Global Journals LaTeX JournalKaleidoscope™
Artificial Intelligence formulated this projection for compatibility purposes from the original article published at Global Journals. However, this technology is currently in beta. *Therefore, kindly ignore odd layouts, missed formulae, text, tables, or figures.*

Developments of E-Government on Smart Government and the Risks and Warnings about the Applications and Programs

Dr. Yasser Elmalik Ahmed Seleman[1]

[1] BISHA UNIVERSITY

Received: 14 December 2015 Accepted: 3 January 2016 Published: 15 January 2016

Abstract

Smart government is a model of evolution of egovernment, e-government in general is government public services on the Internet through Web portals applications (Life Events Business Episodes), smart government and its applications come to complement what has been built and invest in cross closer to citizen on the one hand, the direct and simultaneous interaction with data deployed in society and economic, social and security and its components on the other. Instruments Smart sensors have evolved (Smart Sensors) which are connected to the Internet, such as security surveillance cameras in cities and climate sensors and measuring energy and power associated with the Internet network government consumption.Smart government is the electronic services digital means for us dispense with many things, including the excessive use of paper and time lost in follow-up transactions between departments is an excellent step in the evolution of government services in the state system and the speed of completion of transactions and customer convenience in first class, which he could accomplish his business through his Smartphone without the need to go to the place of the government department and wait.

Index terms—

1 Introduction

he shift from E-government to smart government needs a lot of continuous work to ensure the readiness of services that will be available to users and requires the administrator to understand the digital needs and how they are applied and completed. Therefore, the study of those needs and understand well the government departments Developing or owning a Smartphone application to enter the stage of smart government, if the department does not offer its services properly through electronic pages it is difficult to switch to smart services without going through several stages of development.

Government departments and institutions should first focus on electronic services available on the network, or even non-ready at the moment and develop properly and the use of new technologies and standards, taking into account ease of use and user experience.

The provision of services through several channels including websites, smart phones and text messages and even television.

New developments to lead to a lot of amendments to the e-government model, which is suitable to the harmonic framework updates Data input to the electronic government (Government Interoperability Framework) to match sources and format the new data with back-end systems to the government.

2 II. WIRELESS NETWORKING PROBLEMS

In the development researcher discusses a range of topics including -Application Programming Interfaces (APIs) Using application programming interfaces (APIs) to make smart government services or functions are available

for use by other applications. Thanks to Smartphone, new services replace traditional -Applications and web applications.

Development of new applications quickly by blending existing services and capabilities in creative ways, is no techniques, to target different types of users, and can also be built from several interested parties before doing so. In order to enable multiple interfaces, it became the application programming interface (API) base interface for applications, whether old or new. As it has become the new application programming interfaces distribution channel for government services.

-Security measures relating to the user When you provide smart services to the public, should not be overlooked any of the security risks, whether related to the institution or the user, when the development of smart services, taking into account the privacy and security issues related to the participation of sensitive information while using those services. With regard to the user, the service provider must (the government agency, for example) to ensure safe use of the service by the public.

3 III. PROTECTION FOR WIRELESS NETWORK a) Security

Guidance for encrypting smart applications:

When you develop smart applications, you must take many issues into consideration, including: the use of properties, and the presence of sensitive data, and share information. It should take the necessary security measures in this regard, starting from the development stage, depending on the level of security necessary for each individual case. Review the instructions below and a number of thorny issues related to security in the development of smart applications. Protect sensitive data:

? Make sure the rating data stored according to the degree of sensitivity, and then to take security measures accordingly. Perform data processing and storage operations in accordance with those classifications. ? Store sensitive data on the server (server) rather than stored on the client machine, whenever possible, If it is necessary to store data on the client machine, use the application programming interface (API) to encrypt files, which are provided by the operating system, or through other reliable source. ? should always make sure sensitive stored data encryption, as well as the data in the cache (cached). ? In some cases, you can put restrictions on the data as a precautionary measure (to use in a different geographic location, for example).

longer applicable and single user interface, but several interfaces. These interfaces can be built using different

? For safety reasons, reveal the minimum of user data; namely select the data that will be of benefit to the user, and shapes the rest of the data.

The ability to provide basic functional properties of the work of the APIs, the government entity itself turn into a platform. And here is not enough to provide a set of APIs, it must be those interfaces reliable, scalable and secure at the same time.

4 b) Researcher discusses the data protection during transport

Always assumed that the network layer is safe, and on this basis, has taken the necessary precautions.

? When a specific application to send sensitive data wired or wirelessly, makes use of a secure channel for data transfer between two parties (SSL / TLS) is a prerequisite. ? Use strong encryption algorithms and long keys.

? Ensure that the user interface shows whether the certificates that are used are valid or not. c)

? Navigate through the application of the analysis of the basic functions and the method of work. Select network interfaces that the application uses, and select protocols and security standards it uses. ? Select the properties of the machine that could application and opportunities for piracy and potential uses (such as camera, GPS, etc.) Check out how he believes in the application of payment information, if it provides this property.

? Identify other applications that interact with smart service, and select applications that may harm the safety and privacy standards. ? Ensure that the source code analysis (source code)

for the application, and to identify weaknesses. ? Check out how they carried out the ratification of the user in the application process, and identified potential risks. ? Analyze the data stored within the application process. See the algorithms used in the encryption, and whether vulnerable to known issues.

? Verify that the data that is stored in the cache memory type, and whether sensitive information was stored in the memory. ? tested the application against the ”breakthrough talks” attacks in which the attacker between the interlocutors in the network sneaking unbeknownst to either of them (man-in-the-middle) to analyze the possible interventions in the application.

? Check if the sensitive data being leaked to the log files (log files). ? Be sure to maintain the security of the destination server, not the client-side only.

5 d) Risks from the perspective of the research

Researcher discusses a range of risks and warnings about the applications and programs Use smart devices multiple types of applications, the original or private systems and programs. From time to time, these applications and programs make updates or download programs requested in order to add new functionality to it, as is the case

in smart phones and tablets. However, these programs and applications may contain vulnerabilities or malicious code. There are many risks associated with the programs and applications can be listed as follows:

Applications threats and cipher software and operating systems Installed programs contain smart devices based on certain codes unauthorized procedures.

This code can penetrate the devices by which programs are updated or installed, or applications that are downloaded, or instant messaging, or e-mail. This code has been inconsistent with the normal operation of the device, or causes the risks of theft or loss of data. Operating systems as well as the risk of a Fig. **??** : E-government services Usage Analysis and Risk similar, but they may cause greater problems because their influence and ability on the device and the data is much larger than the impact of applications.

6 e)

When the devices connected to the Internet, you may reach them malicious code through HTML applications or JavaScript or Flash, or other sources through Web pages that are visited. It may also cause weakness browsers in exposing the devices to the risk of external codes. Take preventive measures such as avoiding users' access to unreliable sites through the use of checks or security certificates at the enterprise level and the use of modern versions of web browsers provides a greater degree of safety. You must modify the settings to suit the security policies in the enterprise. You must make sure not to enter into official websites, but through the means of secure communication. The devices Security Administration is critical of the security structure of the whole enterprise, the risks related devices threaten as well as desktop computers, databases and e-mail devices and servers, networks, and may cause the arrival of unauthorized persons to sensitive data, or it may cause slow systems. Moreover, because of the mobile nature, the smart devices are prone to loss or theft of data

7 IV RECOMMENDATIONS

? Data encryption in all communication process to reduce risk wherever possible application of it. However, the encryption method must be compatible with the Federal Information Processing Standard System (FIPS) which does not possess a lot of hardware at the moment. For devices not compliant with FIPS system, institutions must use FIPS 140-2 sandbox security mechanism.

? Provide and encourage the use of formal communication network via virtual private networks (VPN) in high-risk situations, where the authentication and encryption, confidentiality and integrity of secure data across these networks operations.

? must be trained users to be very careful for their effective control on the devices, and that is to give them instructions about the potential for the loss of hardware hazards. ? Ensure that the smart devices do not allow the transaction if we're not connected to the Internet (offline) or to store transaction data for later use. Applications should require it relates to the Internet to complete the transaction. ? For secure smart devices and applications, make sure you download versions concerning the types of new threats and risks updates. ? Do not have to deal with payment applications other than authorized or can exchange data with applications.

2016 

Figure 1: T © 2016 E

Figure 2:

[Hijazi] , Abdel-Fattah Bayoumi Hijazi . (government and legal system, the university thought Dar)

[Jump Up$^{G}rima - Izquierdo()$] *A generic architecture for e-Government and E-Democracy: requirements, design and security risk analysis*, C Jump Up^Grima-Izquierdo . 2010. LAP Publishing.

[China: The Next, Science Superpower ()] *China: The Next, Science Superpower*, 2006.

[Essam Abdel Fattah rain, e-government between theory and practice, the new University House, Alozartih ()] *Essam Abdel Fattah rain, e-government between theory and practice, the new University House, Alozartih*, 2008.

[Jump Up$^{(}$)] 'Public Affairs Division, Public Affairs and Communications Directorate'. Oecd Jump Up^. *Policy Brief* 2003. OECD. (The e-government imperative: main findings)

[References Références Referencias Internet threats] *References Références Referencias Internet threats*,

[United Nations Department of Economic and Social Affairs (2014)] *United Nations Department of Economic and Social Affairs*, 2014. 2014-09-16. UN. Retrieved. (United Nations E-Government Survey)