A Review on - ControlChain: Access Control using BlockChain

Vidyabhushan Adhav[1], Shubham Bhosale[2], Pratiksha Javanjal[3], Namrata Kadam[4]
Gauri Bhange[5]

[1,2,3,4]Student, Department of Computer Engineering, Sinhgad Academy of Engineering, Pune, India
[5]Professor, Department of Computer Engineering, Sinhgad Academy of Engineering, Pune, India

---

Abstract - *The IoT is perceived in every part of our daily activities and lives with devices scattered all over our cities, transport systems, buildings, homes and bodies. This takeover of devices with sensors and communication capabilities brings big concerns, mainly about the privacy and confidentiality of the collected information. These concerns hinder the wide adoption of the IoT. This paper presents a survey on some previous architectures, models that are used for access control mechanism carried out in IoT.*

Key Words: RBAC, ABAC, OrBAC, IoT, XACML, Policy, Access control

1. INTRODUCTION

The Internet of Things (IoT) consists of objective of providing new intelligent services and commodities to facilitate our daily tasks. Its devices are perceived in our cities, public buildings, roads, airways, factories, retail stores, offices, hospitals, homes and bodies. With their sensors, communication and information processing capabilities they affect our interactions on all applications domains: personal, home, government, utilities, enterprise and industry. Together with the great features that arise with such integrated systems, there are many security concerns that block its broad adoption by users, governments and industries. Recently, more than 150,000 IoT devices were compromised and the investigations identified the access control as the main responsible for the security breach. Therefore, the adoption of improper access control systems could cause big privacy and economical harm to individuals and enterprises. A complete access control solution involves three components: authentication, authorization and auditing. The authentication identifies the correct identity of the subject. The authorization verifies if the subject has the rights to do some operation on the object. Finally, the auditing (or accountability) allow the posterior analysis of the realized activities in the system. These components have important roles in securing the system.

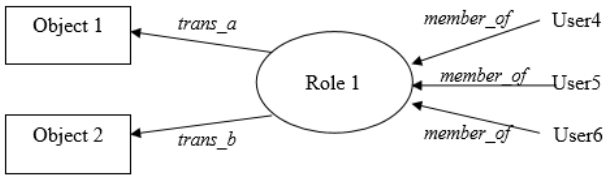
2. LITERATURE SURVEY

A Mandatory Access Control (MAC) is an easier way in establishing and maintaining access, especially when dealing with a great number of users, because you just need to establish a single level for each resource and one level for each user. These levels can be secret, top secret, confidential and each user is linked with one of this level.

The user having lower level clearance cannot access higher level. MAC model is used where confidentiality is more important i.e. Military institution

In Discretionary Access Control (DAC), the owner of the object specifies which subjects can access the object. DAC has advantage of flexibility over the MAC. If level 1 user wants to access one resource from level 1, then only access to that particular resource should be allowed.

Roles of user that takes part in the organization can be used in access control decisions. These roles can be consists of responsibilities, duties. Consider example of College can have roles like Principal, Head of departments, Admin, Accountant, Teacher, Student etc. A Role Based Access Control (RBAC) policy bases access control decisions on the roles or functions of user in that organization[1] . In RBAC, user cannot pass the permission to other user at their discretion as compared to DAC model. A role can be thought of set of transaction that user or set of user can perform onto organization. Roles are group oriented i.e. each role can be allocated set of transactions and as a result RBAC provide means of describing many-to-many relationship between users and rights. In addition roles can be composed of roles



$\forall s : subject, t : tran, o : object, (exec(s,t) \Rightarrow access(AR(s), t, o, x))$

exec(s,t) will true if subject s can execute transaction t. With this description, rule ensures that for all subjects s with transaction t on object o if s can execute t then s can apply transaction t on object o on x mode (e.g. Read, Write).

Role based access control (RBAC) is not well suited for cross-domains as it is well suited for independent domains. To overcome this Attribute Based Access Control (ABAC) was introduced. The main difference between RBAC and ABAC is that RBAC provides access rights depending on role whereas ABAC provides access rights considering user, resource and environment attributes[2]. These ABAC attributes can be described as:

- Subject attribute: An entity that takes action on resource
- Resource Attribute: Entity that is acted upon by subject.
- Environment Attribute: It describes the operational, technical, and even situational environment or context in which the access to the data occurs

Access policies of ABAC systems are defined by XACML, which is XML based standard. It contains XML tags that satisfies all these attribute in ABAC. ABAC model consists of policy model which contains ABAC policies and architecture model which applies these policies.

ABAC working consists of four modules

1. *The message processing module* that encode and decode login information and token
2. The authentication and token management module authenticates the user and generate token for user and manages identity of user with the help of database.
3. Access control Module is core part for access control. It contains :
   - Attribute Authority which is responsible for managing attributes of subjects, resources
   - Policy Enforcement Point (PEP) is responsible for requesting authorization policies and also enforce them
   - Policy Decision Point (PDP) applies policies to take authorization decision
   - Policy Authority (PA) creates and manages these access control policies.
4. Service Management Module extracts resource services that user has requested to.

XACML is an XML-based language for access control that has been standardized by OASIS (Organization for the Advancement of Structured Information Standards) [3]. XACML describes both an access control policy language that are ABAC and an access control decisions (request/response) language. Policy language construct expression that describes who can what and when. The request/response language used for querying a request to access resource and convey response of access grant/deny messages.

The main functions offered by XACML can be summarized as follows:

1. Policy combination: XACML provides a method for combining policies independently specified.

2. Combining algorithms: XACML supports different combining algorithms, each representing a way of combining multiple decisions into a single decision.

3. Attribute-based restrictions: XACML supports the definition of policies based on generic properties (attributes) associated with subjects.

4. Policy distribution: XACML allows one policy to contain, or refer to, another.

5. Implementation independence: This guarantees that different implementations operate in a consistent way, regardless of the specific implementation.

There formed a need such that rules for accessing the resource should be specific to organizations, the organization should be structured into sub-organizations and have their own security policies, rules should have contextual permission to resource, rules that can be applied only in some of circumstances. However RBAC, ABAC are not fully satisfactory apply these needs in organization. To overcome this, Organization Based Access Control (OrBAC) was introduced by authors.

OrBAC can be presented just by using Entity Relationship model[4]. In accordance to Entity Relationship Model, the entities and the relationships of OrBAC model may be associated with attributes. Let us see some entities used by OrBAC.

- Organization: It can be any organization like ABC medical college, XYZ college of engineering
- Subjects and roles: Subject in OrBAC can be either active entity like Student, Teacher or an organization like ABC medical college. Role is used to form a link between subject and organization
- Objects and Views: Object can be a active entity like data reports, files, emails. Combination of objects that satisfies common property considered as view.
- Actions and activities: Action will mainly contain actions that are going to apply on resource being accessed. It can be read, write, send etc.
- Security Policies: It specifies set of permissions, prohibitions, obligation that is used for authorization decisions.
- Contexts: It specifies circumstances where organizations grants permission to perform activities.

A permission corresponds to a fact that have the form Permission(org ,r ,v ,a ,c) can be read as in organization org, within context c, role r is permitted to perform activity a on view v.

OAuth is a framework used for access control. It provides a method for clients to access protected resource on behalf of resource owner by obtaining access token[5]. In OAuth, client must first obtain authorization grant from resource owner and then exchange it to get access token. The token gives granted scope, time and other information granted by authorization grant. The authorization server generate access token. Then client accesses the protected resource presenting access token to the resource server. The client

can have some credential so that it can be presented directly to authorization server to get access token. Hence it reduces having access grant from resource owner. OAuth does this with the help of HTTP GET or POST requests.

For example, the client makes the following HTTP request using transport-layer security :

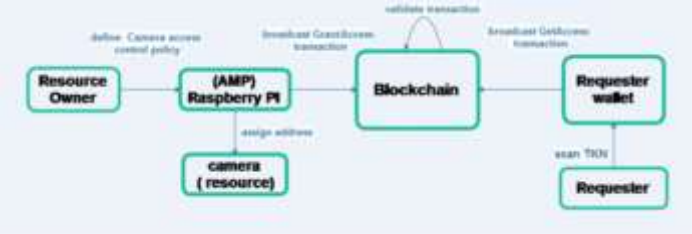
Post /resource HTTP/1.1

Host: server.example.com

Content-type: application/x-www-form-urlencoded

Access-token=mFgr-4.5MMFhks3469

Previous models and architectures are used with help of centralized architecture approach. That may cause ethical and privacy problem for e.g. Company that make Smart watches contains data about fitness activities of people. Company then broadcasts some of their good fitness results to public i.e. they share our information. Sharing our data with third parties we loose control and ownership. FairAccess framework overcomes this problem of sharing information to third parties with the help of blockchain. Blockchain is distributed ledger that stores all processed transaction in chronological order.



FairAccess is token based system where temporary token is generated by resource owner to access resource by users[6]. Resource Owner applies or defines access control policy in blockchain. The temporary token gets generated by resource owner and distributed to blockchain. Resource owner generates GrantAccess transaction to allow users to access its resource. Resource users generates GetAccess transaction to access resource. Resource user uses token generated by RO. If token is not get matched according to token generated by RO in blockchain, access to the resource get rejected. Whenever token gets expired, RO generates new token and distributes it to blockchain.

3. PROPOSED SYSTEM

Proposed access control system will be fully decentralized with utilization of blockchain. It will consist of 4 types of blockchains – context, relationship, rule, accountability. Context blockchain will store context of device, relationship blockchain will store identity of devices and relationship between users and devices, rule blockchain will consist of access control rules formed by different models like RBAC, ABAC, OrBAC, accountability blockchain will contain documentation i.e. Records of accessing devices.

4. CONCLUSION

In this work, we have seen various models and framework used for access control mechanism. This article gives a short review on various methodologies that are used in current access controlling mechanism. It also shows how various types of policies are stored, used, accessed and applied on resource. The paper will help to build a access control that remove drawbacks from these previous architectures.

REFERENCES

[1] David F. Ferraiolo, D. Rechard Kuhn "Role-Based Access Controls" 15th National Security Conference (1992) Baltimore, Oct 13-16, 1992 pp 554-563.

[2] Ni Dan. Shi Hua-ji, Chen Yuan, Gua Jia-hu "Attribute Based Access Control (ABAC)-based cross-domain access control in service-oriented architecture (SOA)" 2012 International Conference on Computer Science and Service System.

[3] A.A. Abd El-Aziz, A.Kannan, "A COMPREHENSIVE PRESENTATION TO XACML1Dept. of Information Science and Technology, College of Engineering, Guindy, Anna University, India

[4] Anas Abou El Kalam, Rania El Baida, Philippe Balbiani, Salem Benferhat, Fr´ed´eric Cuppens, Yves Deswarte, Alexandre Mi`ege, Claire Saurel, Gilles Trouessin, "Organization based access control" unpublished.

[5] Internet Engineering Task Force "The OAuth 2.0 Authorization Framework: Bearer Token Usage"

[6] Aafaf Ouaddah, Anas Abou Elkalam, Abdellah Ait Ouahman. "FairAccess: a new Blockchain-based access control framework for the Internet of Things" published online 19 February 2017 in Wiley Online Library