Access Control Model for Modern Virtual e-Government Services: Saudi Arabian Case Study

Rand Albrahim, Hessah Alsalamah, Shada Alsalamah, Mehmet Aksoy
Department of Information Systems
King Saud University
Riyadh, Saudi Arabia

***Abstract*—e-Government services require intensive information exchange and interconnection among governmental agencies to provide specialized online services and allow informed decision-making. This could compromise the integrity, confidentiality, and/or availability of the information being exchanged. Government agencies are accountable and liable for the protection of information they possess and use on a least privilege security principle basis even after dissemination. However, traditional access control models are short of achieving this as they do not allow dynamic access to unknown users to the system, they do not provide security controls at a fine-grained level, and they do not provide persistent control over this information. This paper proposes a novel secure access control model for cross-governmental agencies. The secure model deploys a Role-centric Mandatory Access Control MAC (R-MAC) model, suggests a classification scheme for e-Government information, and enforces its application using XML security technologies. By using the proposed model, privacy could be preserved by having dynamic, persistent, and fine-grained control over their shared information.**

Keywords—Access control; cloud infrastructure; data classification scheme; data exchange; e-government; fine-grained access; implementation framework; persistent control; XML security technologies; Saudi Arabia

I. Introduction

Electronic government (i.e. e-Government) refers to the use of Information and Communication Technologies (ICTs) to provide citizens with access to the country's public services [1]. The aim of e-Government is to improve efficiency [2], reduce the cost of government agencies' processes, and enhance administrative efforts for citizens and businesses; this is done by managing the interacting process with public authorities in a speedy manner [3], and creating a virtual electronic government that leads to economic growth and better transparency [3].

Many developing countries around the globe are shifting towards an electronic service (i.e. e-service) delivery model, and Saudi Arabia is no different. The Saudi government has invested intensively in building the infrastructure for technologies to support e-Government service [4]. However, government agencies do not deliver citizen-centred services for many reasons, and according to studies in [4], [5], information security risks, misplaced trust, privacy issues, and shortages in terms of available infrastructure take precedence. Therefore, there is still a necessity for the government to work harder towards providing tailored e-services. This can be achieved through a collaboration between its different governmental agencies, both public and private sectors [4], [6].

Government agencies interconnect with each other in different ways, either within the government's premises, across different governmental agencies (G2G), government and business/commerce (G2B), or government and citizens (G2C) [4], [7], [8] These service delivery models pose risks that can undoubtedly compromise the integrity, confidentiality, or availability of data and information being exchanged [8]. E-Governments have established different ways to communicate in a safe manner. The Saudi Arabian e-Government, like many other developing countries, for example, has established the Government Service Bus (GSB), a G2G that connects all agencies in Saudi Arabia and enables them to exchange information and services in the form of web services [9]. This raises the question of who can see what within the GSB. It is the government's responsibility to protect the personal information they possess and use under law [6]. According to Resolution 40 of the Saudi Ministers' Council, "*Information and data relevant to the user or applicant for a government service shall be viewed only by authorized persons*" [10]. This rule clearly states that all information systems used for the collection, transformation, processing, and/or manipulation of e-Government information must enforce appropriate information security controls to maintain the right balance between this information's availability, confidentiality, and integrity. This is to ensure the security of those systems' information. Applying the *"Least Privileg*e" access control principle can attain this balance. This principle grants authorised members of the organization access to the absolute minimum amount of information for the absolute minimum amount of time required to complete their duties [11]. To achieve the *least privilege* security principle, an access control mechanism needs to be deployed. However, traditional access control models are, firstly, static and inflexible to grant access to unknown users of the system. Secondly, they are coarse-grained [12] models capable of granting access either to the whole information resource or none of it, since they do not allow access at finer granularity. Finally, they do not provide persistent control over this information [13]. Most of the studies focus on securing access to data instead of securing the data itself [14]. Nevertheless, to preserve ownership over data even when it resides outside the premises, it is important to have continuous protection with information security controls that move along with the data [14] in both the physical and network levels [15]. This also includes all states of data when stored, processed, transited, and at a final destination [24].

This paper proposes an access control model (named R-MAC) for e-Government's connected web services to the GSB using an access control model that would achieve least privilege principle, and as stated by the Saudi e-government law, it is centred on the security of outsourced governmental data used within GSB to provide specialized online services. R-MAC is a novel approach that incorporates the properties of Mandatory Access Control (MAC) and Role-based Access Control (RBAC) into a new role-centric MAC model and employs XML security technology combined with a data classification scheme suitable for e-government information. MAC is a model in which the security policies and permissions for a subject to access an object are strictly constrained by the system [17], and RBAC grants subjects access to objects based on their role. XML security technologies reuse existing cryptographic and other security technologies whenever possible. It consists of XML digital signature, XML Key Management Specification (XKMS), XML encryption, Security Assertion Mark-up Language (SAML), and XML Access Control Mark-up Language (XACML) [18]. R-MAC provides a secure data exchange framework using some of those components to help preserve the ownership of data at a fine granularity. Fine-grained access control provides the right privileges to a user to grant him/her access to an asset only if this user is authorized [19]. In addition, XML security technologies provide fine-grained and persistent security controls that move with the data. Achieving a safe platform for data exchange in e-Government services enables dynamic, persistent, and fine-grained control for specialised online services through the collaboration of different government agencies.

The remainder of this paper is organized as follows. Section II provides a background of the Saudi e-government program and the use of web services. After that Section III presents the literature review. Then, we present our methodology in Section IV. Finally, the conclusion is provided in Section V.

II. Background

Saudi Arabia's Vision 2030 [20] is a plan adopted by the Saudi Government to guide economical and developmental action in Saudi Arabia [20]. The *National Transformation Program 2020* [21] was launched across 24 governmental bodies across Saudi Arabia to help achieve the ambitious goals of *Saudi Arabia's Vision 2030*. The Ministry of Communications and Information Technology [22] set a number of strategic objectives that correspond to relevant vision 2030 objectives, which include: "*Strategic Objective 3: Develop and activate smart government transactions based on a common infrastructure*" [21].

According to the United Nations' index for the development of e-Government, Saudi Arabia is currently ranked 36 globally and the target rank by 2020 is 25 [23]. The current maturity level of the government services transformation to e-services is 44% and the aim is to reach 85% by 2020 [21]. However, there are a number of reasons that hinder the adoption of e-Government services in general regardless of its model. These include, but are not limited to, poor skills, technology literacy [12], and security and privacy concerns regarding their shared personal information [24] (i.e. personal, financial, and medical data [25]). Moreover, the challenges related to the adoption and implementation of the Saudi e-Government are specific to infrastructure cost, computer literacy, accessibility, availability, trust, and privacy issues [4].

YESSER [34] is one of the key national programs in Saudi Arabia that specifically enables the delivery of e-Government services across government agencies. This is achieved through the development of a number of interrelated initiatives, for interoperability and networking. First and foremost, YESSER deploys an interoperability framework (YEFI) [26] that defines the set of policies to be implemented by government agencies to ensure a standardization of information and service exchange. It also defines the data types, schema, meta-data elements, dictionaries, and technical policies. The technical policies include the integration approach and set of standards, for connectivity, security, and information access and delivery [26]. Second is the GSB [9] which is the central platform of integration and services for government e-services and transactions. The GSB provides support for web services [9] as illustrated in Fig. 1. Currently, there are 69 agencies connected to the GSB providing 115 different services [9].

A Web service is standardized method, which allows different systems to communicate over a network. It can be a user requesting a service from a Web server or a Web server requesting a service from another Web server [27]. Web services have many advantages, including multiple heterogeneous platform compatibility [28], language-independency [36], increased information availability and ease of access [29], and maintaining up-to-date data. However, Web services do not have any predefined security model, and therefore require the additional implementation of techniques to protect exchanged information [28], as well as the deployment of a framework that enforces a strong security architecture [30].

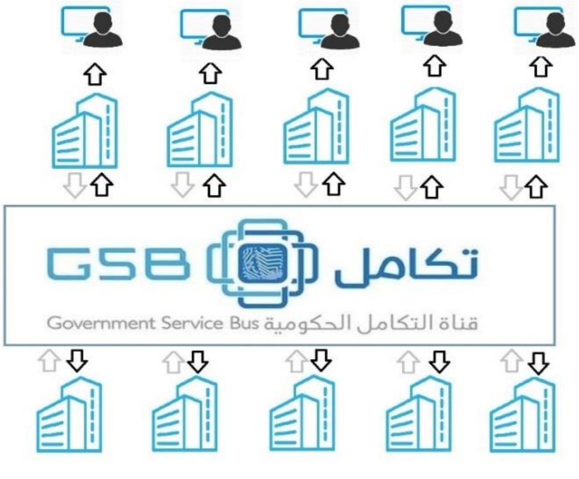

Fig. 1. GSB Overview.

Web services interact using Simple Object Access Protocol (SOAP) messages [27]. SOAP is a standard for one-way and request-response messaging transmitted over HTTP protocol. To protect SOAP messages, Advancing Open Standards for the Information Society (OASIS) set web service standards called Web Service Security (WS-Security), which is a message level security mechanism that consists of digital signature and encryption techniques [27]. SOAP messages are based on Extensible Mark-up Language (XML) data format. XML, on the other hand, is used in many areas to store, retrieve, and provide data and information in an organized format [31] and it is considered one of the most extensively used data exchange languages across the internet [32] because of its immense compatibility in transit [33]. There are many advantages in using XML data representation, such as: the notions of elements, it is extensible, it allows the separation of display and content and it can present complex structure in an easy way [32]. Nevertheless, XML falls short of guaranteeing the security by itself, and hence, a secure application framework is needed as a precondition to have it programmed as needed [32].

III. Literature Review

A. Related Work on Security of E-Governments

Technologies that have been used to maintain security in e-Governments include one-time passwords, cryptography, firewalls, analysis tools, and monitoring tools [34]. The report in [35] introduced a data classification for the e-Government of the United Kingdom which includes three security classifications (OFFICIAL, SECRET, and TOP SECRET) to indicate the level of data sensitivity and to specify how to handle personnel security, physical security, and information security over each data classification type.

The authors in [36] introduce a security model for the e-Government in United Arab Emirates (UAE) that is based on Public Key Infrastructure (PKI) (certificate and digital signature), biometrics (finger print), and hardware security tools (Tokens). Another security model for e-Government was introduced by [37] which is also based on PKI in addition to SSL channel. A proposed design for a framework for the Sudanese e-Government was introduced by [38] which suggests that the technical layer should include: an access control mechanism, authentication and password, cryptography, the use of tamper resistance protocol, a secure communication link, analysis tools, monitoring tools, bandwidth techniques, validate and filter input, and a one-time password. Another study was conducted by [39] which introduced an information security governance model for e-services in South African developing countries e-Government projects which suggests that the operational layer should include an identity management framework for authentication and authorization and a new token-based technique for implementing identity management. Their study also used DES for encryption/decryption process.

B. Related Work on XML Security Technologies

The notion of Web services has been absolutely crucial in the IT industry. Currently, all business transactions depend on Web services to achieve their desired goals [40].

However, the security of Web services is an emerging topic of discussion. To secure Web services, it is essential to secure their content which is based on XML language. XML security technologies reuse existing cryptographic and other security technologies whenever possible. It consists of XML digital signature, XKMS, XML encryption, SAML and XACML. Some of the methods used to secure XML-based Web services were introduced by [15] and the authors present the use of XML Signature to ensure the integrity and XML encryption to provide confidentiality for XML messages in Web services. In [41], the authors evaluated authentication, authorization, integration, confidentiality, and non-repudiation when using XML encryption and XML Signature in web-services in an e-business scenario and proved that all those parameters could be guaranteed when combining both XML encryption and XML signature. Meanwhile, in [33], the authors examined how XML Web security could provide privacy, certification, and integrity. They applied XML encryption and XML signature for data and messages in transaction and in storage. It was found that not only were security requirements established, but also the performance of Search Engine Optimization (SEO) was enhanced with the parsing of descriptive tags rather than unstructured data.

XML encryption and XML signature are both low level features to make the data itself secure [16]. On the other hand, Access Control is considered a high-level approach to security policies that provide secure access to data and both encryption and signature are designed to handle communication security [31]. The authors in [32] proposed an XML access control to guarantee application safety and they proved that the advantages of using XML access control are a fine-grained access on an element level, the use of different safety strategies over different parts on the same document, the use of a safety process for encryption and digital signature, and protecting network resources.

C. Related Work on Access Control

Access control is one of the key aspects of information security [42]. Access Control is a mechanism to provide privileges to a user to access a particular asset, only if this user is authorized [19] and Access Control is domain specific. Methods that are widely used in Access Control mentioned in [17], [43] are: DAC, MAC, and RBAC. There are many studies in the literature on access control methods. A study related to DAC was presented in [44] regarding its complexity, safety, and issues in object-oriented databases. RBAC was widely studied as well, and researchers in [45] proposed object sensitive role assignment, which is a generalized RBAC model for object-oriented languages.

However, much research has focused on exploring ways in which they can integrate different Access Control models to achieve better security and efficiency [17]. In [46], the authors introduced a model which combines MAC and ABAC, retaining the strict nature of MAC approach and providing more access control decisions in attributes. In [47], the authors introduced a model that consists of two layers: one layer is called the “aboveground” level and it is a traditional RBAC that is extended with environment constraints, while a second layer, called the “underground” layer, focuses on constructing attribute-based policies to automatically create primary RBAC model on the “aboveground level”. This model combines both aspects from RBAC and ABAC. Authors in [48] also proposed a model that combines features from ABAC and RBAC to provide effective access for application where there are static attributes such as qualification and city, and dynamic attributes such as the time of the day. Authors in [17] mentioned that if attributes in ABAC were chosen appropriately, they can capture the identities and access lists (DAC), security labels, clearance and classifications (MAC) and roles (RBAC). Hence, ABAC supplements those current dominant models rather than substituting them. The authors in [49] introduced RABAC, which is a Role-centric Attribute-based Access Control and this is an extension to NIST RBAC with policies for permission filtering to overcome the issue of role explosion. Other studies that were introduced to parameterize RBAC were introduced by [50] and [51]. A study by [52] proposed an attribute-based constraint specification language to express constraints in a way that it can be assigned to the attributes of different entities.

Access control for web services has been an issue that was studied in the literature as well. The authors in [53] introduced an approach to handle authorization of web requests in web services based on the concept of identity tracking and access percentile of the invoking of the web service. The authors in [54] argued that the two main issues that need to be addressed in the access control of web services are, firstly, restricting the access to authorized people, and, secondly, protecting the integrity and confidentiality of XML messages exchanged through web services. However, relying on security techniques currently used in web services such as HTTPS (HTTP over Secure Sockets Layer Protocol) cannot provide for example authorization to regulate the actions of users by allowing or disallowing an operation. Researchers in [55] proposed Authorization-based Access Control (ABAC) URL that is compatible with common web tools. A web service access control scheme was proposed in [56] where the access control scheme incorporates user password and web server log, and it grants access based on the user access behaviour by tracking the web access history. The access is granted based on the user password, date of last request, page visited (URL), and status action, association rules mining and PrefixSpan algorithms are used to match the active users’ access pattern with the user access data discovered from the user access history before being analysed to make the access decision. The authors in [57] proposed an Access Control model for information retrieval in EHR (Electronic Health Record) systems where the patient is allowed to define the access rules concerning their clinical information. The aim of their model is to increase the confidentiality and integrity of the data and raise the patients’ trust in the EHR systems. A study by [58] was conducted on Privacy-aware access control model and their use in web services. Although the generalization of data can guarantee user privacy, the over generalization of data may result in useless data, so to guarantee the right balance between data usability and the disclosure of privacy, the authors analyse how to manage an effective access process through a trust-based decision and ongoing access control policies. The authors in [59] proposed a generic access control model for the cloud that can be used with different cloud service models and it is based on Kerberos as well as access control lists and authorization tickets.

The overview of related work presented shows that many recent studies on access control focused on the field of Web services in many domains. Finding the best access control model for specific and generic domains is an emerging and current topic. Therefore, the research in this paper analyses the best access control framework that is suitable within the domain of e-Government and examines this in a real case scenario to prove its feasibility.

IV. Methodology

This research follows the steps of Design Science Research Methodology (DSRM) to present the research design. DSRM is one of the mainly used forms of methodologies in the field of Information Systems (IS); it includes the construction of new knowledge through the design of novel or innovative artefacts [60]. The Design Science process includes six steps which are outlined next.

A. Problem Identification and Motivation

The problem includes overcoming the limitations of traditional access control models and help achieve the principle of least privilege security principle.

B. Definition of the Objectives for a Solution

To define the objectives for a solution, we have explored the challenges that face the successful adoption of the e-Government program in Saudi Arabia. Researchers in [4], [61], [62] have identified security and privacy as one of the main obstacles. This is in addition to other obstacles, such as the establishment of the infrastructure, availability, computer literacy, trust, accessibility, authentication, usability, and accountability. Having security and privacy as a main issue has led (YESSER) to limit the data and services shared to preserve the confidentiality and to avoid privacy violations.

In order to achieve the above goal for e-Government Web services, specific objectives of this paper are set as follows:

- Apply a data classification scheme for the information being exchanged within and outside the GSB.
- Develop a security intermediary between the service requester and the service provider to provide authentication and authorization.
- Utilize XML security technology to provide security controls that are both fine-grained and persistent.
- Implement a case study of a real scenario within GSB using the proposed security model.

C. Design and Development

Our proposed solution is an Access Control model that will serve as a security intermediary that will intercept any access request to a web service and convert it to an authorization request to determine the suitable response output. R-MAC is a role-centric MAC model that incorporates the properties of MAC and RBAC for granting access permissions by giving clearances to roles rather than individual users to provide more flexibility and better expression of application-level security. It also utilizes XML security technologies to achieve persistent and fine-grained security over the information, even when it is outside the physical premises.

To implement the proposed model, first, we apply a dynamic role assignment. For our case study, which is the e-Government of Saudi Arabia, the role assignment within the GSB is determined by YESSER. In addition, YESSER provides Authorization using one-time password [63]. After this, we deploy a MAC model by assigning the following:

1) Classification for objects: We introduce a data classification scheme for information that is based on the Saudi e-Government security law. This classification scheme adopts the Traffic Light Protocol since it is one of the well-known data classification schemes and is widely used in different domains and systems. Traffic Light Protocol employs four colours to indicate the level of data sensitivity and the sharing boundary to be applied on recipients. For example, if the data is classified as Red, only the users that are given the clearance Red will be able to view and modify. For our case study, which is the e-Government of Saudi Arabia, the information classification is based on the Saudi e-Government law. Table I presents a summary of the Saudi e-Government law [64] that specifies the corresponding security control.

2) Clearances for subjects: An attribute is added to the roles to specify the clearance level and this is dynamically performed after the authentication step. After that, the access control model will perform a role-to-permission assignment.

By applying the Read-Down rule used in MAC [31], a subject with Red clearance can view all data classified as Red, Amber, Green, and White. A subject with Amber clearance can view all data classified as Amber, Green, and White. A subject with Green clearance can view all data classified as Green and White. A subject with White clearance can view all data classified as White. Fig. 2 illustrates this rule:

TABLE I. DATA CLASSIFICATION IN E-GOVERNMENT

Colour	Security Control	Description
Red	Top confidential	Information that may cause damage to the security of the state. Such information may only be accessed by senior officials.
Amber	Very Confidential	Information that may cause damage to public or private interests. This information is only available to specialists.
Green	Confidential	Information that relates to individual cases and may have a negative impact on the social life of the community or individuals.
White	Disclosure is not limited	Non-confidential public information.

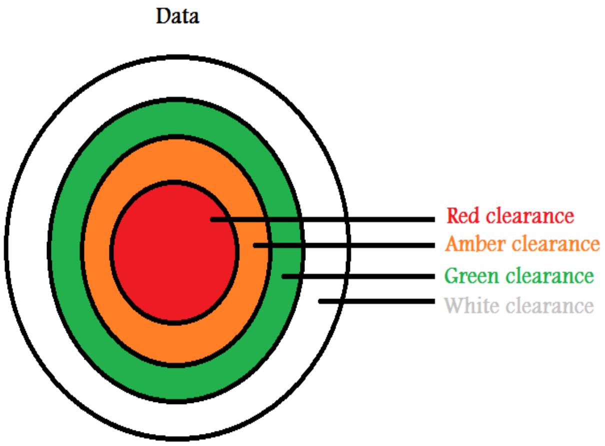

Fig. 2. Read-Down Rule.

Applying an access control mechanism that combines features from MAC and RBAC in addition to securing the data itself with XML encryption illustrated in the architecture in Fig. 3 will help overcome the limitations of traditional access control models and provide a safe platform for data exchange and distribution using web services.

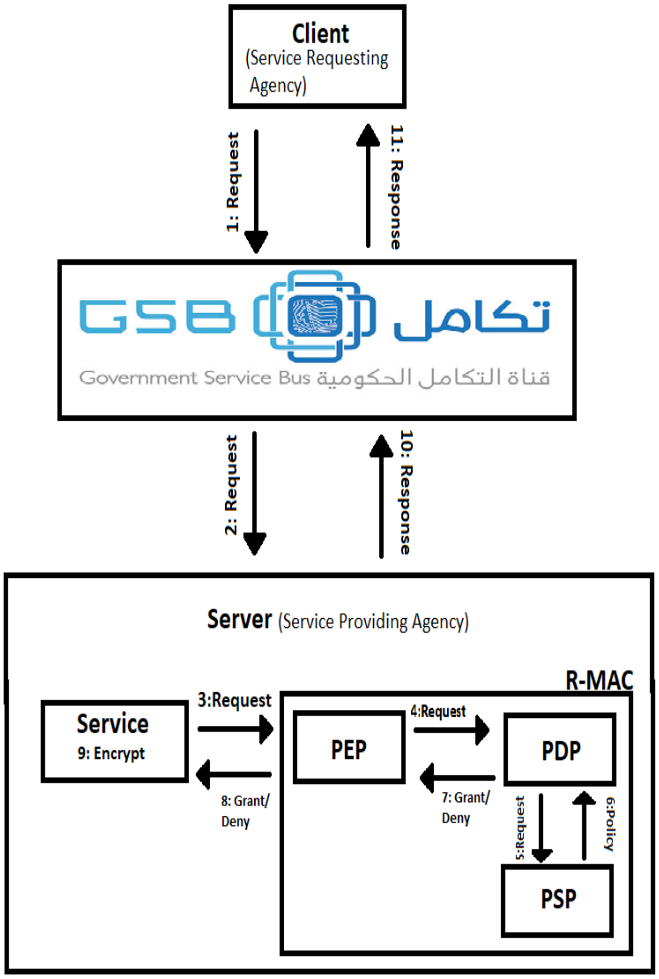

Fig. 3. R-MAC Architecture.

R-MAC model works as an intermediary that will intercept a business request and convert it into an authorization request to provide authentication and authorization for the web service through the following steps:

1) Starts when a business request is made to a service between the agencies connected to the GSB.

2) GSB managed by YESSER will provide Authentication using one-time password and role assignment for the service requesting agency and connect it with the service providing agency which acts as the server.

3) The business request is intercepted by an intermediary which is the proposed access control model (R-MAC) and converted to an authorization request by the Policy Enforcement Point (PEP).

4) The authorization request is then sent to the Policy Decision Point (PDP) to evaluate it and return the decision to the PEP.

5) To evaluate the authorization request, PDP examines the policies saved in the Policy Storage Point (PSP).

6) The suitable policy is then sent back to the PDP to Grant/Deny the access.

7) The decision is then sent to the PEP to enforce it over the service response.

8) The suitable response is then formatted.

9) The response is encrypted using XML encryption to guarantee persistent security control through the transmission of information.

*10)*The suitable response is then returned to the GSB.

*11)*The client receives the response and decrypts it using the appropriate key.

D. Demonstration

To illustrate the proposed access control model, a scenario is provided where RMAC can be implemented to help preserve the confidentiality of data and help achieve the principle of Least Privilege specified by the Saudi law. TAKAFUL charity organization was carefully studied as an exemplar.

TABLE II. INFORMATION REGARDING THE WEB SERVICE

Service Name	**Citizen Profile**
Operation Name	Retrieve the personal profile of the citizen
Service Provider	Ministry of Interior
Service Type	Information Retrieval
Process Description	The process retrieves the full profile of the entered citizen
Input	• ID Number
Output	• Full name (name) • ID information (ID) • Location of Birth (LOB) • Birth Certificate Number (BCN) • Gender • Social status (Sstatus) • Job status (Jstatus) • Life and death status (Lstatus)

TAKAFUL [65] is a charitable organization which helps under-privileged students by providing financial and psychological support. TAKAFUL organization connects with other governmental agencies and data sources to gather information regarding applicants to determine their eligibility such as the Ministry of Interior, the Ministry of Civil Services, General Organization of Social Insurance, Public Pension Agency, Ministry of Commerce and Investment, Ministry of Labor and Social Development, Ministry of Justice and the Ministry of Education.

Our chosen scenario, which is a part of the Eligibility Process, is the interaction between TAKAFUL as a data consumer and the Ministry of Interior (MOI) as a data owner in order to check the status of the parents. Table II provides information regarding this service.

The previous Web service from Table II was implemented where the proposed access control model serves as a security intermediary between the service providing agency and other agencies connected to the GSB. It will deploy a MAC model where the access rights are constrained by the system based on a data classification scheme. The policies were specified using XACML as a separate component to give it more flexibility since data and users can be updated without affecting the policies. Finally, based on the clearance level, classified information is displayed.

E. Evaluation

The evaluation and validation of the proposed model have two dimensions, which are as follows:

1) Testing the model with test cases and comparing the expected output with the actual output to determine that the model works as expected. The test cases proved that the expected output matches the actual output.

2) Checking the value and usability aspects of the model by distributing the validation form developed in [66] to help the participants in selecting the rate of validity from different success standards. The validation form was distributed among five highly recognized security practitioners in e-Government. The results of the analysis confirmed the standards contained in the success of the proposed model. However, some of the suggestions include utilizing a robust authentication mechanism that is not weaker than 2-factor authentication: for instance, a strong password and hardware token.

The advantages of adopting the proposed model include:

- Applying a Role-Centric MAC model provides more flexibility to it since the clearances will be given to roles rather than individual users.
- Adopting our proposed data classification scheme and role clearance provides a fine-grained control to enforce the principle of Least Privilege.
- Utilizing XML security technologies provides a persistent and fine-grained end-to-end security control even when the information is outside the physical premises.

F. Communication

The final step of DSRM is publications in academic journals and professional outlets.

V. Conclusion

The security of e-Government services is one of the major concerns nowadays, especially in terms of the confidentiality of data owned by the e-Government agency. In order to provide specialized online services, governments must interconnect and exchange pieces of information to paint the full picture and make informed decisions. This exchange of information can compromise the integrity, confidentiality, or availability of that information. This paper proposes an access control model that overcomes the limitations of traditional access control models by combining features from MAC and RBAC and by giving clearances to roles rather than individual users to give it more flexibility and better expression of application-level security. This paper also introduces a data classification scheme that will help preserve the security of the information being exchanged within and outside the GSB by providing a fine-grained access control model that complies with the Saudi law which strictly grants access on a Least Privilege security principle basis that enables fine-grained access control. In addition, XML security technologies are utilized to achieve persistent and fine-grained control over the data even when it resides outside the physical premises. The proposed access control model, which uses the combined R-MAC model along with the suggested classification scheme and enforces it through the XML security technology, is novel. The information classification scheme with the corresponding clearance levels proposed in this work is the result of an analysis of the Saudi e-Government law. The proposed model was evaluated with a case study of the interaction conducted through the GSB and it shows that the principle of Least Privilege is enforced, and the security of data is preserved.

The presented work in this paper provides the basis for accomplishing a secure access control model that can provide flexible, fine-grained, and persistent access control for the information shared in Saudi e-Government interaction. However, the novel access control model proposed could be applied in any collaborative cloud-based environment with its own data classification scheme to address the limitations in the current security models. Moreover, other classification schemes and role clearances could be investigated to achieve different granularity of control.

Another aspect that is worthy of further study relates to the role assignment process. Currently, the role assignment process in the e-Government of Saudi Arabia is performed by the administration of YESSER. However, in the future, it would be beneficial to introduce a specific mechanism for the role assignment process since accurate role assignment is a key to preventing privacy violations.

The proposed utilization of XML security technologies presented in this research includes a basic symmetric key encryption for the XML formatted documents. However, in the future, it is crucial to establish a Public Key Infrastructure (PKI) to manage digital certificate and public-key encryptions.

Acknowledgments

This research was sponsored by the Deanship of Graduate Studies at King Saud University.

References

[1] F. Sá, Á. Rocha, and M. P. Cota, “Potential dimensions for a local e-Government services quality model,” Telemat. Informatics, vol. 33, pp. 270–276, 2016.

[2] A. M. Al-Khouri, M. Farmer, and J. Qadri, “A Government Framework to Address Identity, Trust and Security in E-government: the Case of UAE Identity Management Infrastructure,” Eur. Sci. J., vol. 10, no. 10, pp. 85–98, 2014.

[3] H. Ritchi, I. Wahyudi, and A. Susanto, “Research Program on Key Success Factors of e-Government and Their Impact on Accounting Information Quality,” in 2nd Global Conference on Business and Social Science, 2015, vol. 211, pp. 673–680.

[4] S. S. Basamh and H. A. Qudaih, “E-Government Implementation in the Kingdom of Saudi Arabia: An Exploratory Study on Current Practices, Obstacles & Challenges,” Int. J. Humanit. Soc. Sci., vol. 4, no. 2, pp. 296–300, 2014.

[5] E. Nyakwende and A. Al Mazari, “Factors Affecting the Development of e-Government in Saudi Arabia,” in International Conference on Electronic Government and the Information Systems Perspective, 2012, pp. 19–28.

[6] P.-L. Sun, C.-Y. Ku, and D.-H. Shih, “An implementation framework for E-Government 2.0,” Telemat. Informatics, vol. 32, no. 3, pp. 504–520, 2015.

[7] M. Zubi and H. Alonaizat, “E-government and Security Requirements for Information Sysytems and Privacy(Performance Leakage),” J. Manag. Res., vol. 4, no. 4, pp. 367–375, 2012.

[8] R. G. Hassan and O. O. Khalifa, “E-Government- An Information Security Perspective,” Int. J. Comput. Trends Technol., vol. 36, no. 1, pp. 1–9, 2016.

[9] National Enterprise Architecture Office Management at Yesser, “National Application Reference Model,” e-Government Program (Yesser), 2015.

[10] YESSER, “YEFI - Data Standards Catalogue,” Kingdom of Saudi Arabia, 2008.

[11] M. E. Whitman and H. J. Mattord, Management of information security. Stamford: Cengage Learning, 2014.

[12] S. Saha, D. Bhattacharyya, T. Kim, and S. K. Bandyopadhyay, “Model Based Threat and Vulnerability Analysis of E-Governance Systems,” Int. J. u- e- Serv. Sci. Technol., vol. 3, no. 2, pp. 7–22, 2010.

[13] S. Al-Salamah and M. J. Hilton, “Towards Information Sharing in Virtual Organisations: The Development of an Icon-based Information Control Model.,” Cardiff University, United Kingdom, 2009.

[14] S. Alsalamah, A. Gray, J. Hilton, and H. Alsalamah, “Information Security Requirements in Patient-Centred Healthcare Supporting Systems,” in 14th World Congress on Medical and Health Informatics (Medinfo), 2013, pp. 812–816.

[15] G. Yue-sheng, Y. Meng-tao, and G. Yong, “Web Services Security Based on XML Signature and XML Encryption,” J. Networks, vol. 5, no. 9, pp. 1092–1097, 2010.

[16] M. Zubi and H. Alonaizat, “e-Government and Security Requirements for Information Systems and Privacy(Performance Leakage),” J. Manag. Res., vol. 4, no. 4, pp. 367–375, 2012.

[17] Xin JinRam, KrishnanRavi, and Sandhu, “A Unified Attribute-Based Access Control Model Covering DAC, MAC and RBAC,” in IFIP Annual Conference on Data and Applications Security and Privacy, 2012, vol. 7371, pp. 41–55.

[18] B. P. Verma, S. Kumar, and P. Sharma, “A novel approach for Multi-Tier security for XML based documents,” IOSP J. Comput. Eng., vol. 5, no. 4, pp. 1–4, 2012.

[19] S. Chatterjeea and T. Sarmah, “An Efficient Fine Grained Access Control Scheme Based On Attributes For Enterprise Class Applications,” 2014 International Conference on Signal Propagation and Computer Technology (ICSPCT). pp. 273–287.

[20] Saudi Government, “Saudi Arabia’s Vision 2030,” 2016. [Online]. Available: http://vision2030.gov.sa/en/ntp).

[21] YESSER, “National transformation program 2020,” 2016. [Online]. Available: http://vision2030.gov.sa/sites/default/files/NTP_En.pdf.

[22] Ministry of Communication and Information Technology, “Ministry of Communication and Information Technology,” MCIT, 2017. [Online]. Available: http://www.mcit.gov.sa/En/Pages/default.aspx.

[23] Ministry of Interior, “Ministry of Interior,” 2017. [Online]. Available: https://www.moi.gov.sa/wps/portal/Home/Home.

[24] G. Tokdemir and Y. Paçin, “Adoption of e-government services in Turkey,” Elsevier Comput. Hum. Behav., vol. 66, pp. 168–178, 2016.

[25] K. K. Smitha and K. Chitharanjan, “Security of Data in Cloud based E-Governance System,” Spec. Issue Int. J. Comput. Appl. Adv. Comput. Commun. Technol. HPC Appl., pp. 1–6, 2012.

[26] YESSER, “YEFI – Yesser Framework For Interoperability,” 2005.

[27] D. Jamil and H. Zaki, “Security Issues in Cloud Computing and Countermeasures,” Int. J. Eng. Sci. Technol., vol. 3, no. 4, pp. 2672–2676, 2011.

[28] N. Dilber, “Restful web services security by using ASP.NET web API MVC based,” J. Indep. Stud. Res., vol. 12, no. 1, pp. 4–10, 2015.

[29] K. S. Tharun, M. Prudhvi, and S. S. Reddy, “Advantages of WCF Over web services,” Int. J. Comput. Sci. Mob. Comput., vol. 2, no. 4, pp. 340–345, 2013.

[30] S. Subashini and V. Kavitha, “A survey on security issues in service delivery models of cloud computing,” J. Netw. Comput. Appl., vol. 34, pp. 1–11, 2011.

[31] N. S. Farooqi and D. S. North, “Applying Dynamic Trust Based Access Control to Improve XML Databases Security.,” University of Sheffield, 2013.

[32] H. Zhang, Q. Guan, and W. Luo, “The Study of Access Control Model Using XML,” Int. J. Secur. Its Appl., vol. 9, no. 7, pp. 179–188, 2015.

[33] R. Menaka and B. Ashadevi, “Survey on Signatured Xml Encryption for Multi-Tier Web Services Security,” Indian J. Sci. Technol., vol. 9, pp. 1–10, 2016.

[34] S. Singh and S. Karaulia, “E-Governance: Information Security Issues,” in International Conference on Computer Science and Information Technology (ICCSIT’2011), 2011, pp. 120–124.

[35] cabinet office, “Government Security Classifications,” 2014.

[36] J. T. Jaafar, N. Hamza, and N. Hamza, “Security Model in E-government with Biometric based on PKI,” Int. J. Comput. Appl., vol. 93, no. 6, pp. 33–39, 2014.

[37] W. Zhong, “Research On E-Government Security Model,” in International Conference on E-Business and E-Government, 2010, pp. 699–702.

[38] O. Ali, “A proposed Design of a Framework for Sudanese E-Government Security Model,” Sudan University of Science and Technology, 2017.

[39] A. Ramtohul and S. Soyjaudah, K, M, “Information security governance for e-services in southern African developing countries e-Government projects,” J. Sci. Technol. Policy Manag., vol. 7, no. 1, pp. 26–42, 2016.

[40] S. Gadwar and D. Sable, “Securing Web Services Based on XML Signature and XML Encryption,” Int. J. Res. Advent Technol., vol. 2, no. 2, pp. 1–5, 2014.

[41] G. Abraham, Krishnakumar, Venkatasubramanian, and K. Borasia, “Securing Web Services Using XML Signature and XML Encryption,” School of Computer Science and Engineering, VIT University, Vellore, India, 2013.

[42] S. Gostojić, G. Sladic, B. Milosavljević, and Z. Konjovic, “Context-Sensitive Access Control Model for Government Services,” J. Organ. Comput. Electron. Commer., vol. 22, no. 2, pp. 184–213, 2012.

[43] S.Nagaraju, L. Parthiban, and S. Kumar, “An Enhanced Symmetric Role-Based Access Control Using Fingerprint Biometrics for Cloud Governace,” Parallel Cloud Comput. Res., vol. 1, no. 2, pp. 11–16, 2013.

[44] S. Dranger, R. Sloan, and J. Solworth, “The complexity of discretionary access control,” Proceeding IWSEC’06 Proc. 1st Int. Conf. Secur., pp. 405–420, 2006.

[45] J. Fisher, D. Marino, R. Majumdar, and T. Millstein, “Fine-Grained Access Control with Object-Sensitive Roles,” in European Conference on Object-Oriented Programming, 2009, pp. 173–194.

[46] L. Kerr and J. Alvis-foss, “Combining Mandatory and Attribute-Based Access Control,” in 49th Hawaii International Conference on System Sciences (HICSS), 2016, pp. 2616–2623.

[47] Y.-H. Chen, C.-H. Lu, and P.-Y. Hsu, “Multilayered Information Encryption Scheme with Fine-grained Authentication,” in Proceedings of APSIPA Annual Summit and Conference 2015, 2015, pp. 1126–1130.

[48] D. R. Kuhn, E. J.Coyne, and T. R.Weil, “Adding Attributes to Role-Based Access Control,” IEEE Comput., vol. 43, no. 6, pp. 79–81, 2010.

[49] X. Jin, R. Sandhu, and R. Krishnan, “RABAC: role-centric attribute-based access control,” in Proceedings of the 6th international conference on Mathematical Methods, Models and Architectures for Computer Network Security: computer network security, 2012, pp. 84–96.

[50] A. Abdalah and E. Khayat, “A Formal Model for Parameterized Role-Based Access Control,” in Formal Aspects in Security and Trust, 2004, pp. 233–246.

[51] M. Ge and S. Osborn, “A Design for Parameterized Roles,” in Research Directions in Data and Applications Security XVIII, 2004, pp. 251–264.

[52] K. Bijon, R. Krishnan, and R. Sandhu, “Towards An Attribute Based Constraints Specification Language,” in international conference on Social Computing (SocialCom), 2013, pp. 108–113.

[53] R. Nath and G. Ahuja, “An Authorization Mechanism for Access Control of Resources in the Web Services Paradigm,” Int. J. Adv. Comput. Sci. Appl., vol. 2, no. 6, pp. 36–42, 2011.

[54] C. A. Ardagna, “A Web Service Architecture for Enforcing Access Control Policies,” Electron. Notes Theor. Comput. Sci., vol. 142, no. 3, pp. 47–62, 2006.

[55] G. Swamynathan, T. Close, and S. Banerjee, “Scalable Access Control ForWeb Services,” in the fifth international conference on Creating, Connecting and Collaborating through Computing, 2007.

[56] S. Elsheikh, “Access control scheme for Web services (ACSWS),” in international conference on Computer and Communication Engineering, 2008.

[57] M. Sicuranza, A. Esposito, and M. Ciampi, “An access control model to minimize the data exchange in the information retrieval,” J. Ambient Intell. Humaniz. Comput., vol. 6, no. 6, pp. 741–752, 2015.

[58] M. Li, X. Sun, H. Wang, Y. Zhang, and Z. Ji, “Privacy-aware access control with trust management in web service,” World Wide Web, vol. 14, no. 4, pp. 407–430, 2011.

[59] H. Kaffel-Ben Ayed and B. Zaghdoudi, “A generic Kerberos-based access control system for the cloud,” Ann. Telecommun., vol. 71, no. 9–10, pp. 555–567, 2016.

[60] K. Peffers, T. Tuunanen, M. A. Rothenberger, and S. Chatterjee, “A Design Science Research Methodology for Information Systems Research,” J. Manag. Inf. Syst., vol. 24, no. 3, pp. 45–78, 2007.

[61] J. Al-Khouri, A. M., &Bal, “Electronic Government in the GCC Countries,” Int. J. Soc. Sci., vol. 1, no. 2, pp. 83–98, 2007.

[62] O. Alshehri, M., Drew, S., &Alfarraj, “A Comprehensive Analysis of E-government services adoption in Saudi Arabia: Obstacles and Challenges.,” High. Educ., vol. 8, no. 2, pp. 1–6, 2012.

[63] e-G. P. (YESSER), “No Title,” Single sign-on (SSO), 2017. [Online]. Available: https://www.yesser.gov.sa/EN/buildingblocks/pages/the_single_sign-on.aspx.

[64] National Center for Documentation and Archives, “List of Documents to be Consulted and Circulated,” 2004.

[65] TAKAFUL Charity Foundation, “TAKAFUL,” 2017. [Online]. Available: https://www.takaful.org.sa/.

[66] M. Lankhorst, Enterprise Modelling, Communication and Analysis, vol. 2. London, United Kingdom, 2009.