IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 16, Issue 3, Ver. VII (May-Jun. 2014), PP 61-66
www.iosrjournals.org

An Efficient Windows Cardspace identity Management Technique in Cloud Computing

Smita Saini[1], Deep Mann[2]
1(Dept. of Computer Science Engineering, Lovely Professional University, India)
2(Dept. of Computer Science Engineering, Lovely Professional University, India)

Abstract: *Cloud computing provides the shared infrastructure to the user this lead to the privacy and security violation. Privacy is regarding to the user's sensitive information that resides onto the cloud, unauthorized secondary usage of the data. Windows Cardspace is a digital identity management system that deals with the privacy. It is managed the digital identities inform of Security Token. This paper described the shortcoming of the windows Cardspace that direct to a privacy violation. First issue is reliance on the single layer authentication, second is relying on service provider judgment and third is token storage on cloud. This proposed work will overcome the limitation of the windows cardspace identity management solution.*
Keyword: *windows Cardspace*

I. Introduction

Web applications are moving toward the share infrastructure it raises the privacy and security issues for user data. Cloud computing provides the large storage capacity and platform to the user (There user can deploy services without installation). Users are stored his/her sensitive data onto cloud server but users are not aware how the data are used by administrator (lack of user control) this lead to the privacy violation. For accessing the services users sends a request to the service provider and service providers ask for the claims, these claims can be inform of name, email-id, date of birth, sensitive information(credit card information) and this lead to the phishing attack, identity theft and pharming attack.

To deal with the above problem different identity management solution are OPEN-ID, Windows Cardspace, PRIME (privacy identity management identity management for Europe). This solution provides the help to user what information is to reveal or what should not and who is using his/her data.

In this paper will described the existing windows cardspace identity management solution, limitations of the existing windows cardspace and how those limitation can be overcome by the proposed solution. This paper is ordered as follows: section 2 define the overview of the windows cardspace, section 3 limitation of the existing windows cardspace, section 4 Improving windows cardspace, section 5 Analysis, section 6 Conclusion.

II. Overview Of The Windows Cardspace

Windows cardspace manages the digital identities of the client. Windows cardspace is based on the identification process such as in real world for prove client identity, client need to different identity card for different scenarios (at airport user need passport to prove his/her identity). It exchanges the digital identities in form of security Token and security token contain the set of claims value (SSN, name, email address etc…). Security token is used to prove the client's to whom he/she is claiming. Identity management system is based on three parties [2].

Service Requestor (client) - To whom they are claim.
Service Provider (Relying Party) - It provides the service to the client.
Identity Provider (IDP) - It issues the digital identities to the client (Trusted third party).

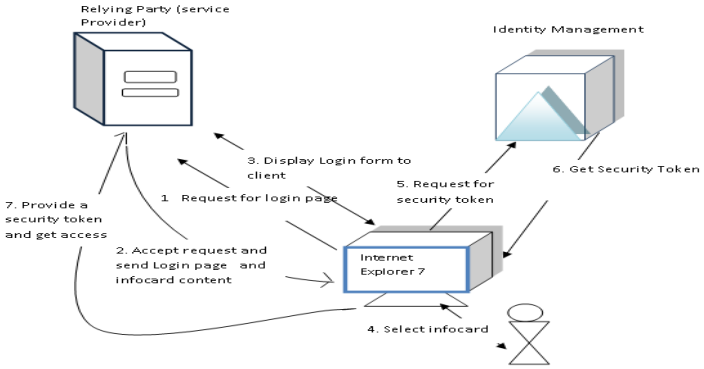

Fig 1 Windows Cardspace Architecture

Fig 1 It described the basic windows cardspace framework of identity management, Windows cardspace makes use of XML based protocols, including Web services (WS-*) protocol and SOAP [1]. Flow of the message is described below.
Step 1: CEUA (card enable user Agent) → RP Request for HTML login Page.
Step 2: RP-> CEUA HTML Login page plus Infocard Tags (XHTML or HTML object tags).
Step 3: CEUA ←→ RP Retrieves security policy Via Ws Security Policy.
Step 4: CEUA ←→ Client. Client chooses the Infocard.
Step 5: CEUA ←→ IDP. User authentication
Step 6: CEUA ←→IDP. Retrieve security Token via the WS Trust.
Step 7: CEUA ←→ RP. Provide security Token via WS trust.
Step 8: RP ← → CEUA Welcome, Successfully Logged in.

III. Limitation Of Windows Cardspace

It described the certain security limitation of the windows cardspace.
***3.1 Relying on the third party judgments*:** User Judgment is based on the trustworthiness of the relying party and it raises privacy violation. User authenticate to the RP by using the Infocard that is recommend by the RP (Step 2).User trustworthy RP judgment is based upon the "Microsoft Recommended high assurance Certificate" such as X.509. Sometime user does not pay attention at the time of approval the digital certificate they do not understand the importance of the certificate they just want to access the services. In Step 7 Security token send to the RP (Authentication) and Security token is a set of claim, claims can be any sensitive information of the user. If RP is not truthful, RP can omit the Users personal information and use this information for unauthorized access of the data. This could lead to the privacy violation. It breaks the Microsoft 3rd Law of identity (which is the law of justifiable parties). According to the law disclose the minimum amount of information. Even RP is providing high assurance certificate but still user must need to Rely on third party Judgment and it is leading to privacy violation.

3.2 Rely on a single layer authentication: As it shown in section 2, security of the Cardspace identity metasystem based on the authentication of the user by the IDP. In case where the single IDP is involved for the multiple RP are involved in a single working session. User authentication to IDP is Rely on single layer authentication, the user authentication is achieved by High Assurance certificate (X.509), and self issued token. In majority of the cases Username/password is used for the authentication, if the session is hijacked entire system can compromise example password can be break by using the brute force attack, key logging and dictionary attack and by using self issued token compromising [3].

3.3 Token Storage on cloud server: RP need to store the security token. As we know security token is the set of claims Step 3 that have the sensitive information it could lead to the identity theft and user may pay for storage service

IV. An Efficient Windows Cardspace Identity Management Technique

It is based upon the existing windows card space and Federated identity management technique this technique will help to improve the limitation of the existing windows cardspace. It prevents the privacy violation of unauthorized secondary usage of data and lack of user control. Sometime user data can be used by the unauthorized user or administrator. This model will prevent from these issues.

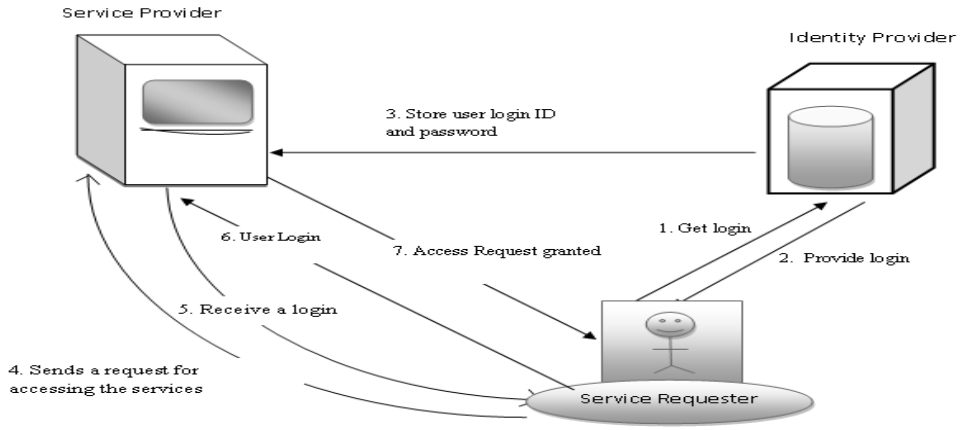

Fig 2 User Authentication Process

In Fig 2, it will describe the user authentication process. The following step will described the message flow for the authentication process.
Step 1: SR (service requestor) → IDP (authentication) Service Requestor authenticates by using username and password.
Step 2: IDP →SR (provide user name and password). If the service requestor is authenticated, Identity provider will provide the Login ID and password.
Step3: IDP → SP. Service provider stores the hash value of the login ID plus password.
Step 4: SR → SP (Request for accessing the service). Now if user wants to access the services, it will send Html login request to the service provider
Step 5: SP → SR (Request for login ID+ password). Service provider request for the login ID and Password for authentication
Step 6: SR→SP (Provides user name +password).For authentication it will provide the login plus password. If the user is authenticated user, Service provider gives the access to the user.
Step 7: SP->SR Welcome, successful login
After user authentication process user can store and fetch his /her data. Following step will describe this process and it will show how it will prevent from privacy issues such as unauthorized secondary usage and lack of user control.

Fig 3: Storing Data

In Fig 3, it is showing how user will store his/her data on cloud.
Step 1 SR → SP It will send request for the services.
Step 2 SP → SP it will follow the user authentication process step 2.
Step 3: SR→ SP user will select the file and upload on the cloud (service Provider generates a File name and security Token).
Step 4: SP → SR. Retrieve security token via Security Trust.
Token will generate by using the filename, Login ID/password and seeder value (Random number algorithm).

Fig 4: File Accessing

Step 1 and Step 2: same as above.
Step 3: SR→SP user will select the File
Step 4: SP → SR it will request for the Token for the particular file that user wants to access.
Step 5: SR→ SP Present a token via Ws security
Step 6: SP→SP verify the token and it will match to the corresponding file. It will provide access to the file.
Token will not store on the cloud server, user will store Token on any storage device so it will prevent from unauthorized secondary usage of the data and lack of user control because for accessing the file user must authenticate and he/she needs Token to the corresponding file. Only legitimate user can access the data even administrator cannot be access the file (Prevent lack of user control) without token.

V. Result

It is implemented by using the Cloud Analyst. It will demonstrate, how it will resolve the privacy issues such as unauthorized secondary usage and lack of user control by using "an efficient windows cardspace identity management technique-in cloud computing", as shown in following message flow.
5.1 Storing the data: it will show how user will store his/her data onto the cloud server and how it will prevent from unauthorized secondary usage.

Step 1: Authentication process, user will login with his/her login name and password. If it is a verified user, user will successfully log into the next window.
Step 2: After successfully login this window will be appearing. It shows the option for browsing a file Upload and Download, as shown in fig 4

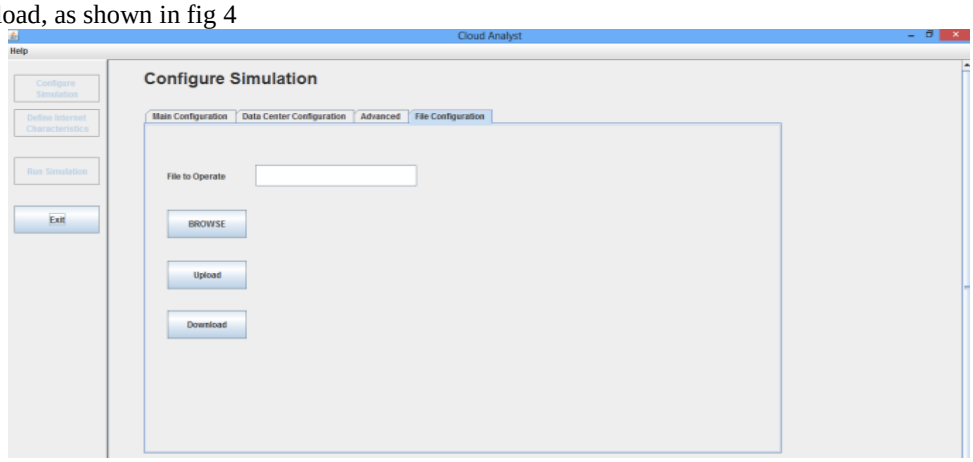

Fig 4 Service accessing

Step 3: After Browse the file, user will click on upload Service Provider will request for seeder number, as shown in fig 5

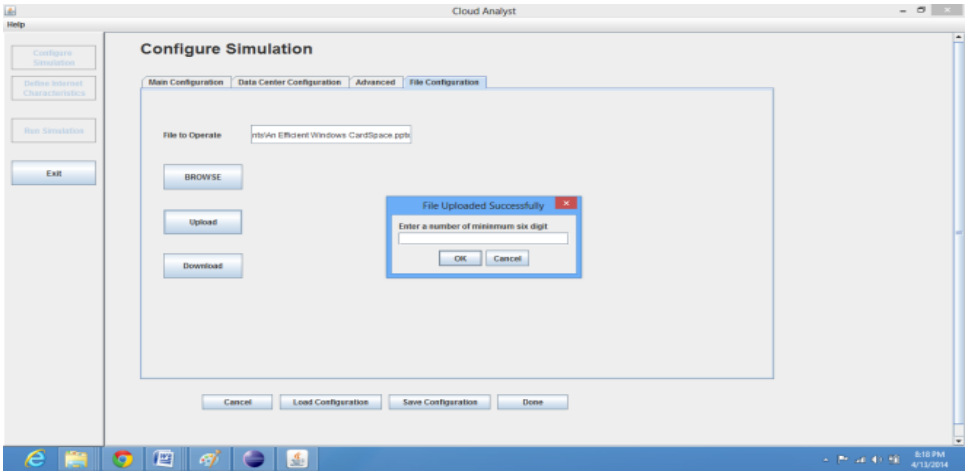

Fig 5 service accessing

Step 5: After entering the seeder value it will generate a file name by using Random number algorithm, it will generate five digit random numbers. This random algorithm based on seeder value that is entering by the user and computational number (Based upon time, processor value, platform etc…). For token generation it will take the seeds value plus password and it will produce a hash value by using the SHA algorithm. User will save this token value on magnetic strip or any other storage device, as shown in Fig 6 and it will successfully upload the file.

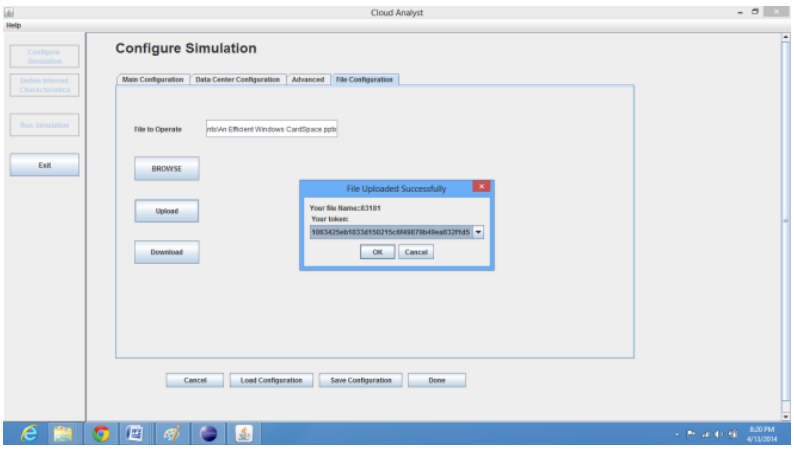

Fig 6 Token and File Number Generation

5.2 Fetching the Data

Step 1: If user wants to access the file it will select the file number as shown in fig 7

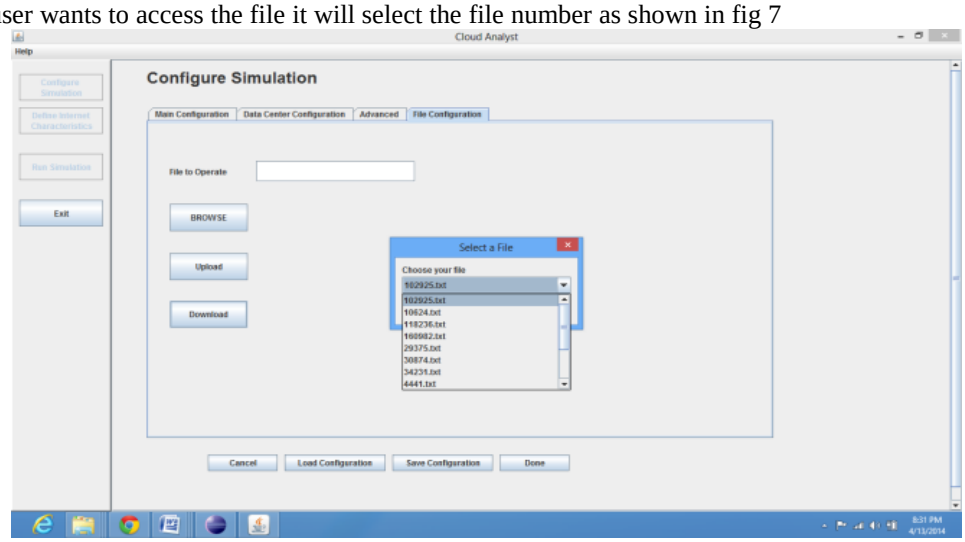

Fig 7 Select file number

Step 2: It will request for the corresponded file token if enter token will verify it will provide the access to the user, as shown in fig 8

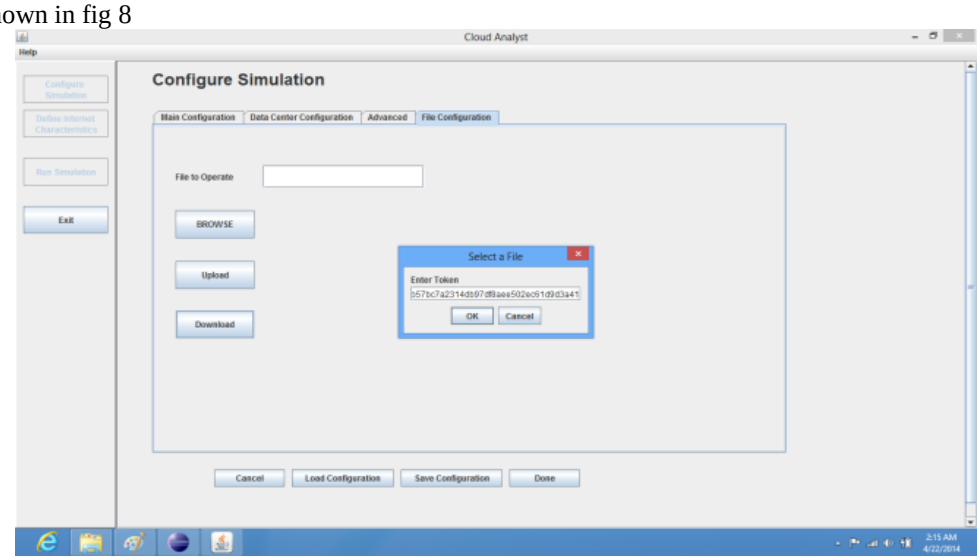

Fig 8 Fetch the file

VI. Analysis

TABLE 1 comparison between existing windows cardspace and improved Windows cardspace

Parameter	Existing windows cardspace	Improved windows cardspace
Authentication	Single layer authentication	Multi layer authentication
Relying on Third party judgment	It provide the claims to the third party	No third party involvement
Token storage	Token is managed by service provider	Token is managed by user

It resolves the privacy issues such as unauthorized secondary usage and lack of user control. An efficient window cardspace identity management technique is not based on the Relying party judgment, so user has appropriately direct on his/her data. If unauthorized user access login name/ password (by using Brute force attack and dictionary attack etc.) but without token, unauthorized user cannot get access on file (Token value is managed by the user). So it is providing the multilayer authentication.

VII. Conclusion

Cloud computing provides a shared infrastructure. An efficient windows cardspace technique-in cloud computing better than existing windows cardspace because existing windows cardspace is based on third party judgment, user provides the claim value to the third party and it is a single layer authentication. It leads to the

privacy issues such as unauthorized secondary usage and lack of user control and efficient windows cardspace identity management technique in cloud computing is not based on relying on third party judgment, it provides the multilayer authentication and the token is managed by the user, so unauthorized user can not access the data.

References

[1]. Understanding Ws-security (2011); http://msdn.microsoft.com
[2]. Bhargav, Noopur Singh, Asher Sinclair (2011) "Privacy in cloud computing through identity Management", Computer Science ,Purude University west Lafayette, IN47907 united state.
[3]. Walees A, Alrodhan and Chris J.Mitchell (2009) "Improve the security of CardSpace" EURASIP Journal on information Security;
[4]. Bharat Bhargav, Rohit.R, Noopur.S "An Entity-centric approach for and identity Management in cloud computing" Computer Science , Purude University west Lafayette, IN47907 united state.
[5]. Kumar Gunjan, G.Sahoo, R.K.Tiwari (2012) "Identity Management in Cloud Computing"; International Journal of Engineering Research & Technology (IJERT); Dept. of Information Technology ; B.I.T. Mesra, Ranchi, India
[6]. Smita saini, Deep mann (2014) "Identity management issues in cloud computing" International Journal of Computer Trends and Technology (IJCTT).