp.4343-4351,2008.
14. Lik Mui, MojdehMohtashemi, "A Computational Model of Trust and Reputation", *IEEE.*,2002.
15. DaoxiXiu ,Zhaoyu Liu, "A Formal Definition for Trust in Distributed Systems", *Spring verlag Berlin Heidelber*. Pp.482–489,2005.
16. Abirami.G, Dr. N. Revathi Venkataraman, "Access control policy on mobile operating system frameworks-Asurvey", *INDJST,* vol.9(48),2016.

AUTHORS PROFILE

G Abirami, is an Assistant Professor in Department of Computer Science and Engineering at SRMIST (formerly SRM University). She received her B.E. degree in Computer Science and Engineering from the Bharathidasan University, India, in 2003 and M.E degree from Annamalai University, India in 2008. She is pursuing the PhD degree in Access control mechanism at the Department of Computer Science and Engineering in SRM IST, India, She is a member of IET, ACM, and ISCA.

RevathiVenkataraman, is a Professor in Department of Computer Science and Engineering, SRMIST (formerly SRM University), India. She received her B.E. degree in Electronics and Communication Engineering from the University of Madras in 1994, and M.E. degrees in Computer Science and Engineering from University of Madras, India, in 2002 and the PhD degree in Trust Computing, from SRM Institute of Science and Technology(formerly SRM University), in 2012. She has published more than 20 journals, also she has got fund from DRDO for the project titled Implementation of algorithms for Trust and Replication in Mobile Ad-hoc Network, in 2009, again in 2012, she has received another project titled, Securing AODV based MANETs by DRDO as the funded project. Additionally, she is working for Estimation of Soil Moisture in Agricultural Lands using Wireless Sensor Networks funded by Department of Science & Technology, Government of India in 2015 (On-going) (PI). She is a Member of IEEE, ACM, ISCA, IET, and IST.