Secure Cloud-Mediator Architecture for Mobile-Government using RBAC and DUKPT

https://doi.org/10.3991/ijim.v14i04.11075

Qasem M. Kharma (✉), Nidal M Turab, Qusai Shambour, Mohammad Hassan
Al-Ahliyya Amman University, Amman, Jordan
q.kharma@ammanu.edu.jo

Abstract—Smart mobile devices and cloud computing are widely used today. While mobile and portable devices have different capabilities, architectures, operating systems, and communication channels than one another, government data are distributed over heterogeneous systems. This paper proposes a 3-tier mediation framework providing single application to manage all governmental services. The framework is based on private cloud computing for adapting the content of Mobile-Government (M-Government) services using Role-Based Access Control (RBAC) and Derive Unique Key Per Transaction (DUKPT). The 3-layers in the framework are: presence, integration, and homogenization. The presence layer is responsible for adapting the content with regard to four contexts: device, personal, location, and connectivity contexts. The integration layer, which is hosted in a private cloud server, is responsible for integrating heterogeneous data sources. The homogenization layer is responsible for converting data into XML format. The flexibility of the mediation and XML provides an adaptive environment to stream data based on the capabilities of the device that sends the query to the system.

Keywords—Mobile-government, M-Government, Content Adaptation, User Context, Government, mediation, cloud computing, Role Base Access Control.

1 Introduction

Nowadays, people are using various technologies in order to complete their day-to-day transactions. Some of the most important transactions are governmental, such as follow up applications, querying of records, submission of applications, etc. These data are distributed over many governmental units that use various applications and apply diverse restrictions on accessing data. These databases are heterogeneous in structure and name of conventions. All ministries maintain a website and mobile application, and in most cases, these websites and mobile applications are informative. Unfortunately, these applications are not integrated, and in most cases, the application support transaction inquires only. Therefore, because of the lack of cooperation among governmental units in m-government, there is a need to design mobile application that can handle the interoperability and integration of governmental applications [1, 2].

On the other hand, people these days use different technologies such as smartphones and PDAs. Although these devices have the capabilities similar to personal computers in terms of Internet connection and browsing, they have different operating systems and different capabilities, such as differing Internet connection speeds and screen resolutions [1]. These differences between mobile devices will affect content presentation and usability [2]. Portability is an important factor that encourages people to use technologies; on the other hand, content presentation, integration, and security need to be taken into consideration [2].

Another factor that affects the adoption of technology is the recent increase in high-speed communication infrastructures [1, 3, 4] and computer services which have allowed organizations to host their data on cloud computing database servers. Cloud computing has many important advantages such as the ability to store large quantities of data, the fast data query processing, and the high data availability. In addition, initial acquisition costs in cloud computing are lower than self-hosted data management. Cloud computing hosting allows organizations to focus their money and resources on expertise rather than on information technology. Yet, trust issues between data owners, data users, and cloud data storage service providers limit the usability of these systems.

In this research, we propose a framework for handling the two aforementioned problems: accessing heterogonous data sources and manipulating different presentations for mobile devices using cloud computing. The solution is based on a cloud mediation framework to be placed on top of the data sources using private cloud computing. This framework will be in charge of solving the problem of having different data structures and namings. Also, when a new device is connected to the mediator, it will promote its capabilities and will be taken into consideration when returning the data. Therefore, our framework is capable of handling a heterogeneous data source and delivering data in different formats.

This paper describes the framework for a single mobile application for M-Government based on mediation architecture using role-based access control. Section 2 presents some related works, and Section 3 describes M-Government as well as the differences between E-Government and M-Government. Section 4 describes the mediation framework, and we conclude by noting some future features that can be added to the framework.

2 Related Works

Today, many countries and researchers invest in developing M-Government not only to automate the government processes but also to enhance services by adopting new technologies such as portable devices and communication technologies [1, 2]. Kumar and Sinha [5] discussed the technologies and challenges that affect adopting an M-Government as shown in Figure 1. The authors analyzed M-Government applications, and they evaluated mobile technologies (MTs) which are used in M-Government. They have also categorized E-Government services into four categories: government-to-citizen, government-to-employee, government-to-government, and government-to-business. Furthermore, the authors discussed two main challenges of M-Government in

adapting these technologies: privacy and security, and accessibility. Our proposed framework integrates data from heterogeneous resources, then presents the content on different devices to enhance the services for the users which increases the usability of the m-government.

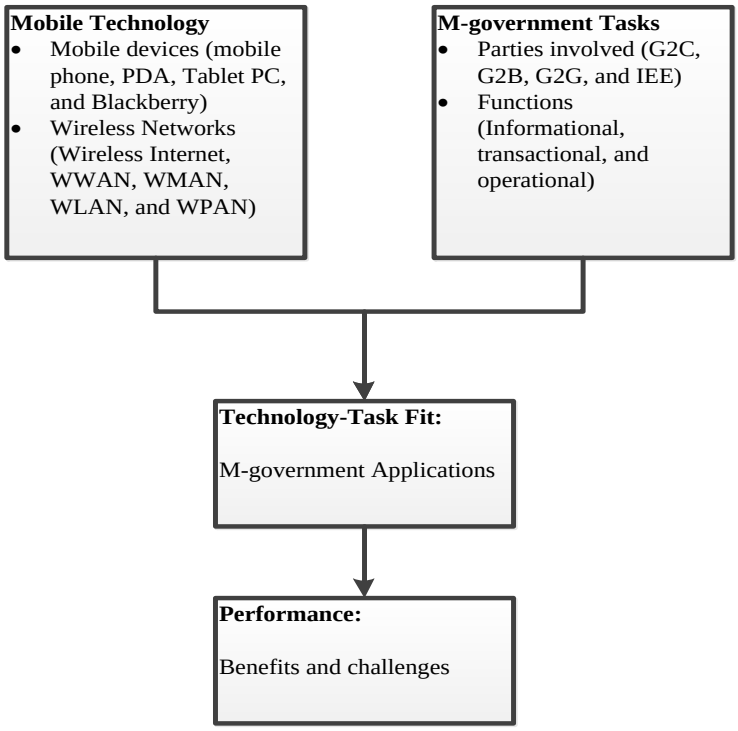

Fig. 1. A framework for understanding m-government [5]

Sheng and Trimi [6] discussed M-Government in terms of some technologies and policies, as well as the content and presentation management of M-Government. The authors proposed a Content Management System (CMS) to utilize the content. Their framework was based on adopting an enterprise-wide web and content design standards. The framework used the Extensible Markup Language (XML), Extensible Style Sheet Language (XSL), and Simple Object Access Protocol (SOAP) technologies. Like the proposed framework in this paper, XML is used in a global mediation schema and in connector schema.

Al-khamayseh, et al. [7] proposed a framework for M-Government that takes into consideration geographical location awareness and personalization techniques such as recommender systems to ensure the delivery of the correct service to the right users. The architecture is based on four main components: content server, application server, gateway, and mobile location center. The proposed architecture focuses on delivering informative messages based on location and personalized features.

Roggenkamp [8] emphasized that M-Government could support government strategies. In order to get benefits from mobile technologies, user's needs and technologies should be considered when developing an M-Government application. Also, the author describes the characteristics of mobility, which are spatial, temporal, and contextual mobility. In addition, the author describes three user needs: user's readiness to use certain technological innovations, user's willingness to do so, and user's requirements collection.

Different mediation frameworks have been proposed [9-14] to be deployed as a middleware to resolve heterogeneous data sources integration. In general, this middleware is deployed on top of heterogeneous data sources and provides services to applications that are deployed on the top of the mediator. The main role of the mediator is to manage heterogeneous structures and to present the results to a client. An example of an architecture that uses a mediator and cloud technologies was presented by Ege [15]. The proposed architecture is a framework that is based on a 3-layer mediator architecture and is implemented in an augmented reality presentation. Each layer can be maintained by several mediators which is based on a cloud-server. A cloud-mediator receives requests from a client and compiles the data to generate a life-like presentation. The solution is based on peer-to-peer cloud computing, and mediator architectures to provide a life-like presentations. Our proposed framework is a relax version of a 3-layer mediation framework, hosted the mediation of global schema in a cloud server.

One of the risks of using cloud computing is security. Therefore, data need to be encrypted to secure data accessing in cloud [16, 17]. Besides, when using a database, users should execute transactions according to their roles. Role-Based Access Control (RBAC) is to authorize accessing data in large systems [18]. Yang, et al. [19] suggested to implement RBAC in mediation architecture to authorize accessing to data.

3 M-Government

A government is a dynamic mixture of goals, organizations, services, and roles [20]. The main responsibility of any government is to provide its functions and services in an improved style, using different resources and communication channels to enhance the quality of delivery service. All new government web and mobile applications are aligned with government strategies by providing services in an electronic format.

As the usage of mobile devices to provide governmental services and functions gains increasing interest based on the mobility of users, the need to extend these services and functions using the Anytime, Anywhere, on Any Device (ATAWAD) concept also increases. The mobility feature is the main difference between M-Government and E-Government or any other developments in the government sectors [21]. Statistics show that mobile devices have a better reach than any other technology, such that in 2017, two thirds of the worldwide populace were mobile owners [22].

Mobility refers to two key components: first, user mobility means using public services anytime, anywhere and on the go, and second, the mobility of equipment that is applied in M-Government such as mobile and tablet devices. In this research paper, we describe M-Government as a flexible delivery of public functions and services through

mobile devices and through using wireless technologies to support the concept of anytime and anywhere services.

Any mobile device that can be used in M-Government must attain some important requirements such as the capability to distribute governmental services and the capability to support customer mobility. According to these requirements, smart phones and other mobile devices can be the best tool for use in M-Government. Mobile devices are any devices that are small in size, autonomous, and unobtrusive enough to support one in every moment of one's daily life [23].

3.1 M-Government services

Norris and Moon [24] classified the M-Government services into three categories: informational, transactional and operational. Informational services are one-way communications in which government broadcasts are sent to users. Informational services are also used to send alerts and warnings to the user through SMS [25], e-mail, or push notifications[26]. Transactional services are two-way communications in which the government and the user send and/or receive information. This category of services permits consumers to interact with governmental organizations, such as online procurement and payments. The last category of services is operational services that target the internal governmental processes and enable the government staff to access information using their mobile devices. This research paper focuses on the content of the informational and operational services and identifies the ways that this content must be modified and adapted to meet customer preferences, locations, and technologies.

3.2 M-Government heterogeneous data sources

The governmental data sources are distributed over many ministries and departments. Each ministry uses its own information system, and some ministries maintain different information systems for their different departments, one information system for each department. As a result, the data are considered heterogeneous because of their structures and naming are different. Also, each organization applies different roles of access to their data. In order to manipulate those sources efficiently, data must be homogenized to solve all naming and structure differences.

Many mediation architectures have been proposed in the last two decades [9-12, 27-31]. All these architectures aim to integrate heterogeneous data sources and present results to a higher layer of mediation. However, there are three main differences among mediation architectures. First, they are different in work distribution among the several layers in the mediation architecture. Some of the architectures delegate more work to the wrappers while others design the wrapper to be as simple as possible. Secondly, the common data model which is used in communication between layers is different. While some architectures use an object-oriented model such as Garlic[12, 30, 31], or an object-oriented like model such as TSIMMIS [7, 28, 29], others use semi-structured models such as MIX [9, 10, 13]. Finally, the mediation architectures differ in the degree of centralization. For instance, some architectures maintain global schemas while others distribute the mediation schema over domain-specific mediators. The degree of schema

distribution will not only affect the system's reliability but will also control the integration process.

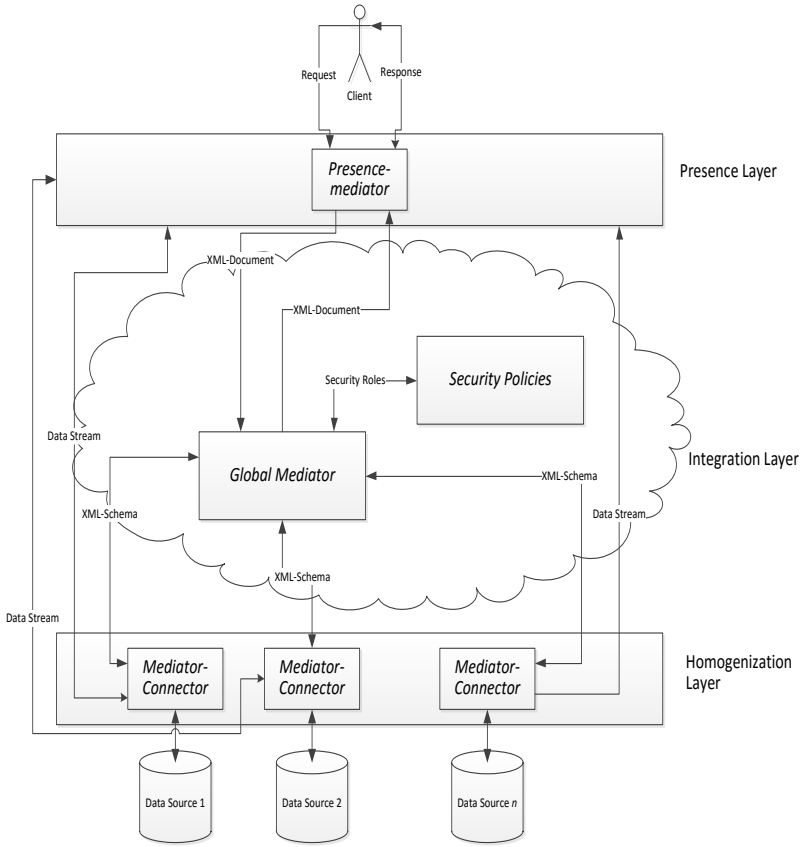

Fig. 2. 3-layer Mediation Architecture

4 Proposed Framework

The aforementioned M-Government functions can be enhanced using a single mobile application that provides stakeholders with online-requested information and sends alerts and notifications to users. The proposed framework supports a single application to access multiple services from different departments without transferring the actual data to the mediation server. In the following sections, an M-Government mediation framework based on private-cloud mediation architecture is introduced. The cloud servers are distributed over many governmental units using the proposed framework by Fan and Perros [32].

4.1 Adapting mediation architecture

We opt to choose a relaxed version of the proposed 3-layer mediation architecture [13, 27, 33] (Figure 2). The integration layer will be simplified, since each query will be served by only one server, and since data sources are disjoined.

The nature of data is distributed. Because of the breakthroughs in communication, it has become feasible to access the distributed data sources. Wireless telecommunication increases users' desires to access data sources from wireless computing devices such as Personal Digital Assistant devices (PDAs). Unfortunately, in most cases, distributed data sources are heterogeneous in platforms, types, and structures. One suggested solution is to integrate heterogeneous data sources through mediation.

The 3-layered architecture [33], which was designed by Secure System Architecture research group (SSA) at Florida International University (FIU), is a 3-layer mediator-based architecture that provides a dynamic and scalable framework for telecommunication software environments. The architecture uses XML, so it is capable of managing various data types. The architecture is based on three layers; a presence layer which takes requests from clients who use the M-Government application. It is responsible for the caching and buffering of streams that it receives from the integration and homogenization layers. Also, the presence layer is responsible for formatting the delivered data based on the device capabilities. The second layer is the integration layer. It is responsible for indexing the participated data sources, applying security roles before forwarding the request to the data sources, and negotiating between heterogeneous naming and datatypes. The integration layer also maintains the global schema, which is an XML formatted file, to solve the naming convention in different sources. Besides, the global schema maintains the connector data. The third layer is the homogenization layer, where a connection to the actual data sources is established, where data is converted into an XML file to be sent to the presence layer.

4.2 Mediation security framework

To secure our proposed M-Government architecture, a set of requirements must be met. The first requirement is that both transaction parties should know the identity of each other. The second requirement is that all communications between parties must be secured. The third requirement is to ensure that any transaction is not altered or modified during transmission. Last set of requirements is to ensure that the services provided to each user are in accordance to his\her role.

The first stage is the registration process (Figure 3) starts when the user sends a registration request to the intended M-Government global mediator. The sent request includes the proposed user name and the national ID. The security component checks whether the ID is valid; if it is, the user's name is further checked for duplication and complying with the user name's policy roles. After that, the username is verified and stored in the authentication repository in the security component. The authentication process is centralized using central authentication server hosted in Integration Layer to provide central authentication repository.

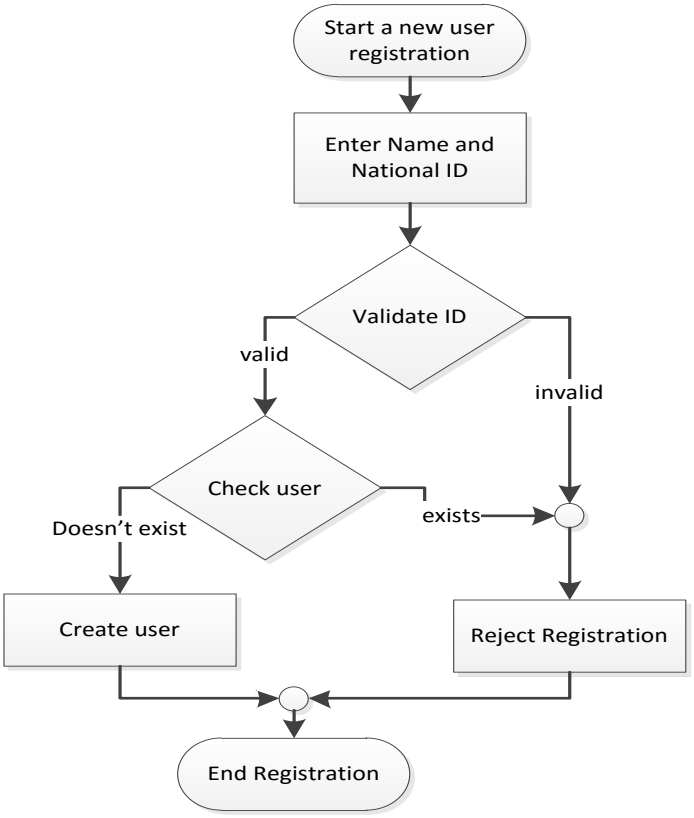

Fig. 3. Registration Process

The transaction between the user and the M-Government (Figure 4) starts by authenticating the user, which submits user's name and password pair to the security component, and then checks whether the user is valid or not. There are two cases: either the user's name is invalid, or the password is not. Here the user is given three attempts to submit, after that his account will be locked. If the user submits a valid username and password, he will be assigned privileges according to the Role Based Access Control (RBAC) and will be forwarded to the intended service.

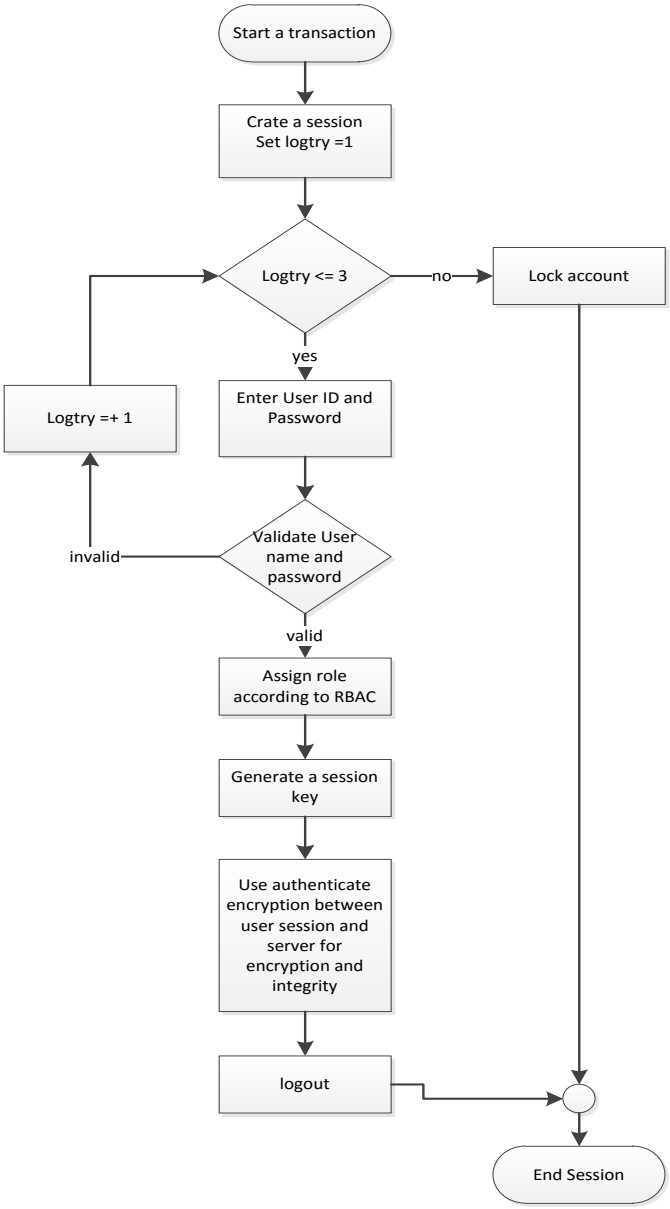

Fig. 4. Transaction Authorization Using RBAC

RBAC is an approach to restrict system access of authorized users within the M-Government. Theroles are created for various access services based on predefined groups of the users. A user may be assigned with more than one group, but at most one group belongs to a specific governmental unit. Accordingly, permissions are assigned to specific users due to specific roles. Every user belongs to a set of groups, where a set

of roles are applied to each group to assign them the necessary permissions of the intended service(s). Users inherit permissions from groups to which they belong.

The proposed RBAC for the M-Government is shown in (Figure 5)

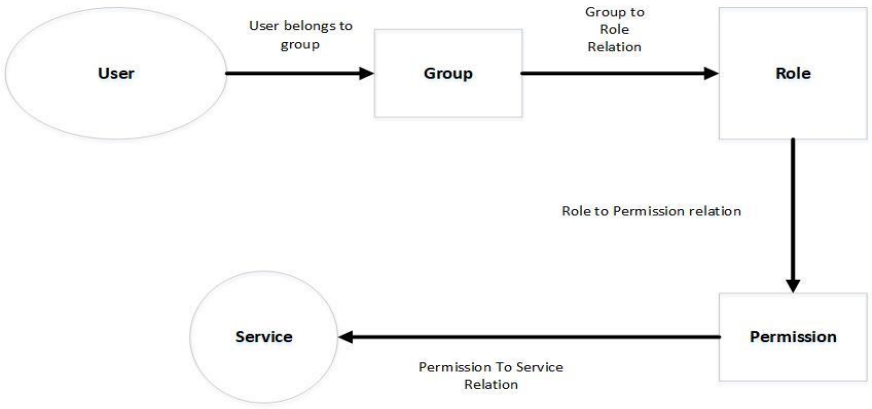

Fig. 5. Assigning Roles to Users Base on RBAC

In Figure 5, the components of the RBAC are: U = User, G= Group of Users, R=Role, M=Permission and S= Service respectively. While the relations between the components using Set Theory terminology are as follows:

- User Group: $U \rightarrow P(G) - \emptyset$ (a user can be assigned to one or more group)
- Group cannot be an empty group $G \neq \emptyset$
- Group Role: $G \rightarrow P(R)$ (Each group is mapped to a set of role(s), so the Group to Role relation is many-to-Many mapping)
- Permissions: $R \rightarrow P(M \times S)$ (a role is mapped to the power set of the Cartesian product of Permission and Service).

The transaction process is secured by proper encryption technique, after the user is registered, authenticated and granted access to the intended resources. The proposed framework uses authenticated encryption techniques for both encryption and message integrity in the integration layer. Encryption and message integrity use a single processing step. The authenticated encryption schema is Hummingbird-2 that uses 128-bit key that is efficient in both hardware and software implementations.

The operation of Hummingbird-2 can be summarized as the following. The Hummingbird-2 cipher has a 128-bit secret key (K), a 128-bit internal state (R), and a 64-bit Initialization Vector (IV). Hummingbird-2 encryption utilizes different operations on 16-bits words: The X-OR ($\oplus$), the modulo 216. In addition to a nonlinear mixing function f(x) that consists of S-Boxes of four bits permutation lookups on each 4-bits(nibble) of a word, followed by some linear mix. After the encryption process, the hash of the header and nonce are computed and transmitted alongside with the encrypted message [34, 35].

An essential part of the encryption and authentication stages is the secret key, which needs to be shared and kept secretly between the user and the integration layer. Another challenge of the shared secret is how to distribute the key between the user and the integration layer. One promising solution is the use of Derive Unique Key Per Transaction (DUKPT) [36] , which is a key management scheme rather than an encryption scheme. In DUKPT a unique key is derived from a master key and used. If this unique key is compromised neither the future nor the past keys will be affected because there is only one single key for each transaction.

The specifications of DUKPT algorithm needs an initial single key known as Base Derivation Key (BDK). Both communication parties: the recipient of the encrypted messages and the encrypting device manufacture. However, in the case of M-Government there is no specific encrypting device manufacture, as the users used to use mobile devices from various manufacturers. Our proposed solution is as follows:

- For a specific user i, the authentication server at the security layer sends a PIN code or Nonce to the user device denoted by (Ni)
- Ni is used with the MACi address of the mobile device to derive the BDK: BDKi → f (Ni, MACi)
- A table that maps BDK and MAC address pairs is stored at the authentication server at the security layer.
- The BDK is used to derive Initial PIN Encryption Key (IPEKi) and injected to the user's mobile device, the BDK cannot be derived from the IPEK
- The IPEKi used to derive future keys used for future transaction between the device and the service, and then the IPEKi is discarded to ensure it will not be used again.
- One of the future keys is used for specific transaction; this key has a serial number composed of the mobile device MAC address and Internal counter. This key is sent along side with the encrypted message to the security layer.
- At The security layer, the BDKi is located, IPEKi is derived using information contained in the key serial number. The IPEK generates session key to decrypt the message [36, 37].

4.3 Adapting content presentation

Content adaptation which will be the responsibility of the presence layer, and is a key part in designing M-Government applications [38]. The presence layer receives an XML file that includes the data to be presented to the user. The presence layer adapts the data in the received contents according to the device settings in the application in which it is installed. The settings include mobile device context, personal context, connectivity context, and location context (Figure 6).

Personal context includes demographic and personal information describing the user's name, gender, date of birth, role and content preferences. This information is used in global mediation, which is deployed in the integration layer of the mediator. The purpose is to check user's access role before forwarding the request to a connector on top of the destination data source in order to stream the data to the presence layer. If

there is an error with user's privileges, it is returned to the presence layer without connecting to the data connectors (data sources).

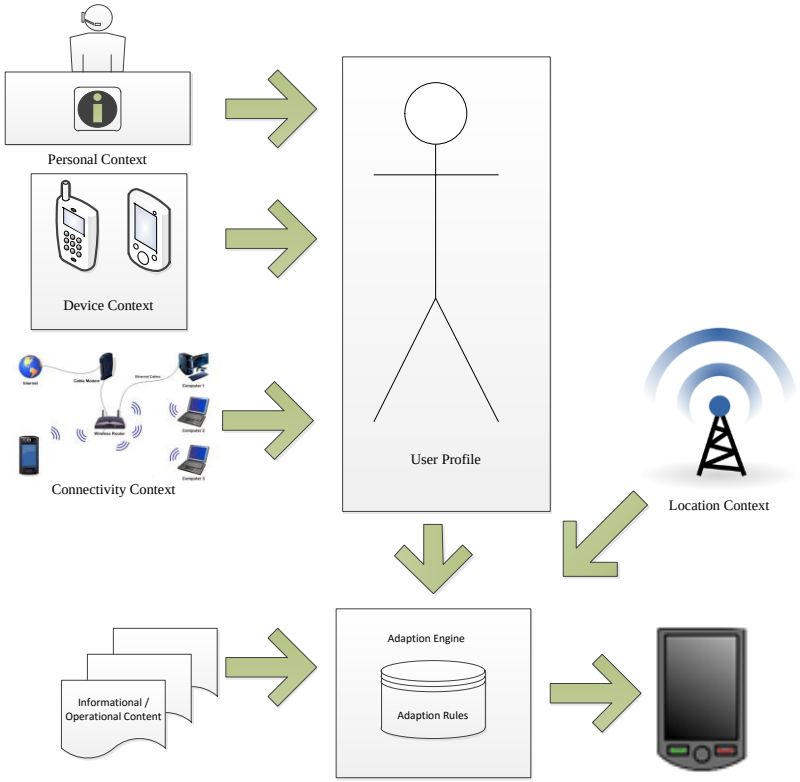

Fig. 6. Adaptive m-government content framework

User's device capabilities are described in device context attributes. Since devices are varying in capabilities, it is very important that the presence layer identifies these capabilities in order to deliver and to use the data in the M-Government application in a meaningful and appropriate way. For example, identifying the screen size and the resolution of the device, can affect the presentation of the data.

Two important issues in mobile devices are the Internet connection and the location services. The mobile devices can be connected to the Internet via 3G+ or wireless connections. The presence layer will take into consideration the quality of the Internet connection. This is called the connectivity context. Mobile applications can determine a device location using global position services (GPS) or 3G+ connectivity. These services allow the application to receive or send notifications related to the location. For example, the user may use the application to find the nearest police station or hospital. This feature is called location context services.

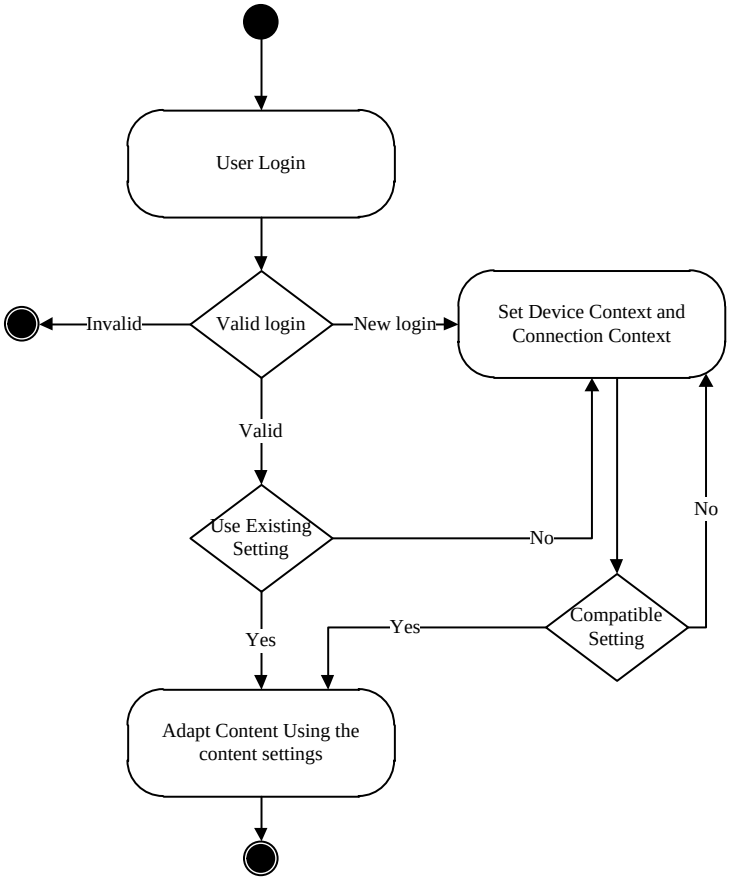

Fig. 7. User and system dialog

Our framework supports many features. One feature is that the framework adapts the content, which is based on the setting in the different aforementioned contexts: mobile device context, personal context, and connectivity context. The values in those categories are maintained by the integration layer, which manages users' profiles as well as the mapping schema among the distributed data sources. The location context is maintained by the presence layer since it is changed frequently. Another important feature is that the integration layer maintains the security policies. Those policies define who can access and what. Since there are different categories of users, each category of them will be able to access different services. Some scenarios of the services that are provided by the M-Government application are listed below:

Informative messages can be sent based on the personal (demographic) values. For example, if the ministry of health organizes a free screening mammogram event, a message is sent to users based on the age and the gender. Informative traffic messages can be sent based on the location context. A notification can be sent using a push messaging

system in order to reduce the cost and increase the efficiency. [26] Based on the previous model, the expected dialog between the user and the system is shown in Figure 7.

5 Conclusion

In this paper, an adaptive framework based on a three-tier mediation architecture and a private cloud is proposed to enhance the services of M-Government. The framework manages four contexts which are the personal (demographic) context, the device context, the connectivity context, and the location context. The first three contexts affect the adaptation and presentation of the data, while the location context does not affect the presentation. The location context is currently used for filtering informative messages and it does not affect the presentation of data. In addition, the proposed framework is based on a mediation architecture that can handle heterogeneous data sources, apply different levels of security, and adapt different presentations to the same data based on the capabilities of the connected user's device. Finally, the proposed framework embedded security and authentication using RBAC, Hummingbird-2, and DUKPT.

6 References

[1] T. Isagah and M. A. Wimmer, "Mobile Government Applications: Challenges and Needs for a Comprehensive Design Approach," presented at the Proceedings of the 10th International Conference on Theory and Practice of Electronic Governance, New Delhi AA, India, 2017. https://doi.org/10.1145/3047273.3047305

[2] T. Isagah and M. A. Wimmer, "Addressing Requirements of M-Government Services: Empirical Study from Designers' Perspectives," presented at the Proceedings of the 11th International Conference on Theory and Practice of Electronic Governance, Galway, Ireland, 2018. https://doi.org/10.1145/3209415.3209469

[3] S. Jauhari and D. Maheshwari, "M Governance: Challenges and Prospects," International Journal of Innovative Research and Development, vol. 3, no. 12, Nov. 2014.

[4] B. Dutra and D. Soares, "Decision-making factors for the provision of mobile government solutions," presented at the Proceedings of the 11th International Conference on Theory and Practice of Electronic Governance, Galway, Ireland, 2018. https://doi.org/10.1145/3209415.3209500

[5] M. Kumar and O. P. Sinha, "M-government–mobile technology for e-government," in International conference on e-government, India, 2007: Citeseer, pp. 294-301.

[6] H. Sheng and S. Trimi, "M-government: technologies, applications and challenges," Electronic Government, an International Journal, vol. 5, no. 1, pp. 1-18, 2008, https://doi.org/10.1504/eg.2008.016124

[7] S. Al-khamayseh, O. Hujran, A. Aloudat, and E. Lawrence, "Intelligent m-government: application of personalisation and location awareness techniques," in Proc. of Second European Conference on Mobile Government, Brighton, UK, 2006.

[8] K. Roggenkamp, "Development modules to unleash the potential of Mobile Government," in European Conference on E-government, 2004.

[9] C. Baru et al., "XML-based information mediation for digital libraries," in Proceedings of the fourth ACM conference on Digital libraries, Berkeley, California, USA, 1999, 313321: ACM, pp. 214-215, https://doi.org/10.1145/313238.313321.
[10] C. Baru et al., "XML-based information mediation with MIX," in Proceedings of the 1999 ACM SIGMOD international conference on Management of data, Philadelphia, Pennsylvania, USA, 1999, 304590: ACM, pp. 597-599, https://doi.org/10.1145/304182.304590.
[11] S. Chawathe et al., "The TSIMMIS Project: Integration of Heterogenous Information Sources," presented at the Information Processing Society of Japan (IPSJ 1994), Tokyo, Japan, 1994. [Online]. Available: http://ilpubs.stanford.edu:8090/66/.
[12] M. J. Carey et al., "Towards heterogeneous multimedia information systems: The Garlic approach," in Proceedings RIDE-DOM'95. Fifth International Workshop on Research Issues in Data Engineering-Distributed Object Management, 1995: IEEE, pp. 124-131. https://doi.org/10.1109/ride.1995.378752
[13] Q. Kharma, R. K. Ege, O. Ezenwoye, and L. Yang, "Data integration in a three-layer mediation framework," in Proceedings. IEEE SoutheastCon, 2005. 2005: IEEE, pp. 477-482. https://doi.org/10.1109/secon.2005.1423290
[14] H. O. Al-Sakran, Q. Kharma, and I. Serguievskaia, "Agent Based Framework Architecture for Supporting Content Adaptation for Mobile Government," International Journal of Interactive Mobile Technologies (iJIM), vol. 7, no. 1, pp. 10-15, 2013. https://doi.org/10.3991/ijim.v7i1.2131
[15] R. K. Ege, "CloudMediate Showcase Implementation with Google Firebase," presented at the CLOUD COMPUTING 2018: The Ninth International Conference on Cloud Computing, GRIDs, and Virtualization, Barcelona, Spain, February 22, 2018.
[16] H. O. Al-Sakran, "Accessing secured data in cloud computing environment," International Journal of Network Security & Its Applications, vol. 7, no. 1, p. 19, 2015. https://doi.org/10.5121/ijnsa.20157102
[17] C. A. Ardagna, R. Asal, E. Damiani, and Q. H. Vu, "From security to assurance in the cloud: A survey," ACM Computing Surveys (CSUR), vol. 48, no. 1, p. 2, 2015. https://doi.org/10.1145/2767005
[18] C. Bellettini, E. Bertino, and E. Ferrari, "Role based access control models," Information security technical report, vol. 2, no. 6, pp. 21-29, 2001. https://doi.org/10.1016/s1363-4127(01)00204-7
[19] L. Yang, R. K. Ege, O. Ezenwoye, and Q. Kharma, "A role-based access control model for information mediation," in Proceedings of the 2004 IEEE International Conference on Information Reuse and Integration, 2004. IRI 2004. 2004: IEEE, pp. 277-282. https://doi.org/10.1109/iri.2004.1431474
[20] T. Pardo, "Realizing the promise of digital government: It's more than building a web site," Albany, NY: Center for Technology in Government, 2000.
[21] I. Kushchu, S. Arat, and C. Borucki, "The impact of m-government on organisations: a mobility response model," in Electronic Government: Concepts, Methodologies, Tools, and Applications: IGI Global, 2008, pp. 2395-2408. https://doi.org/10.4018/978-1-59904-947-2.ch178
[22] G. Intelligence, "Global mobile trends 2017," GSMA, September, 2017.
[23] A. Trifonova and M. Ronchetti, "Hoarding content for mobile learning," International Journal of Mobile Communications, vol. 4, no. 4, pp. 459-476, 2006. https://doi.org/10.1504/ijmc.2006.008952
[24] D. F. Norris and M. J. Moon, "Advancing e-government at the grassroots: tortoise or hare?" Public administration review, vol. 65, no. 1, pp. 64-75, 2005. https://doi.org/10.1111/j.1540-6210.2005.00431.x

[25] M. Al-Dalahmeh, O. Al-Shamaileh, A. Aloudat, and B. Obeidat, "The Viability of Mobile Services (SMS and Cell Broadcast) in Emergency Management Solutions: An Exploratory Study," International Journal of Interactive Mobile Technologies (iJIM), vol. 12, no. 1, 2018. https://doi.org/10.3991/ijim.v12i1.7677
[26] R. A. sattar El Stohy, N. e. K. el Ghetany, and H. A. M. el Gharib, "A Proposed System for Push Messaging on Android," International Journal of Interactive Mobile Technologies (iJIM), vol. 10, no. 3, pp. 29-34, 2016. https://doi.org/10.3991/ijim.v10i3.5567
[27] Q. Kharma, "Enhanced skip-list search algorithm in 3-layer mediator framework," Ph D, Florida International University, 2005.
[28] H. Garcia-Molina, J. Hammer, K. Ireland, Y. Papakonstantinou, J. Ullman, and J. Widom, "Integrating and accessing heterogeneous information sources in TSIMMIS," in Proceedings of the AAAI Symposium on Information Gathering, 1995, vol. 3: Stanford, pp. 61-64. https://doi.org/10.1145/568271.223896
[29] H. Garcia-Molina et al., "The TSIMMIS approach to mediation: Data models and languages," Journal of intelligent information systems, vol. 8, no. 2, pp. 117-132, 1997.
[30] M. T. Roth et al., "The Garlic project," SIGMOD Rec., vol. 25, no. 2, p. 557, 1996, doi: 10.1145/235968.280363.
[31] W. F. Cody et al., "Querying multimedia data from multiple repositories by content: The Garlic project," in Working Conference on Visual Database Systems, 1995: Springer, pp. 17-35.
[32] W. Fan and H. Perros, "A novel trust management framework for multi-cloud environments based on trust service providers," Knowledge-Based Systems, vol. 70, pp. 392-406, 2014. https://doi.org/10.1016/j.knosys.2014.07.018
[33] O. Ezenwoye, R. K. Ege, L. Yang, and Q. Kharma, "A mediation framework for multimedia delivery," presented at the Proceedings of the 3rd international conference on Mobile and ubiquitous multimedia, College Park, Maryland, USA, 2004. https://doi.org/10.1145/1052380.1052415
[34] D. Engels, M.-J. O. Saarinen, P. Schweitzer, and E. M. Smith, "The Hummingbird-2 lightweight authenticated encryption algorithm," in International Workshop on Radio Frequency Identification: Security and Privacy Issues, 2011: Springer, pp. 19-31. https://doi.org/10.1007/978-3-642-25286-0_2
[35] Q. Chai and G. Gong, "A Cryptanalysis of HummingBird-2: The Differential Sequence Analysis," IACR Cryptology ePrint Archive, vol. 2012, p. 233, 2012.
[36] J. Stapleton, Security Without Obscurity: A Guide to Cryptographic Architectures. Auerbach Publications, 2018. https://doi.org/10.1201/9780429467523-6
[37] W. E. Smith, L. F. Fisher Jr, and B. Vargese, "System and method for securing a base derivation key for use in injection of derived unique key per transaction devices," ed: Google Patents, 2009.
[38] M. Hassan, T. Jaber, and Z. Hamdan, "Adaptive mobile-government framework," in Proceedings of the International Conference on Administrative Development: Towards Excellence in Public Sector Performance,2009.

7 Authors

Qasem Kharma is an assistant professor in Computer Science Department at Al-Ahliyya Amman University. His research interests are information systems, software engineering, databases, and using technology in education. He worked as a director of

the E-Learning Center. Currently, he is currently Chairman of the Computer Science Department. q.Shambour@ammanu.edu.jo

Nidal M Turab is a professor in Networks and Information Security Department at Al-Ahliyya Amman University. He is the vice dean of Faculty of Information Technology. He can be contacted at n.turab@ammanu.edu.jo.

Qusai Shambour is an associate professor in Software Engineering Department. He is the dean of Faculty of Information Technology. He can be contacted at q.Shambour@ammanu.edu.jo.

Mohammad Hassan is an associate professor in Computer Engineering Department at Al-AhliyyaAmman University. He is the vice dean of Faculty of Engineering. He can be contacted at mhassan@ammanu.edu.jo.

Article submitted 2019-06-20. Resubmitted 2019-11-20. Final acceptance 2019-11-27. Final version published as submitted by the authors.