International Journal of Cloud Computing and Services Science (IJ-CLOSER)
Vol.2, No.3, June 2013, pp. 159~169
ISSN: 2089-3337

Security Model for Microsoft Based Mobile Sales Management Application in Private Cloud Computing

Kuan Chee Houng, Bharanidharan Shanmgam, Ganthan Narayana Samy, Sameer Hasan Albakri, Azuan Ahmad
Advanced Informatics School (AIS), Universiti Teknologi Malaysia (UTM), Malaysia

Article Info

Article history:

Received Mar 20th, 2013
Revised Apr 20th, 2013
Accepted May 20th, 2013

Keyword:

Information Security
Mobile Applications
Cloud Computing

ABSTRACT

The Microsoft-based mobile sales management application is a sales force management application that currently running on Windows Mobile 6.5. It handles sales-related activity and cuts down the administrative task of sales representative. Then, Windows launch a new mobile operating system, Windows Phone and stop providing support to Windows Mobile. This has become an obstacle for Windows Mobile development. From time to time, Windows Mobile will be eliminated from the market due to no support provided by Microsoft. Besides that, Windows Mobile application cannot run on Windows Phone mobile operating system due to lack of compatibility. Therefore, applications those run on Windows Mobile need to find a solution addressing this problem. The rise of cloud computing technology in delivering software as a service becomes a solution. The Microsoft-based mobile sales management application delivers a service to run in a web browser, rather than limited by certain type of mobile that run the Windows Mobile operating system. However, there are some security issues need to concern in order to deliver the Microsoft-based mobile application as a service in private cloud computing. Therefore, security model is needed to answer the security issues in private cloud computing. This research is to propose a security model for the Microsoft-based mobile sales management application in private cloud computing. Lastly, a User Acceptance Test (UAT) is carried out to test the compatibility between proposed security model of Microsoft-based mobile sales management application in a private cloud and tablet computers.

Copyright © 2013 Institute of Advanced Engineering and Science.
All rights reserved.

Corresponding Author:

Second Author,
Advanced Informatics School (AIS),
Universiti Teknologi Malaysia (UTM), Malaysia.
Jalan Semarak, Kuala Lumpur, 54100, Malaysia.
Email: bharani@ic.utm.my

1. INTRODUCTION

Windows Mobile is a mobile operating system developed by Microsoft, which is designed to have similar features and screen appearance with Windows version personal computer. Its kernel is based on the Windows CE 5.2 [1]. Besides that, Microsoft allows third parties to develop software for Windows Mobile user without any rules and regulations. Initially, the Microsoft-based sales application is running on Windows Mobile 6.5 version, which is a mobile sales force management software. It is used to raise sales related activity and cutting down the administrative task, such as planning and reporting. However, Windows Mobile was taking place by Windows Phone in year 2010, where it does not compatible to run Windows Mobile software [2]. This is an obstruction to the development of software running on Windows Mobile.

Windows Mobile is not upgradable to Windows Phone mobile operating system because Windows Phone is completely a new mobile operating system and incompatible with Windows Mobile [3]. In addition, Windows Mobile software cannot support and run on Windows Phone version due to different kernel

architecture. The kernel of Windows Mobile is based on Windows CE 5.2 whereas Windows Phone is based on Windows CE 6.0/7.0 [4]. The differences of kernel version between Windows Mobile 6.5 and Windows Phone 7 has made the Microsoft-based mobile sales management application is only able to run on Windows Mobile 6.5 but not in Windows Phone 7. Besides that, it also made the application in Windows Mobile 6.5 only supports one touch point. However, multipoint touch features is supported by Windows Phone 7. Since smartphone is starting to generalization, from mobile to tablet, therefore the Microsoft-based mobile sales management application can be access by multi types of mobile devices instead of mobile that run on Windows Mobile 6.5 only.

The appearance of cloud computing technology has become a ray of hope for continuing to develop Microsoft-based mobile sales management application into software-as-a-service (SaaS) in cloud computing. In the SaaS model, the application software is delivered based on the demand of the client [5,6]. In other word, the data is stored on the cloud provider where the security issues of data are emphasized on the cloud provider. A very successful example of SaaS is salesforce.com. In this work, Microsoft-based mobile sales management application is delivered in private cloud computing because the application needs to connect from Internet to enter the organization's intranet. Besides that, it's able to establish the trust between the user and the organization and monitoring purpose in private cloud computing.

This paper investigates the security model for Microsoft-based mobile sales management application in private cloud computing, design a security model and test the effectiveness of proposed security model of Microsoft-based mobile sales management application in private cloud computing. This paper organized as follows; the next section is introducing literature review. Section 3 discusses the methodology. The section 4 summarizes the implementation. Some of the findings and analysis are listed in the section 5. Section 6 discussing the future research and finally a conclusion is given in section 7.

2. LITERATURE REVIEW

Numerous research works are conducted in order to secure the application in cloud computing. These research works investigate the security models such as the Secure Socket Layer (SSL), one and two factor authentication, out of band authentication, access control mechanism, Mobile Trusted Module (MTM), and Security Assertion Markup Language (SAML) based Single Sign On.

2.1. Secure Socket Layer (SSL)

Secure socket layer (SSL) is a common protocol used for secure the communication to website over the internet, developed by Netscape. Since web application or services is accessed through a web browser, nowadays most of the web server product and web browser have included SSL as one of the internet security features [7]. It is used to secure the layer located between the Internet's Hypertext Transfer Protocol (HTTP) and Transport Control Protocol (TCP) layers to become HTTPS [8]. Any information undergoes this layer will be encrypted during transmission. The phrase "socket" refers to the method of transfer the data between a client and a server to a connected network or within the computer itself. Besides that, SSL is run above Transport Control Protocol/Internet Protocol (TCP/IP), where it provides client-server authentication and allow exchanging a series of encrypted messages [7].

SSL provides some advantages to the client and the server. It ensures the authentication process run in the correct way where a certificate is used to identify and authenticate client or web browser before connection is made. Besides that, it also provides privacy and integrity to the message by using secure connection. In addition, encryption is made all along the communication between the server and client with a unique "session key". However, SSL also has some limitations. SSL strip or sniff attack can cut off the secure connection between client and server and can be disclosed to the attacker [9] Besides that, SSL encryption focus on the transport level rather than in the application itself. Messages are encrypted only during transmission over the network. Therefore, other security mechanisms are required to handle the security of the messages on the Web application.

2.2. One Factor Authentication

One-factor authentication is the traditional representative user authentication method that requires a user name and password before access to the data resources. It is also known as knowledge-based authentication (KBA). In general, this type of authentication usually refers to something only other known, including password, passphrase, shared secret, account details, personal identification number (PIN), and etc [10]. Besides that, it requires the user to take additional precaution to create a strong password at a certain level and regular renewal to avoid other people access to your account. However, this type of authentication can prone to phishing or key logging attack where attacker sets up a trap to collect the password of the user account [9].

2.3. Two Factor Authentication

Two factor authentication is not a new concept. Today, most of the banking industries apply this type of authentication for online transaction. In a two-factor authentication system, the user need to provide two times of identification, something known to the user only, such as passphrase or account details, and the author refer to something user have only, such as mobile devices, security token, smart cards, chip readers and etc. [10]. After the user entering password, a verification code is sent to your mobile phone via SMS or voice calls. However, two-factor authentication also contains weaknesses such as Trojan controlled web sites and man-in-the-middle attacks.

2.4. Out of Band Authentication (OOB)

The appearance out of band authentication carries out the discussion all around the world, a new second factor authentication. The currently available methods include speech recognition and fingerprint via mobile phone. In general, the OOB authentication service provider will contact the mobile number of cloud's user when he/she access to the application in cloud computing. User response to the request according the instruction given and send back to the OOB authentication service provider via mobile phone [10]. Then the particular service provider will send the reply to the application in the cloud. This solution able to provide stronger authentication comparing to the one-time-password, work as an alternative way of second factor to identify credentials of the cloud user. However, this is not the best solution when a cloud user accesses the cloud application few times a day, where it does not achieve trade-off between user convenience and security.

2.5. Access Control Mechanism

In cloud computing, cloud user can access the information needed from anywhere of the world through Internet. Therefore, a mechanism is needed in order to identify and control the access to the web services. An access control mechanism is able to administrate and control the cloud user from access the important data by placing some restriction on the established identities. Any organizations that use services on the cloud will have its own access control management system to protect the important data and computing resources for authenticated users. There are three types of access control, discretionary access control (DAC), media access control (MAC), and role-based access control (RBAC) [11].

In DAC, the ability to share resources in a peer-to-peer configuration allows user to control and possibly provide access to information or resources at their disposal. Besides that, the system administrator can allow general, unrestricted access, or they can allow specific individuals or sets of individuals to access these resources. Whereas in MAC, it is an access policy determined by the system, not the owner. MAC is structured and coordinated with a data classification scheme that rates each collection of information where users and data owners have limited control over their access to information resources [11]. Each user or subject is rated to specify the level of information that one user can access. This rating is referred as sensitivity level. RBAC are determined by a central authority in the organization. It gives an access authority to a user or user group based on roles and position hold in an organization. Besides that, RBAC is making the access control easier for control maintenance and restriction, especially if the individual performing the role changes often. Role-based access control (RBAC) remains the most frequent use method of identity management mechanism [12]. This is due to the simplicity, flexibility in capturing different requirements of cloud user, and efficient privilege management of cloud user.

2.6. Mobile Trusted Module (MTM)

The Mobile Trusted Module (MTM) is a hardware-based security module for mobile phone and devices which is introduced by the Trusted Computing Group (TCG) [13]. Besides that, the main purpose of MTM is to implement the trust in mobile computing platform and embedded devices. This is because MTM able to isolate all information in a protecting environment due to its architectural framework. The device services of MTM provide authentication and authorization to all access requests. In addition, MTM also provides security function include secure then execution environment, shielded storage location, protection for storage, and also public key cryptography [14]. However, it is being considered as a Cloud Computing authentication method with Subscriber Identity Module (SIM) due to the generalization of Smartphone.

In general, every trusted engine in Mobile Trusted Module is located in a particular building block accordingly and provides its own service. This particular engine and services can categorized as a device, cellular, application, and user [15]. The device block provides its service to cellular block. Then cellular block provides its service to application block, and application block provides its service to user block. Each service is connected with trusted services, trusted resources, and mobile remote-owner trusted module (MRTM) except user services, is connected to mobile local-owner trusted module (MLTM). This is because the device, cellular, and application engines do not have physical access to the phone. Besides that, these

three engines need to ensure their particular services execute tasks in a secure boot process, which is the additional capability in MRTM but no in MLTM. However, the only user engine has the physical access to the phone and executes the wanted software. This mean that after the trusted software execute in user engine, it will load to the three engines to execute in a secure boot process. Although MTM is considered as a cloud computing authentication method with the usage of SIM, but the duplication or cloning of the SIM card will consider as one of the threat for this method. Therefore, MTM needs to be enhancing the security either in the design of architecture or hardware itself including also the security of SIM.

2.7. Security Assertion Markup Language (SAML) based Single Sign On

Security Assertion Markup Language (SAML) is an Extensible Markup Language (XML) based open framework for the communication of identity, attribution, authentication, and authorization information between security domains [16]. It was driven by the Organization for the Advancement of Structured Information Standards (OASIS) that promotes the interoperable and development of open standards for security and web services (14). Besides that, the main purpose of SAML is to establish the circle-of-trust for users in multi web service environment. This can be done by asserting the XML document to asserting authority which includes the basic attributes, authentication, and authorization of particular end user [17]. Then, destination site will validate the assertion with the asserting authority when user access to web services. Whenever a user wants to access to other web services under the same domain, the user need not to login again because the user is authenticated based on XML documents.

In the XML document, the attribute assert is refers to a role or a group of membership for each user of the web services, whereas authentication assert is refer to the asserted user that was previously authenticated by an authority in a particular context, while authorization assert refer to whether the user can access to a specified resource based on the same statement in the XML document [18]. However, the connection between the Web browser and an identity provider appear as the weakest link where it can be the target of the man-in-the-middle attack [19].

3. METHODOLOGY

This section presents the methodology of proposed security model for the research study, as developed from the Literature Review in section II. Besides that, a flow chart of application will be included in this section in order to show the way of the proposed security model take place on the Microsoft-based web application.

3.1. Proposed Security Model

In this research, the Microsoft-based mobile sales management application is a prototype application in order to test the proposed security model. Figure 1 shows the proposed security model for Microsoft-based mobile sales management application in private cloud computing. The first proposed security model in this research is using the secure socket layer server certificate to secure and authenticate the login connection of cloud user. Besides that, it provides encryption to the transmission data between application and server. Secondly, one-factor authentication method will be used in the authentication process of this research, such as password. Furthermore, role-based access control is chosen as the third security model in order to control the cloud user to access the sensitive data in the cloud. In this access control, three roles will be created in order to assign roles and authorize cloud user access the needed information: administrators, top management, sales manager, sales representative, and marketing representative.

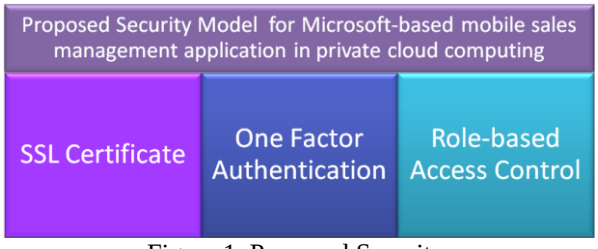

Figure 1. Proposed Security

3.2. System Overview

System overview can help the researcher understand the idea of the research as it able to show a directorial method on how the application works. This can let the researcher to imagine the process of an application. Figure 2 shows the flow of Microsoft-based application in a private cloud and how the security model takes place.

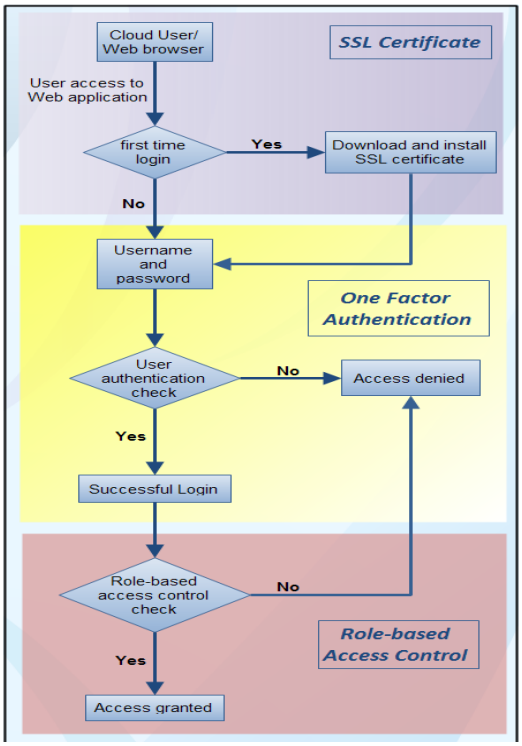

Figure 2. System overview flow chart

From the Figure 2, it is able to see the flow of the research on how the security model works in the application. When cloud user access to Web application for the first time, it will require the user to download and install an SSL certificate on the Web browser for identification and authentication. If the cloud user is not the first time login the Web application, it means that the SSL certificate is installed in the Web browser. Then, cloud user is required to provide a username and password to login the Web application. If the cloud user has successfully passed the second authentication with correct username and password, then the role-based access control will check to see whether the cloud user is assigned with any role. If the user assigned with one of the roles in the system, then the cloud user is authorized to access the Web application. In the case of user is authenticated but not assigned with any role in the system, then cloud user is not able to access any function of the Web application.

4. IMPLEMENTATION

This section discusses in detail the required components in order to implement the Secure Socket Layer certificates into a Web browser, One Factor Authentication and the implementation of User Acceptance Test (UAT). Besides that, it also includes the way of request and binding SSL certificate for a Web site.

4.1. Socket Layer Certificate

In this research, the Microsoft-based mobile sales management application is delivered in private cloud computing. Therefore, a server with Windows Server 2008 Standard operating system installed is used and connected within the intranet. Other required components are: Internet Information Services (IIS), Active Directory Certificate Authority (AD CS), Certification Authority (CA), and Certificate Authority Web Enrollment. The last two components are included in the AD CS, as shows in Figure 3.

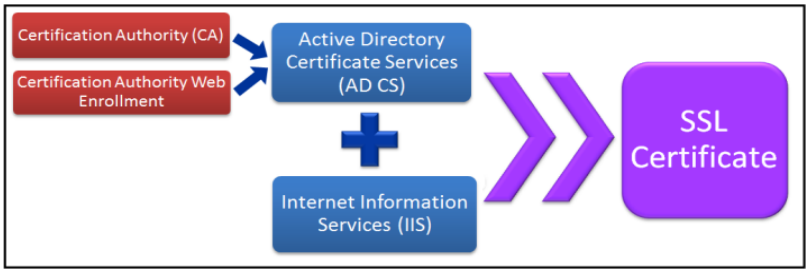

Figure 3. Components for generation of the SSL certificate

Internet Information Services (IIS) is a site administering and management application created by Microsoft with additional capability that can integrate with Windows server operating system. Besides that, it is also used for support Web Site and Web-based application hosting on Windows Server. In addition, this is required to enable before Active Directory Certificate Services installed on the Windows Server. Furthermore, IIS is used to request and manage SSL certificate for the Microsoft-based application on the Web in this research.

Active Directory Certificate Services (AD CS) in the Windows Server 2008 operating system play an important role in managing certificate activity and also acts as an authority in public key infrastructure (PKI) system. Besides that, the certificates can be used for authenticate user on a network in order to achieve the goal of information security, confidentiality, integrity, and authentication. In order to generate SSL certificate, Certificate Authority (CA) and Certificate Authority Web Enrollment components are required to install with AD CS. Certificate Authority (CA) component is used as a root CA to issue certificates to users, computer, and manage the validity of certificates. Whereas Certificate Authority Web Enrollment is used for the Web browser to connect to a CA in order to request and review certificate, retrieve certificate revocation lists (CRLs), and perform smart card certificate enrollment.

The process of requesting an SSL certificate from a Certificate Authority and binding it on an IIS in Windows Server 2008 server includes; *Create a Certificate Signing Request (CSR)*, *Request a certificate from Certificate Authority*, *Approve the certificate request* and *Download and bind the approved certificate to the Website*.

4.2. One Factor Authentication

Sequence diagram able to shows the flow of logic or the operate process of the system in a visual manner. Figure 4 illustrates the user authentication process and in this research. First of all, user open web browser and type in the Website address. Then it will redirect the user to the login page. User key in his/her correct username and password, and press "Log In" button. The written code behind the "Log In" button will validate the key in a username and password, and will redirect user to default page if the username and password are matched. However, if the username and password are incorrect, the authentication process is failed and login page will display an error message.

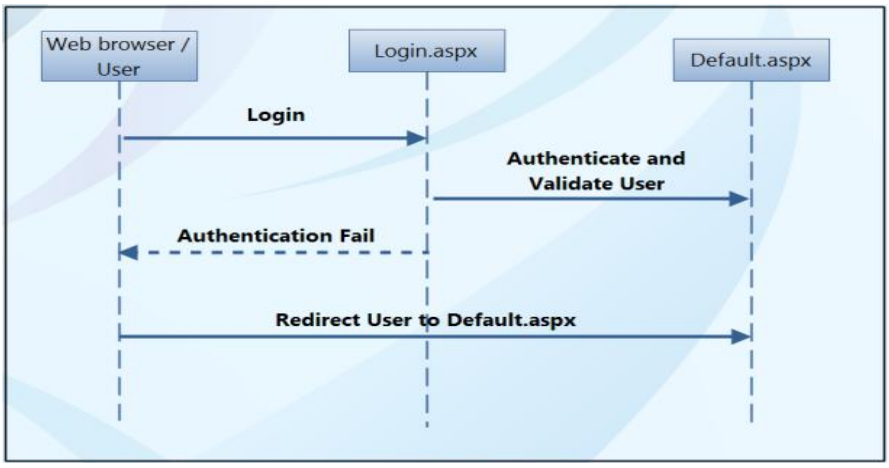

Figure 4.Sequence diagram of user authentication process

In this research, the application's authentication method is configured to use forms authentication in Web.config. Forms authentication identifies the user by prompting them to enter their credentials through a web form. Below is the coding of configuration in Web.config:

```
<authentication mode="Forms">
<forms slidingExpiration="true" timeout="60"/>
</authentication>
```

The attribute slidingExpiration is set to true, which indicate the authentication cookies' timeout is reset every time the user visits the Web site. Besides that, the timeout describes the specific time of authentication ticket cookies get expires. In other words, the user's authentication ticket cookies expire in 60 minutes and reset again after the user connects to the Websites. The following code of "Log In" button is the responsible part of user validation and authentication. User able to login and access the Website if the key in username and password are matched, otherwise access is denied.

```
Protected Sub myLogin_Authenticate(ByVal sender As Object, ByVal e As System.Web.UI.WebControls.AuthenticateEventArgs)
Handles myLogin.Authenticate

If Membership.ValidateUser(myLogin.UserName, myLogin.Password) Then
            e.Authenticated = True
    Else
      e.Authenticated = False
    End If
  End Sub
```

4.3. Role-Based Access Control

This section is dedicated to describe the implementation of third security model, role-based access control. It shows the way to classify the users based on roles and access certain functionalities on a role-by-role basis. To implement this access control, it involved three steps. Creating and managing roles is the first steps to be implemented, followed by assign role to user, and lastly, role-based authorization.

In the following coding below, there are three parts of coding is used to create and managing roles. The first part, DisplayRolesInGrid() is used to display all the roles created. It will retrieve the roles created from the database and display in grid view. The second part is the create role button, CreateRoleButton_Click, where it will create a new role if the role does not exist in the system. The last part is deleting button to delete created roles, RoleList_RowDeleting.

```
Private Sub DisplayRolesInGrid()
    RoleList.DataSource = Roles.GetAllRoles()
    RoleList.DataBind()
  End Sub
Protected Sub CreateRoleButton_Click(ByVal sender As Object, ByVal e As System.EventArgs) Handles CreateRoleButton.Click
    Dim newRoleName As String = RoleName.Text.Trim()

    If Not Roles.RoleExists(newRoleName) Then
      ' Create the role
      Roles.CreateRole(newRoleName)
      ' Refresh the RoleList Grid
      DisplayRolesInGrid()
    End If
    RoleName.Text = String.Empty
  End Sub
```

The second step is assigning role to use, where it consists of two methods. The first method is managing roles by user, with a list of user is provided to select and assign roles to user. The second method is manages user by roles, where a list of users is displayed based on the selected role.

Finally yet importantly, the next step is role-based authorization. It permits and authorize user to access certain Website based on role. For user that not in any role, he or she able to log in but not able to access any functions of the Website. Below is the coding of the role-based authorization.

```
If Request.IsAuthenticated Then
      If User.IsInRole("Administrators") Then
        Response.Clear()
        Response.Redirect("Admin\Default.aspx")
      ElseIf User.IsInRole("Sales Representative") Then
        Response.Clear()
        Response.Redirect("SalesRepresentative\Default.aspx")
      ElseIf User.IsInRole("Sales Manager") Then
        Response.Clear()
        Response.Redirect("SalesManager\Default.aspx")
      ElseIf User.IsInRole("Marketing Representative") Then
        Response.Clear()
        Response.Redirect("MarketingRepresentative\Default.aspx")
      ElseIf User.IsInRole("Top Management") Then
        Response.Clear()
        Response.Redirect("TopManagement\Default.aspx")
      End If
 WelcomeBackMessage.Text = "Welcome back, " & User.Identity.Name & "!"
      AuthenticatedMessagePanel.Visible = True
      AnonymousMessagePanel.Visible = False
    Else
      AuthenticatedMessagePanel.Visible = False
      AnonymousMessagePanel.Visible = True
    End If
```

In the coding above, the role-based access control check is activated if the user is authenticated and login successfully. It will redirect the user to the correct Website page based on the early assigned role. For an example, if a marketing representative is logged successfully and gets authenticated, Web browser will redirect the particular user to MakertingRepresentative\Default.aspx page. However, it will redirect user to welcome page without displaying any menu button if the user is not assigned any role.

4.4. User Acceptance Test

UAT is a form of testing to verify the system in terms of rules, various workflows, data correctness and others. This is to find out any vulnerability or error on the system and fix it before put it into production.

In this research, we have distributed the UAT form to end-user through email. This group of end-user includes sales representative, sales manager, and marketing representative. The distributed UAT is referring to the UAT example from http://www.SQAtester.com.

5. RESULTS AND DISCUSSION

From the result of testing activity, it shows that the three security models has successfully implemented in this research. In the first testing on the SSL certificate, it only fulfils the first and second procedure, which is a basic indicator (web address, padlock and HTTPS) and the name of the SSL certificate or the CA. In the second testing on one factor authentication, the user is testing the login module with a set of incorrect username and password. However, it displayed a warning message to the user if he/she is not successfully log in. At last, a user is successfully login the Web site with correct username and password. In the third testing on role-based access control, it involves three stages before the user is authorized to access the particular Website. First, create the role based on the user position hold in an organization, next assign the particular role to the user. Lastly, write the authorization coding based on the role to allow user access the particular Website.

This part provides a comparison analysis between the general security models discussed in literature review part and the proposed security models in this research. The purpose of this analysis is to generate a better idea and comment to the proposed security models. Besides that, we can know the weak spot of the security model in this work from the analysis.

The process of a Web browser connects to a secure website via SSL in Literature Review part is almost the same with the way of SSL certificate in this research. The only difference is the Web browser will not trust the SSL certificate in this research until it installs the root certificate that contains the respective domain name. This has happened because the created SSL certificate is issued by our own Active Directory Certificate Services (AD CS). This will benefit our side because we manage the public key cryptography system ourselves. After installing the root certificate, the Web browser will automatically verify and validate the SSL certificate for first time access to the Website. Besides that, SSL certificate in this research may face SSL strip or sniff attack, same as the discussed security model in the literature review. This is because the SSL certificate is not an enhanced version of this research.

The one factor authentication in this research is better than the one discussed in Literature Review part. This is because it will display a warning message when user key in incorrect username or password. Besides that, it does not allow anonymous to login into the Website. In addition, it also requires user to take additional precaution to create a strong password at certain level, same as the discussed one factor authentication in Literature Review part. However, this security model also prone to phishing or key logging attack, where the attacker can do a fake Website and capture the username and password from the user.

The role-based access control research provides better view compare to the model that discussed in Literature Review part. This is because it provides two methods to manage the user and roles. The first method is managed roles by user, where you can select the user from the list and assign the respective role. The second method manages user by roles, where you can view the list of users by select the roles from the list. However, no graphical user interface (GUI) is provided to manage and authorize user to access certain Websites. Administrator need to manually add the coding if there are any new roles created.

UAT Result Analysis

This section will present the analysis of the user acceptance test (UAT) result that is implemented in section IV. The result will present in statistics graph as Figure 5 below in order to provide visual analysis.

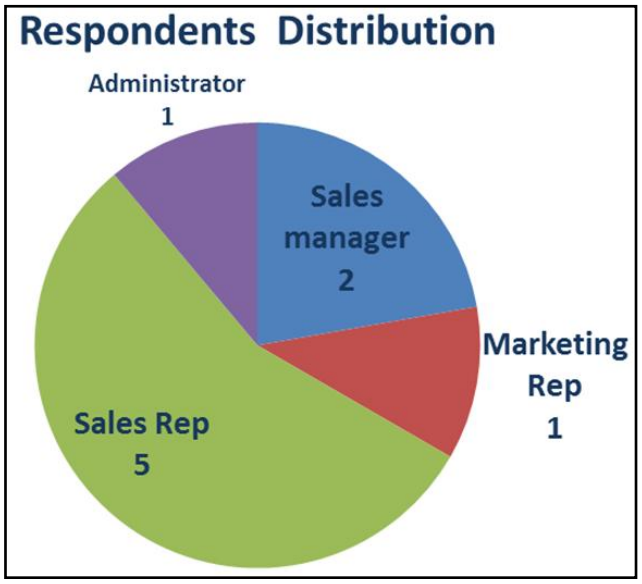

Figure 5.Distribution of respondents

Total UAT forms that sent out to target end user are 11 forms. However, only 9 forms are returned. Out of 9 respondents, 5 respondents are from sales representative, 2 respondents from sales manager, 1 marketing representative, and 1 administrator.

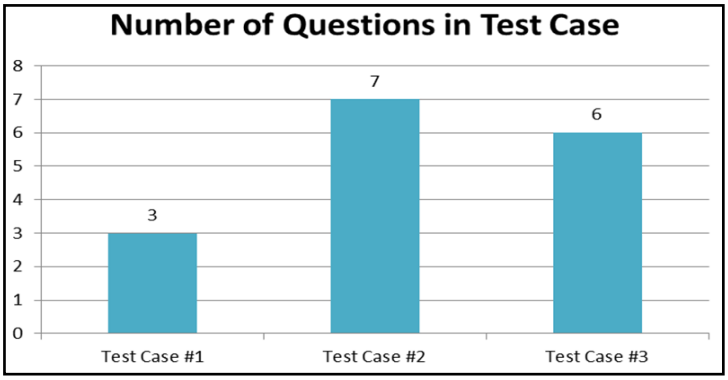

Figure 6. Number of questions in the test case

Figure 6 shows the number of questions in for each test case of the UAT. The UAT contains three test cases. The first test case is for testing the SSL certificate, second test case is to test the one factor authentication, and the third test case is for testing the role-based access control. Throughout the UAT form, there are 16 total questions; with distribution of questions according to test case is 3, 7, and 6. Fortunately, the success rate for the UAT is 100% based on the forms returned.

6. FUTURE RESEARCH

Implementing the proposed security model with Microsoft-based application and reviewing relevant literature open new horizons and bring many ideas to improve the research. The security of SSL certificate can be improved by enhancing it with SSLock, protect and defeat the SSL strip attack. The purpose of SSLock is to sustain the trust on entity brought by SSL. In addition, SSL-VPN can be another option for the network security since the application is delivered in private cloud computing. Besides that, one factor authentication can improve to two factors or out of band authentication in order to enhance the security and avoid phishing and key logging attack. In addition, with the emerging of Internet connection, it is easy to implement a biometric authentication mechanism as the tablet is getting common nowadays.

7. CONCLUSION

This research is entirely about the formulation of security models for Microsoft-based sales mobile management application in private cloud computing, which proposed the security models in order to secure cloud user to access the application. As shown in previous sections, the implementation of the security

models and testing activity was perfect in term of the results of SSL certificate, one factor authentication, and role-based access control. Implementing the three security model into the Microsoft-based application is a hard mission as the complexity of coding, testing activity, compatibility and others.

Due to SSL certificate is issued by our own Certificate Authority, therefore a root certificate is required to install with the respective domain name in order to trust and recognize the SSL certificate in the next action. After applying the SSL certificate, there are two conditions need to fulfil for the testing activity. Firstly, make sure the Web address, padlock icon, and HTTPS header is activated. Secondly, the name of the SSL certificate must match with the Web URL. However, the HTTPS connection may face SSL strip or sniff attack.A warning message is displayed when user key in incorrect username or password apply in one factor authentication mechanism. A password protected is enabled on the login page in order to disallow anonymous to login into the Website. However, one factor authentication mechanism may face phishing or key logging attack.

ACKNOWLEDGEMENTS

This research was supported by the Research Management Center (RMC), Universiti Teknologi Malaysia (UTM), Malaysia, under grant No. 07J92.

REFERENCES

[1] A. Hammershoj, A. Sapuppo, and R. Tadayoni, Mobile Platforms-An analysis of Mobile Operating System and Software development platforms, presented at the CMI International Conference on Social Networking and Communities, Copenhagen, Denmark, 2009.
[2] D. Flynn. (2010, 07-03-2013). *Microsoft: No Windows Phone 7 upgrade for Windows Mobile 6.x devices*. Available: http://apcmag.com/microsoft-no-windows-phone-7-upgrade-for-windows-mobile-6x-devices.htm
[3] S. Schroeder. (2010, 07-03-2013). *Upgrading to Windows Phone 7 May Not Be Possible*. Available: http://mashable.com/2010/03/01/windows-phone-7-upgrade/
[4] O. Bloch. (2010, 07-03-2012). *Windows CE is NOT dead!*
[5] Pal, Devki Gaurav. A Novel Open Security Framework for Cloud Computing. International Journal of Cloud Computing and Services Science (IJ-CLOSER)1.2 (2012): 45-52.
[6] Carlin, Sean, and Kevin Curran. Cloud Computing Technologies. International Journal of Cloud Computing and Services Science (IJ-CLOSER) 1.2 (2012): 59-65.
[7] D. Zissis and D. Lekkas, Addressing cloud computing security issues, *Future Generation Computer Systems*, vol. 28, pp. 583-592, 2012.
[8] M. Bhiogade, Secure Socket Layer, presented at the Computer Science and Information Technology Education Conference, 2002.
[9] H. Chang and E. Choi, User Authentication in Cloud Computing, *Ubiquitous Computing and Multimedia Applications*, pp. 338-342, 2011.
[10] D. Chou, Strong User Authentication on the Web, *The Architecture Journal, Microsoft*, 2008.
[11] H. Chang, C. Jang, H. Ahn, and E. Choi, Authentication Platform for Provisioning in Cloud Computing, *Convergence and Hybrid Information Technology*, pp. 244-248, 2011.
[12] A. Verma and S. Kaushal, Cloud Computing Security Issues and Challenges: A Survey, *Advances in Computing and Communications*, pp. 445-454, 2011.
[13] A. U. Schmidt, N. Kuntze, and M. Kasper, On the deployment of mobile trusted modules, in *Wireless Communications and Networking Conference, 2008. WCNC 2008. IEEE*, 2008, pp. 3169-3174.
[14] C. Covey, M. Redman, and T. Tkacik, An Advanced Trusted Platform for mobile phone devices, *Information Security Technical Report*, vol. 10, pp. 96-104, 2005.
[15] T. MPWG, The TCG mobile trusted module specification, *TCG specification version 0.9 revision*, vol. 1.
[16] S. Islam and J.-C. Grégoire, Multi-domain authentication for IMS services, *Computer Networks*, vol. 55, pp. 2689-2704, 2011.
[17] H.-J. Vögel, B. Weyl, and S. Eichler, Federation solutions for inter-and intradomain security in next-generation mobile service platforms, *AEU-International Journal of Electronics and Communications*, vol. 60, pp. 13-19, 2006.
[18] R. Marín-López, F. Pereñíguez, G. López, and A. Pérez-Méndez, Providing EAP-based Kerberos pre-authentication and advanced authorization for network federations, *Computer Standards & Interfaces*, vol. 33, pp. 494-504, 2011.
[19] Y.-Y. Chan, Weakest link attack on single sign-on and its case in saml v2. 0 web sso, *Computational Science and Its Applications-ICCSA 2006*, pp. 507-516, 2006.

BIIOGRAPHY OF AUTHORS

Kuan Chee Houng obtained his Master in Computer Science (Information Security) from University Teknologi Malaysia (UTM). Besides that, he is Certified Ethical Hacker and Hacking Forensic Investigator by EC-Council. He is currently working as an information security engineer. He has a Bachelor's Degree of Computer Science major in communication and networking. He can be reached at kuan.gcs@gmail.com.

Bharanidharan Shanmugam has received his Ph.D from Univesriti Teknologi Malaysia and is attached to Information Assurance and Security Research Group, Advanced Informatics School, Universiti Teknologi Malaysia. His research interest is towards Network Security, Cloud computing, Intrusion detection systems and risk assessment. He has published works related to those areas. He is a member of IEEE and actively participates in the review process for many journals and conferences.

Ganthan Narayana Samy is a senior lecturer in information security at the Informatics Department, Advanced Informatics School (UTM AIS), Universiti Teknologi Malaysia (UTM), Malaysia. He received her PhD in Computer Science from Universiti Teknologi Malaysia (UTM), Malaysia. His research interests include information security risk management, healthcare information systems security and information security policy.

Sameer Hasan Albakri is a PhD student in information security at UTM), Malaysia. He obtained his Master in Computer Science (Data Communication and computer networking) from University of Malaya (UM), Malaysia. His research interests include information security, cryptography, mobile phone security, information security risk assessment and cloud computing security. For more information about the researcher, please refer to http://scholar.google.com.my/citations?user=swbyAHUAAAAJ&hl=en.

Azuan Ahmad is currently a PhD student in UTM KL.Previously he have Bsc. Hons. Computer Science (Information Security Assurance) in USIM, Malaysia and Msc Computer Science (Information Security), UTM, Malaysia. His research work is on cloud security and malware research. His current research is on Cloud-based Intrusion Detection System.