A Novel Access Control Model Based on the Structure of Applications

Afshin Rezakhani[1], Hossein Shirazi[2] and Naser Modiri[3]

[1,2] Information, communications and security technologies Complex, Malek-Ashtar University of Technology, Tehran, Iran
[3] Department of Computer Engineering, Islamic Azad University, Zanjan Branch, Iran
af.rezakhani@gmail.com, Shirazi@mut.ac.ir, Nassermodiri@yahoo.com

***Abstract*:** Nowadays, access control has an important role in the management of access to resources in the networks and applications. The establishment of access control in applications is important particularly. Traditional methods of access control, manage the users' access only at data-centric level. In this paper a new model is presented in which the access control in applications is performed not only at data-centric level but also at component and plug-in levels. By applying the proposed model, the execution of plug-ins or components will be authorized only in the case of enrollment process and in the necessary authorities. In addition, users can access to plug-ins and components only in the case of gaining the necessary authorities. By using the proposed model, the access control can be applied based on both operational needs and applications capabilities accurately.

***Keywords*:** Access Control, Plug-ins, Components, Data-Centric**.**

1. Introduction

The access control is one of the security features that can control access to systems and resources [1]. It is defined as the act of determining whether a particular privilege can be granted to the requester of a particular credential. The privilege can be right of access to a resource, such as a communications link, an information database, a computing machine, or many other things owned by a network or service provider. The presenter of the credential can be either a device or a user [2]. Access control is arguably the most fundamental and the most pervasive security mechanism in use today. Access control can take many forms. In addition to determining whether a user has rights to use a resource, the access control system may constrain when and how the resource may be used. For example, a user may have access control to a network only during working hours. Some organizations may establish more complex controls, such as requiring that two staff members conduct certain high-risk operations such as opening a vault or launching a missile. Access control is only one aspect of a comprehensive computer security solution but it is one of the most visible one. Every time a user logs on to a multiuser computer system, access control is enforced [3]. A business process is a combination of structured activities to achieve specific purposes. It is set of several related activities that accomplish the specific goal of enterprises.

In the report [4], which was published by SANS, twenty critical security controls for effective cyber defense are raised. The second key security control in this report is related to application access control that represents the important position of this control.

So, in this paper a new approach is presented, which controls the access to the integrated applications in the networks at three different levels (three different perspectives). From the perspective of Plug-in, the access to application subsections is managed. From this perspective, the plug-in execution authority and also authorized users' access are controlled. Access from the perspective of the component is also discussed and it covers the plug-in's capabilities. From this perspective, the users' access to components is managed. Finally, at the third level, from the perspective of data-centric, the users' access to data (information that provided by application) is controlled.

2. Related Works

In this section, we consider some related works in the access control in the applications and networks.

In the research [5], the authors have developed a dynamic access control system for cloud computing environment along with policy conflict resolution algorithm and several access control validation processes. Their proposed system included four models, namely access right model, policy model, access control management model and access control model. The proposed system introduced a more efficient security scheme using an enhanced access control scheme. The paper [6] proposed a novel access control framework that combines trust with risk and supports access control in dynamic contexts through trust enhancement mechanisms and risk mitigation strategies. That allowed to strike a balance between the risks associated with a data request and the trustworthiness of the requester. If the risk was too large compared to the trust level, then the framework could identify adaptive strategies leading to a decrease of the risk (e.g., by removing/obfuscation part of the data through anonymization) or to increase the trust level (e.g., by asking for additional obligations to the requester). There was concern that some campuses was not using such protective systems, hence the paper [7] attempted to resolve this weaknesses in such institutions' by developing a simpler CAC system using the Radio Frequency (RF) and contactless smart card technologies. The scope of the developed system was not only limited to access control but also to utilize the gathered data to automate and potentially to support other processes of the institution, such as lecture scheduling and attendance tracking. In the paper [8], the authors proposed an access control model that combined the two models in a novel way in order to unify their benefits. Their approach provided a fine-grained access control mechanism that not only takes contextual information into account while making the access control decisions but was also suitable for applications where access to resources was controlled by exploiting contents of the resources in the policy. The paper [9] proposed "a novel smart access control (SAC) system, which can identify and categorize suspicious users from the

analysis of one's activities and bio information. The SAC system observed and recorded users' daily behavioral activities. From the analysis of the collected data, it selectively chose certain users for additional layers of authentication procedure and quickly isolated those individuals who might pass through scrutiny by security personnel. In the paper [10], was presented state-of-the-art survey of the MAC protocols available for vehicular safety. Authors classified those protocols based on different applications and the techniques they adopt. They also reviewed the performance metrics used for evaluating these protocols. Also, they qualitatively analyzed the protocols based on different parameters along with related issues and the challenges they generated. The paper [11] presented a novel approach to medium access control for single-hop wireless sensor networks.

The ALOHA-Q protocol applied Q-Learning to frame based ALOHA as an intelligent slot selection strategy capable of migrating from random access to perfect scheduling. Results showed that ALOHA-Q significantly outperformed Slotted ALOHA in terms of energy-efficiency, delay and throughput. In the paper [12], the authors seamlessly incorporated the dynamic attributes to the conventional access control scheme. Inclusion of dynamic attributes provided an additional layer of security to the conventional access control. They demonstrated that the efficiency of the proposed algorithm was comparable to the efficiency of the conventional schemes. A user or subject, who was given a discretionary access to a resource, was prepared to do passing the access to another subject. This model received the idea of user ownership [13]. One of the basic models in DAC was Lampson access control Model. The access of domains to objects was determined by the access matrix. Its rows were labeled by domain names and its columns by object names [3]. Mandatory access control (MAC) model [13, 14] can be characterized as a method for restricting access to resources based on the sensitivity of the information contained in it and the access control of subjects. The RBAC Model characterizes sets of fundamental RBAC components (i.e., users, roles, permissions, operations and objects) and relations as types and capacities that were incorporated in this standard. The RBAC reference model serves two needs. First, the reference model characterizes the extent of RBAC components that were incorporated in the standard. Second, the model gives an exact and predictable language, as far as component sets and capacities for use in characterizing the useful specification [15]. Some of extended models based on RBAC are Temporal-RBAC [16], Risk-aware RBAC [17] and Budget-aware-RBAC [18]. The idea of Attribute Based Access Control (ABAC) has existed for a long time. It show a point in the space of access control that incorporates access control list, role-based access control, and the ABAC model for giving access based on the evaluation of attributes [19]. An extended attribute based access control model with trust and privacy [20] is one of the extended attribute base access control model. The Risk-Adaptive Access Control (RAdAC) model was contrived to bring real-time, adaptable, risk-aware access control to the enterprises. It stretches out upon other prior access control models by presenting environmental conditions and risk levels into the access control decision, notwithstanding the concept of "operational need". RAdAC also utilized situational components for the decision making [21].

3. Proposed Model

As previously stated, one of the issues that is raised as an important challenge in access control is establishment of access control model for integrated applications in the networks. In this paper, a novel model is presented in which the access control can be stated and implemented accurately. The proposed access control model is propounded for the user's access in integrated applications. In the proposed model, we define three perspectives for the access control in applications in the networks which have been shown in Figure 1.

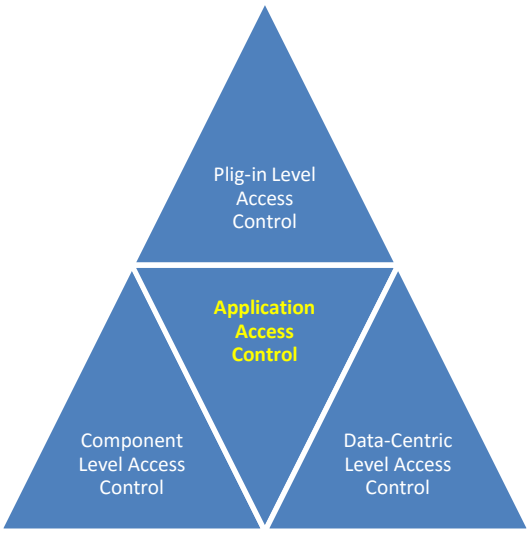

Figure 1. The Proposed Model for the Access Control in Applications

As can be seen in above figure, the first layer of the proposed model is access control in applications from the perspective of plug-ins. From this perspective, an integrated application is composed of several plug-ins and each new subsystem is defined as a new plug-in. Therefore, the first layer of the proposed model is the access control of applications plug-ins. The second layer of the proposed model is the access control from viewpoint of available components in plug-ins. From this perspective, the capabilities in the plug-ins are raised in the form of components. The suggestion of the paper in this layer is that the access to these components should be controlled based on their capabilities. The third layer of the proposed model is the access control in data level that we named it data-centric. In this layer, the users' access to data provided in classes is controlled. In the following subsections, we will take a closer look at the proposed model.

3.1 Access control in Plug-in Level

The access control in applications from the viewpoint of plug-ins creates a new vision for the researchers. Many traditional researches in the field of access control to applications are directed to the data that are accessed. However, we present a new approach in the proposed model that defines the access to applications in three different levels. In the first level of the proposed model, the plug-ins are defined. Plug-ins are the application parts, which are added to applications according to enterprise functionalities. From this perspective, it is suggested that each plug-in must be registered and obtain the necessary authorities to be executable as a part of applications. After obtaining the authorities, only authorized applications allowed to execute

beside other Plug-ins. Given that the enterprise's needs are dynamic, thus authorizing the plug-ins is dynamic and it can be updated. The life cycle of access control in plug-ins is as the Figure 2.

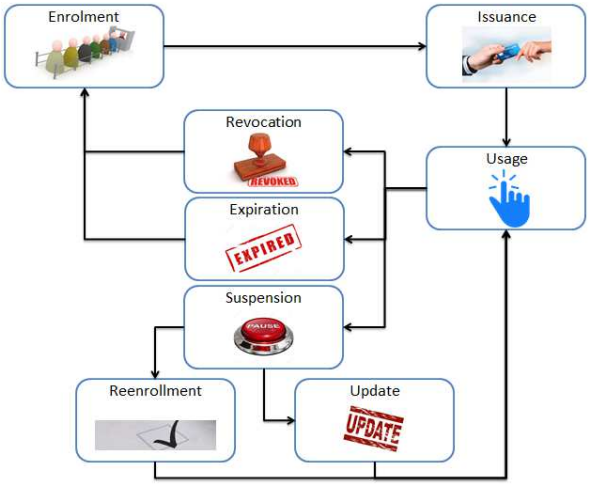

Figure 2. The Proposed Life Cycle of Access Control in Application Plug-ins

- ***Enrollment***: In the registration process, a certificate is requested to be issued for a plug-in. At this stage, the required information is collected and confirmed to ensure the validity of plug-in. This operation is often called plug-in validation.
- ***Issuance***: in the issuance phase, a certificate is assigned to plug-in and it is issued for it. At this stage, a special token may be needed and registered.
- **Usage**: in the usage phase, plug-in obtains the authorities to execution by the received certificates and it can be executed.
- ***Expiration***: certificates usually have a certain period time to use and then, they are expired. This time is based on the plug-in's need. When the life of a certificate is expired, it is not valid so the plug-in will not have the authority to execute.
- ***Revocation***: Sometimes a plug-in certificate needs to be revoked according to certain conditions before ending its expiration time. This case is named revocation in the proposed life cycle. For example, when a token is compromised, such a situation will happen.
- ***Suspension***: Sometimes a certificate becomes temporarily invalid or it may be in the suspension status before ending its validity. This occurs when a plug-in is temporarily unenforceable based on security needs.
- ***Reenrollment/Update***: If a certificate goes to suspend mode, it should be updated or enrollment should be done for activation. With this, the name or certificate specifications may be changed.

3.2 Access control in Components Level

One of the other innovations of this paper is creating a new perspective on access control in applications. From this viewpoint, the capabilities that provided by plug-ins are classified and then, the access to these capabilities is managed. Therefore, the capabilities of each plug-in is defined at the second level of the proposed model, and the access to them is controlled. As an example, suppose that there are *Administrative plug-in* in an Application. This plug-in consists of several high capabilities including the welfare affairs, personnel affairs, salary affairs, and automation affairs. We named them as the components of Administrative plug-in. It is important that the access to them is controlled and only the authorized components must be executed.

3.3 Access control in Data-Centric Level

The third level of the proposed model is the access control at the level of data that provided by applications. XACML language is standard from OSSIS [22] and is based on XML to describe access control policies. Also it is used by more than 35 big companies around the world such as IBM, SUN, to describe organizations policies. General scenario of XACML in access control is to check if requester is allowed to access resources. So, access control policies in data-centric level will be defined and expressed in XACML format. The proposed architecture for the access control, which is based on ISO 10181 [23], has been shown in Figure 3.

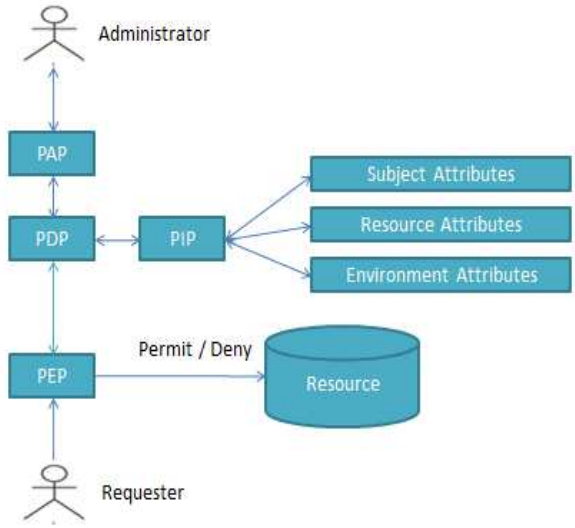

Figure 3. The XACML Structure in Data-Centric Level Access Control

As seen in above figure, to manage the user's access to a method within classes, it is needed to send the request to Policy Enforcement Points (PEP) in the network. The decision making of this unit is provided based on the response of the Policy Decision Point (PDP). PDP decides by two main units of both Policy Administration Point (PAP) and Policy Information Point (PIP). In PAP all the policies are written by the managers and this unit plays the role of user policies knowledgebase. Another unit, Policy Information Point, should be existed beside PDP in the network for determining the attributes of the requester. In fact PDP gives the permission of accessibility based on policies and information in PIP.

4. Implementation

In this section, we will explain the implementation of proposed model accurately. Initially, we will introduce the special test bed for implementation and then, the implementation of the proposed model at the three levels is described. The screenshot of implemented tools (after login page) that manage the application access in the network is shown in Figure 4.

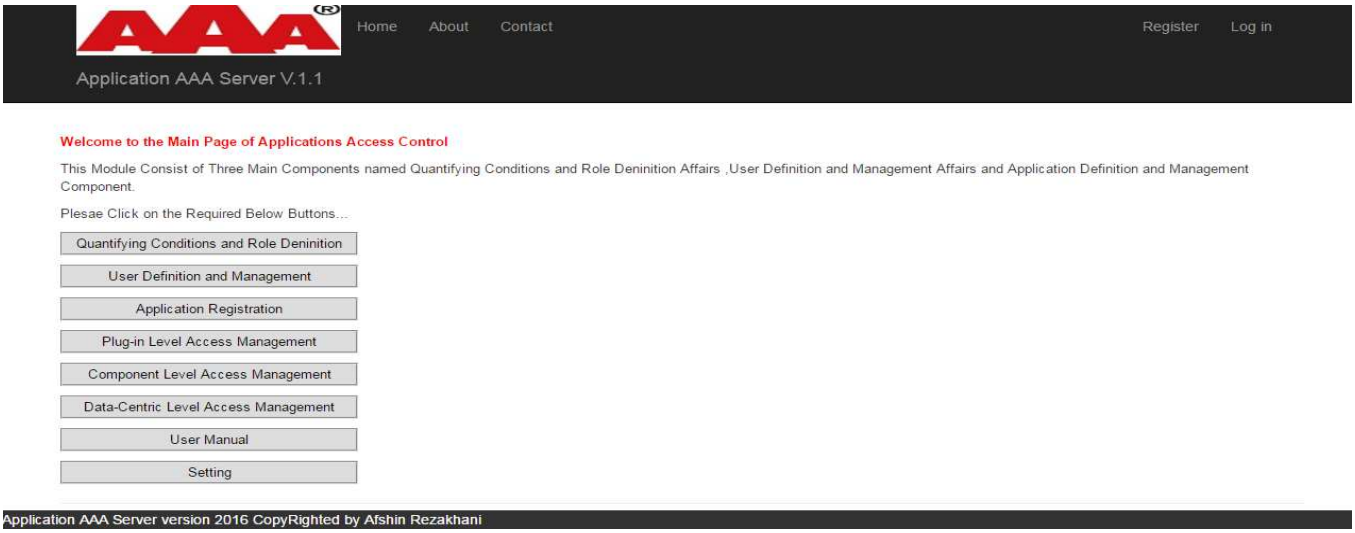

Figure 4. The Developed Tools for Application's Access Control

4.1 Case study

It is necessary to give an expression of the implementation conditions and case study for implementation. For this, we consider an integrated system and specify some parts of it. The characteristics of this system are as Figure 5.

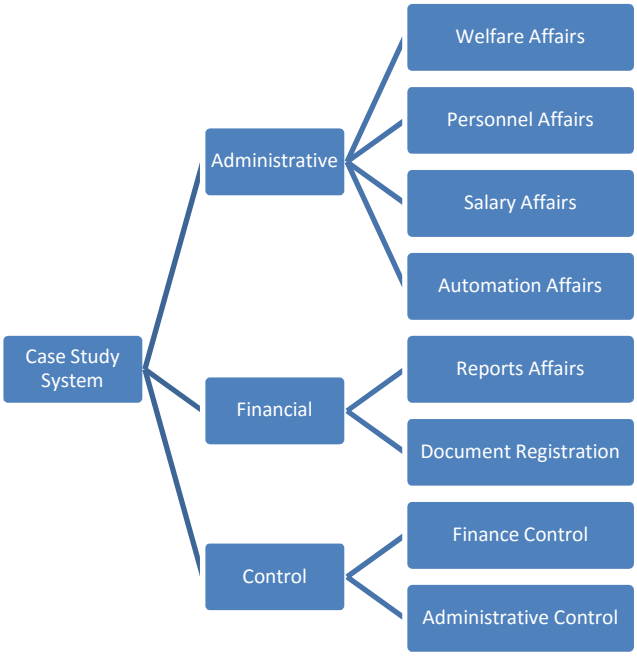

Figure 5. Definition of Case Study Structure

As shown in above figure, it can be seen that an integrated application is defined to meet the goals of the system, which includes three administrative, financial, and control plug-ins. Each of these plug-ins has different capabilities. For example, an administrative plug-in includes the capabilities of welfare affairs, personnel affairs, salary affairs, and automation affairs.

4.2 The Implementation of Plugin-level Access control

Given the mentioned case study, supposing a new plug-in named administrative plug-in, is needed to add to the integrated application. For the execution authority of this plug-in, the explained life cycle in the previous sections should be done. In the following parts, the required processes are explained to add this plug-in.

4.2.1 The Implementation of Enrollment Phase

To add the *administrative plug-in*, the enrollment process should be run for the plug-in according to the described life cycle in section 3.1. To carry out this process, a profile is created for this plug-in with the following characteristics. The details of this profile will be important for plug-in's access management. For example, it should be determined what is the identity related to the plug-in, or when is the effective and expiration date. We named this profile as plug-in profile. This profile is also used to specify user's authorities.

- *Plug-in ID: 100*
- *Plug-in Name: Administrative Plug-in*
- *Enrollment Date: 03/10/2016*
- *Effective Date: 03/20/2016*
- *Expiration Date: 03/10/2017*
- *Suspension Conditions: Regulation Updates*
- *Revocation Conditions: Regulation Changes*
- *Authorized Roles: Role1 & Role3 and Role5*
- *Plug-in-Purpose: Administrative Affairs Management*
- *Plug-in-Introduction: Plug-in Definition*
- *Plug-in-Scopes: Administrative Affairs*

4.2.2 The Implementation of Issuance Phase

After doing the enrollment phase for the administrative plug-in, issuance phase should be done. For this purpose, a special certificate should be setup and exported correspond to the discussed plug-in. In this section, we use hardware tokens to certify the execution of administrative plug-in. The characteristics of the applied hardware token are given in Figure 6.

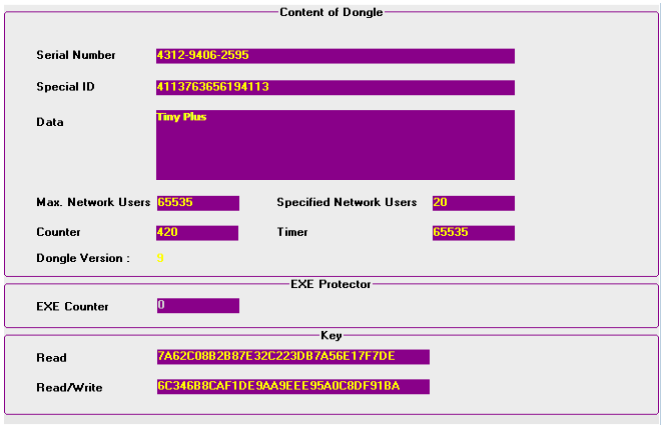

Figure 6. The Characteristics of the Hardware Token for the Administrative plug-in

4.2.3 The Implementation of Usage Phase

After doing issuance phase, the access manager should import the designed token to the system through USB port to issue the usage certificate in the mentioned plug-in. In addition, a condition is provided in which the users are only authorized to login to the plug-in when this certificate is introduced to the application. A part of the Asp.net code for checking the validity of the certificate is as follows.

```
string strSafeKey1 = " … ";
 string strSafeKey2 = "… ";
 string[] ArrRequest = new string[5000] { … };
 string[] ArrResponse = new string[5000] { … };
if (found == 1 && axTinyPlus.FindFirstTPlus("… ", strSafeKey1, strSafeKey2)
== 0)  {
     if (User.Text == "Admin" || Pass.Text == "*****")   {
      if (ArrResponse[irand] == axTinyPlus.GetTPlusQuery(ArrRequest[irand]))
{
       strSerialNbr =
       axTinyPlus.GetTPlusData(EnumTPlusData.TPLUS_SERIALNUMBER).To
       String();
      strspacialid =
       axTinyPlus.GetTPlusData(EnumTPlusData.TPLUS_SPECIALID).ToString
       ();
      strdata =
       axTinyPlus.GetTPlusData(EnumTPlusData.TPLUS_DATAPARTITION).To
       String();
      icounter =
       Convert.ToInt16(axTinyPlus.GetTPlusData(EnumTPlusData.TPLUS_COU
       NTER));
      itimer =
       Convert.ToInt16(axTinyPlus.GetTPlusData(EnumTPlusData.TPLUS_TIM
       ER));
      inetuser =
       Convert.ToInt16(axTinyPlus.GetTPlusData(EnumTPlusData.TPLUS_NET
       WORKUSER));
      imaxnt =
       Convert.ToInt32(axTinyPlus.GetTPlusData(EnumTPlusData.TPLUS_MAX
       NETWORKUSER));
      axTinyPlus.SetTPlusData(EnumTPlusData.TPLUS_DATAPARTITION,
       strdata);
      axTinyPlus.SetTPlusData(EnumTPlusData.TPLUS_COUNTER, icounter);
       axTinyPlus.SetTPlusData(EnumTPlusData.TPLUS_TIMER, itimer);
       axTinyPlus.SetTPlusData(EnumTPlusData.TPLUS_NETWORKUSER,
       inetuser);
       Response.Redirect("MainPage.aspx");   }  }
    Else  {
        Response.Redirect("ErrorPage.aspx"); }   }
 Else   {
     lblerr.Text = “Error in token identification”;    }
```

4.2.4 Additional Capabilities

Besides the fact that only the authorized plug-ins are executable in the network, the proposed model in this paper provides a condition that only authorized users could login in the plug-ins. This is done through checking the plug-in profile while user logging in. For this purpose, it should be specified after determining the user identity (by authentication process), whether this user is authorized to login to special plug-in or not (through the plug-in profile). Therefore, it is clear that we have created a mechanism that will not allow unauthorized users in addition to preventing the execution of unauthorized plug-ins.

4.3 The Implementation of Component-level Access control

As stated, the second level of the proposed model in the access control of applications is component level. Suppose that there are four main components of *welfare affairs*, *personnel affairs*, *salary affairs*, and *automation affairs* in the *administrative plug-in*. A profile is defined for each component, in which the execution authority is determined. In addition, the authorized users to login are determined in this profile. Implementing the component access control is done at this level by using the defined certificates.

If a capability has the authority to execute based on the enterprise's security policies, the desired component specifications are placed in whitelisting components. This means that this component has the ability to execute. In addition, the authorized users are specified in the component profile. The list of created certificates at the component level for the *personnel affairs* capability in IIS7.0 is given in Figure 7.

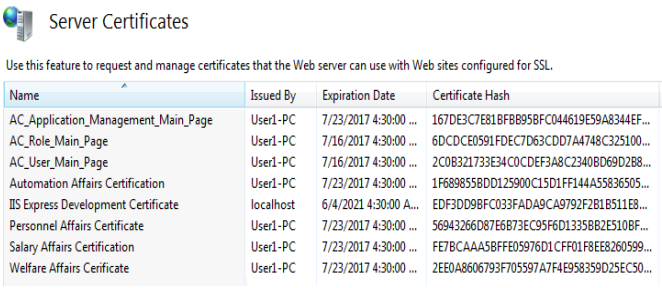

Figure 7. The Created Certificates for the Administrative Plug-in

4.4 The Implementation of Data-Centric-level Access control

XACML language is used to implement the access control in applications in the network at the data-centric level. This language is used to express the access control policies to access the methods within the classes. One of the special developed policies to access the class methods that provide the *personnel affairs* data for users is shown as follow. This XACML code expresses the role of *Administrative_Manager* has the permission *set()* on *Employment_Method* method.

```
<?xml version="1.0" encoding="UTF-8"?><!--## This XACML is the collection of
policies (e.g., POLICY 1) to be merged (by users).-->
<PolicySet xmlns="urn:oasis:names:tc:xacml:2.0:policy:schema:os"
PolicySetId="MergedPolicySet"
PolicyCombiningAlgId="urn:oasis:names:tc:xacml:1.0:policy-combining-
algorithm:first-applicable">
   <Target/>
<!--## POLICY START1-->
    <Policy PolicyId="ABAC1"
RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:first-
applicable">
      <Target/>
```

```
<!-- ABAC Model: ABAC1-->
    <Rule RuleId="rule_1" Effect="Permit">
     <Target>
      <Subjects>
       <Subject>
        <SubjectMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-
equal">
         <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">Administrative_Manager<
/AttributeValue>
         <SubjectAttributeDesignator
SubjectCategory="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"
AttributeId="Role" DataType="http://www.w3.org/2001/XMLSchema#string"/>
        </SubjectMatch>
       </Subject>
      </Subjects>
      <Resources>
       <Resource>
        <ResourceMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-
equal">
         <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">Employment_Method</Att
ributeValue>
         <ResourceAttributeDesignator AttributeId="Name"
DataType="http://www.w3.org/2001/XMLSchema#string"/>
        </ResourceMatch>
       </Resource>
      </Resources>
      <Actions>
       <Action>
        <ActionMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-
equal">
         <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">Set()</AttributeValue>
         <ActionAttributeDesignator AttributeId="MLSDefaultAction"
DataType="http://www.w3.org/2001/XMLSchema#string"/>
        </ActionMatch>
       </Action>
      </Actions>
      </Target>

    </Rule>
   </Policy>
<!--## POLICY 1 END-->

</PolicySet>
```

5. Evaluation

In this part, the evaluation of the proposed model is considered. Given that a set of metrics have been added in the proposed model compared with current existing models, we will consider these metrics in the evaluation method. We have used seven experts to compare different models according to the criteria. For this purpose, we tried to explain the evaluation criteria to experts accurately. The different models explained to them and then they determined ranking of different models. To evaluate the proposed model, some metrics should be determined as the evaluation criteria. These criteria are defined as follows.

- *Multi-layer access control Supporting*
- *Whitelisting technology Supporting*
- *Plug-in based access control Supporting*
- *Component based access control Supporting*

In addition, we choose some valid methods (alternatives) as following:

- *Ranking-ABAC [1]*
- *CAC&MS [7]*
- *AE-RBAC [8]*
- *ARL-AC [11]*
- *Proposed Approach*

To check the validity of the proposed model, seven experts were chosen in this field and the necessary explanations are given to them. Then, we rank the approaches according to the described criteria based on special questionnaires. The considered ranking is based on OWA method. This ranking method has been examined precisely in our previous paper [1] and is based on [24]. The methodology of ranking the above approaches is as following sections. Our Special tool is used for ranking, which is shown in the Figure 8.

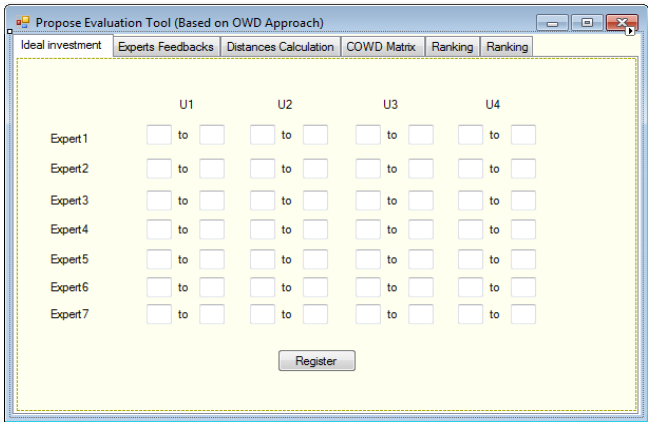

Figure 8. The Proposed Evaluation tools

5.1 Decision-maker Feedbacks

After providing preliminary parameters, feedbacks should be taken from the decision-makers. These feedbacks are done in two stages. In the first stage, every decision-maker enters his/her viewpoints from perspective of different criteria about the approaches, and in the second stage every decision-maker enters his/her opinions about the importance of criteria to each other.

5.2 Calculate Distances

After receiving feedback from the decision-makers, their opinions which are expressed as ranges change into numbers. These are calculated based on a comparison of decision-makers' opinions about the approaches (according to criteria) and importance of each criterion. The numbers are calculated as follow:

$$d(\tilde{a}_{ij}^{k}, \tilde{y}_{j}^{k}) = |\mu(\tilde{a}_{ij}^{kU} - \tilde{y}_{j}^{kU}) + (1-\mu)(\tilde{a}_{ij}^{kL} - \tilde{y}_{j}^{kL})| \quad (1)$$

$i = 1, 2, \ldots, m,\ j = 1, 2, \ldots, n,\ k = 1, 2, \ldots, t$

5.3 Calculate COWD

After obtaining the distance matrices, we will calculate COWD matrix as follow. In this matrix, first dimension shows approaches and second dimension shows decision-makers. In other words, this matrix keeps integration of decision-makers opinions about approaches.

$$\tilde{r}_{ik} = \text{COWD}(\tilde{a}_{i}^{k}, \tilde{y}^{k}) = \left(\sum_{j=1}^{n} W_j \left(d(\tilde{a}_{ij}^{k}, \tilde{y}_{j}^{k})\right)^{\lambda}\right)^{1/\lambda} \quad (2)$$

$i = 1, 2, \ldots, m,\ k = 1, 2, \ldots, t$

The weighting vector w is determined by decision makers in aggregation, also obtained by some objective methods.

5.4 Ranking the Approaches

The importance rate of each approach was calculated at the point of view of experts in above sections and in this phase we create the ranking of approaches. For this purpose, the following process will be done:

1. Determining the weight of Decision-makers' opinion
2. Calculating GOWA to integrate decision-makers' opinions
3. Normalizing approaches distance
4. Ranking the importance of approaches

At first, the weight vector is determined for decision-makers which is represented their strength in comments and it is displayed by V. In this regard, opinions of T decision-makers are integrated in accordance with their importance. So GOWA is calculated as follows:

$\tilde{r}_i$ = GOWA($\tilde{r}_{i1}$, $\tilde{r}_{i2}$, ... , $\tilde{r}_{it}$)

⇨ $\tilde{r}_i$ = GOWA(a1, a2, . . . , an) = $\left(\sum_{i=1}^{n} w_j b_j{}^r\right)^{1/r}$ (3)

i = 1, 2, . . . ,m

After calculating GOWA, we normalize obtained values and then regard its reveres. Finally, with this calculation, the importance of approaches is determined. However, because the worst possible distance for an attribute will be 100, so the ranking of approaches is as Table 1. As shown in the related table, our proposed approach has the most ranking and it is selected as the best interesting approach according to expert opinions.

Table 1. Ranking the Approaches

	Considered Models	Ranking
1	Ranking-ABAC	80.55%
2	CAC&MS	74.33%
3	AE-RBAC	60.76%
4	ARL-AC	55.34%
5	Proposed Model	95.76%

Now, we compare the proposed method with other above models. This comparison is done based on the number of features including Multi-layer access control Supporting and Whitelisting technology Supporting, etc. As seen in Table 2, the proposed method covers more parameters than other methods.

Table 2. The Comparison of proposed method with other models

Models	Multi-layer access control Supporting	Whitelisting technology Supporting	Plug-in based access control Supporting	Component based access control Supporting	Data-Centric based access control Supporting
Ranking-ABAC [1]	NS	NS	NS	NS	FS
CAC&MS [7]	LS	NS	NS	NS	FS
AE-RBAC [8]	LS	NS	NS	FS	FS
ARL-AC [11]	NS	NS	NS	LS	LS
(Proposed Model)	FS	LS	FS	FS	FS
					FS: Full support LS: Low support NS: No support

6. Conclusion

In this paper, a new model was expressed for access control in applications in the networks. According to this model, the access control went beyond the data-centric traditional level. The authority to execution and also user's access at plug-in level is proposed. Component levels were raised for access control based on the capabilities, too. By using the results of the present research, the dynamic and multi-level access control for applications can be created without reducing the applications' performance. This paper can be useful for improvement of application level of access control.

References

[1] Rashidi, A.J & Rezakhani, A., "A new approach to ranking attributes in attribute based access control using decision fusion". Neural Computing and Applications, 1-10, 2016.
[2] Nakhjiri, M & Nakhjiri, M. , "AAA and Network Security for Mobile Access: Radius, Diameter, EAP, PKI and IP Mobility". : Wiley, 2005.
[3] Bertino, E, Ghinita, G & Kamra, A., "Access Control for Databases: Concepts and Systems". Foundations and Trends in Databases, 3(1-2), 1-148, 2011.
[4] Sansorg., Sansorg. Retrieved 17 June, 2016, from https://www.sans.org/critical-security-controls, 2016
[5] Habiba et al., "A New Approach to Access Control in Cloud". Arabian Journal for Science and Engineering, 41(3), 1015-1030, 2016.
[6] Armando, A., "Balancing Trust and Risk in Access Control". In Debruyne, C (Ed), On the Move to Meaningful Internet Systems: OTM 2015 Conferences (pp. 660-676). :Springer International Publishing, 2015.
[7] Voon, M.J., "Campus Access Control and Management System". In Lavangnananda , K (Ed), Intelligent and Evolutionary Systems (pp. 395-404). : Springer International Publishing, 2016.
[8] Rajpoot, Q.M., "Attributes Enhanced Role-Based Access Control Model". In Ischer-hübner, S (Ed), Trust, Privacy and Security in Digital Business (pp. 3-17). : Springer International Publishing, 2015.
[9] Penubaku, L., "Access Control System Which Uses Human Behavioral Profiling for Authentication". In Thampi, S.M (Ed), Advances in Signal Processing and Intelligent Recognition Systems (pp. 419-430). : Springer International Publishing, 2015.
[10] Gupta, N, Prakash, A & Tripathi, R., "Medium access control protocols for safety applications in Vehicular Ad-Hoc Network: A classification and comprehensive survey". Vehicular Communications, 2(4), 223–237, 2015.
[11] Chu et al., "Application of reinforcement learning to medium access control for wireless sensor networks". Engineering Applications of Artificial Intelligence, 49(1),23–32, 2015.
[12] Li et al., "Robust access control framework for mobile cloud computing network". Computer Communications, 68(1), 61–72, 2015.
[13] Majumder, A., "Taxonomy and Classification of Access Control Models for Cloud Environments". In Mahmood, Z (Ed), Continued Rise of the Cloud (pp. 23-53). : Springer London, 2014.
[14] Aluvalu, R., "A Survey on Access Control Models in Cloud Computing". In Satapathy, S.C (Ed), Emerging ICT for Bridging the Future - Proceedings of the 49th Annual

Convention of the Computer Society of India (pp. 653-664). : Springer International Publishing, 2015.
[15] Secretariat information technology industry council (iti)., "Role Based Access Control". : American National Standard for Information Technology (NIST), 2003.
[16] Sharma et al., AMTRAC: An administrative model for temporal role-based access control. Computers & Security, 39(1), 201–218, 2013.
[17] Chen, L., "Risk-Aware Role-Based Access Control". In Meadows, C & Fernandez-gago, C (Eds), Security and Trust Management (pp. 140-156). : Springer Berlin Heidelberg, 2012.
[18] Salim et al., Budget-aware Role Based Access Control. Computers & Security, 35(1), 37–50, 2013.
[19] Vincent C. Hu et al., "Guide to Attribute Based Access Control (ABAC) Definition and Considerations". USA: NIST Special Publication 800-162, 2014.
[20] Smari, W, Clemente, P & Lalande, J., "An extended attribute based access control model with trust and privacy: Application to a collaborative crisis management system. Future Generation Computer Systems", 31(1), 147–168, 2014.
[21] Almutairi, A, Sarfraz, M & Ghafoor, A., "Risk-Aware Management of Virtual Resources in Access Controlled Service-oriented Cloud Datacenters". IEEE Transactions on Cloud Computing, PP(99), 2015.
[22] Wu, J., "Authorization-authentication using XACML and SAML". United Kingdom: University of Newcastle upon Tyne, Computing Science, 2005.
[23] Isoorg., ISO. Retrieved 17 June, 2016, from http://www.iso.org/iso/catalogue_detail.htm?csnumber=18199, 2016.
[24] Zhou, L, Chen, H & Liu, J., "Continuous Ordered Weighted Distance Measure and Its Application to Multiple Attribute Group Decision Making". Group Decision and Negotiation, 22(4), 739-758, 2013.