Unified Session Transfer Across Heterogeneous Platforms

Blessy Mathew
Department of Computer Science and Engineering
TKM Institute of Technology, Karuvelil
Kerala, India

Anjali R
Department of Computer Science and Engineering
TKM Institute of Technology, Karuvelil
Kerala, India

***Abstract*— Nowadays, a great variety of electronic gadgets are available in the market. Each user may possess more than one gadget. Also, many services like music or video streaming are made available to the users through Cloud providers. The usage of each device depends on the situation of the user. As the device changes, the continuity of the service lost. This becomes a serious issue in the continuation of work. This paper proposes pmusys, a personalized approach in session transfer between devices, a multi device single sign on approach. This system personalizes the user and gives great security for privacy preservation. This helps many users to enjoy long running Medias across devices with great security.**

***Keywords*— Session transfer , Multi device single sign on,personalization.**

I. INTRODUCTION

Nowadays, multimedia communication and internet services become so popular. Different electronics gadgets become so popular in the present world. It allows a user to enjoy his services anytime/anywhere regardless of the devices or terminals. Each user have more than one gadget. Due to the dynamic change in situation, the service enjoyment became a problem. As a result, a user enjoying a long duration service may desire to keep the same session across different devices during the lifetime of the service consumption, maintaining continuity. Here comes the need of adequate multi-device Single Sign-on technology (MD-SSO). Single sign on is a property of access control of multiple related, but independent software systems. With this property a user logs in once and gains access to all systems without being prompted to log in again at each of them. The credentials used at initial authentication are used for comparison for different applications.

Benefits of using single sign on includes: reducing password fatigue from different user name and password combinations, reducing time spent re-entering passwords for the same industry and reducing IT costs due to lower number of IT help desk calls about passwords. SSO shares centralized authentication servers that all other applications and systems use for authentication purposes and combines this with techniques to ensure that users do not have to actively enter their credentials more than once. Multi-device single sign is defined as" single sign-on that crosses the devices"[13]. That is, the session initiated from one device, and subsequently transferred to a second.

Service delivery is typically motivated by a desire to avoid management of commodity services which, through economies of scale, can often be delivered more efficiently by such providers. This trend, together with the increasing usage of small portable devices and wireless networks is paving the way to real anytime/anywhere computing. Nowadays, due to the dramatic evolution of technological convergence, the different consumer electronic devices that a user owns have similar capacities and may allow him to access the same applications and services. The usage of one device or another will depend on the context, i.e. on which option suits better to the current situation. Furthermore, users want to enjoy services on the move, which entails dynamic changes of context. As a consequence, a user enjoying a long duration service may desire to keep the same session across different devices during the lifetime of the service consumption, maintaining continuity. Majority of the previous work concentrated on session initiation protocol.

Many varieties of consumer smart devices with support of mobile computing combined with emerging cloud computing paradigm is paving way to real anytime/anywhere computing. Usage of these devices depends on context. But service continuity when moving across different terminals is a serious problem. So a middleware architecture is necessary to solve this problem. Even though some traditional ways are there, few implementations have been developed and there is no mainstream adoption of MD-SSO technologies, which is especially remarkable and led me to analyses the reasons and proposes a solution. Major works are concentrated on session initiation protocol. In this architecture, session, context and communication are described. This paper mainly focuses on the handling of multiple users. It also helps to personalize the nature of the user. The session handling is the major function involved in this. The state of the applications are stored and processed by considering the security of the system. Repeated authentication is completely avoided here.

IJERT

The values of application state vary according to the nature of applications. These values are stored at the cloud storage and there by speed up the computation. Security state values are also stored at the cloud storage securely. Thus it gives a high performance. This paper can make many drastic changes in the field of consumer electronics since it works independent of the electronic gadgets. This work gives importance to the user and his characteristics. That is, a user-centric system. So user can select the security system that is available in his/her gadgets. According to the nature of the site also user can configure the system. This is very important when considering the personalization and privacy isssues.

II. SESSION MOBILITY

Session mobility is the process of transferring an active session running on a device to another terminal connected to another access technology. Traditionally, there are four types of mobility : Terminal Mobility, allowing a device to change location and still be able to communicate; Personal mobility(or user mobility), when a user can keep his or her user identity irrespective of terminal or network; Service Mobility ,making a particular service accessible by the user, regardless of terminal or network, and lastly Session

Mobility(or continuous user mobility), letting the user change location or device and still be able to keep media streams active[6].

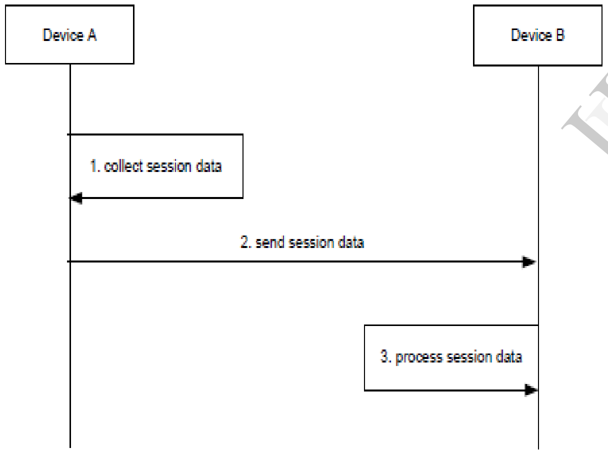

Fig 2.1 Simple session mobility

Let us consider the example of a session mobility scenario between device A and device B as depicted in Fig 4.2. In the first step of the session transfer, device A gathers the information about the current session. During this step information such as what media is being consumed; the current media position; and the current status of the session (play, pause, etc.) are collected. As a second step in the session transfer, the collected information is sent to device B and device A stops the session. To complete the session transfer, device B processes the received information and continues the session.

Although this is a simple example of session mobility, there are three clear steps:

- Collect session data
- Transfer session data
- Process data and continue session

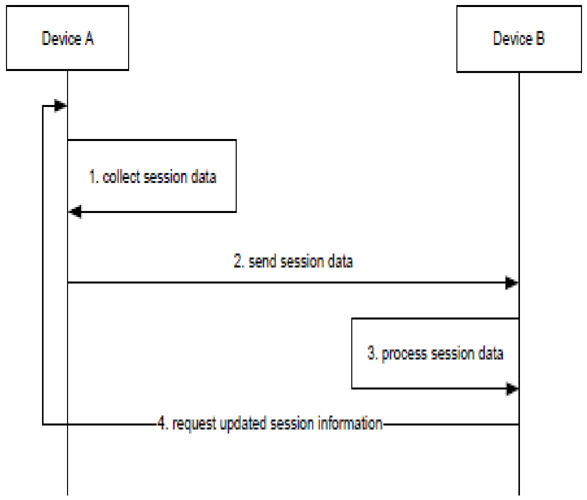

Fig 2.2 Advanced session mobility

IJERT

It is possible to think of more sophisticated protocols for session transfer; for example, the protocol described above can be extended to allow multiple updates of the session information. This can be useful when clients A and B are required to be synchronized before the session transfer is

completed. Fig 4.3 shows how this can be realized. Until the initial startup of the session on device B the algorithm is identical except for the fact that, here, device A does not stop the session but continues until device B tells it to stop. After the initial startup of the session, device B requests new updates so that the current position of the media can be adjusted. The updates can be repeated until the session on device B is synchronized with device A. At that point device B can tell device A to stop and the session is then successfully transferred to device B.

Session Mobility is one of the aspects of mobility that bring out many advantages including:

- New Capabilities for the customers
- Better Utilization of Resources
- Higher user satisfaction level
- Service Persistence: Services more attractive
- Leverage frequency and duration of service usage: More benefit for the service operators.

III. SCOPE OF THE PROJECT

Along with the evolution of session mobility, the transfer of sessions across heterogeneous devices becomes more and more important. So ensuring security to the session mobility is an important thing. The proposed system aims at implementing security in session mobility across devices in heterogeneous environment. The functions of this system are user centricity, flexibility, performance and security. Its most important features are security and flexibility compared to the traditional systems. It allows users to move sessions from more than one application and can be restored without considering the operating systems. Here , the problem when considering multiple users also solved. It uses the Quick response code for solving this problem.

IV. RELATED WORK

Some traditional concepts are there for the session mobility across terminals. But few implementations have been developed and there is no mainstream adoption of MD-SSO technologies. SUSSO is a middleware architecture that allows sessions initiated from one device to be seamlessly transferred to a second one, as might be desirable in the enjoyment of long running media.

Proposals	User centricity	Flexibility	Performance	Security
SIP-based	-	-	NA	+
Proxy based	-	-	NA	Security+ Privacy -
SuSSo	+	+	+	Security+ Privacy- (single user)
Pmusys	+	+	+	+ (multiple users)

Table 4.1 :Comparison of different session transfer solutions

IJERT

Uta Christoph et al.(2011)[2] proposed an architecture for the automatic adoption of the behavior of a mobile device depending on the change of user context. It detects the movement patterns, based on the built–in sensors of the android GC smart phones. Fig 4.1 shows a clear comparison between other proposals to inderstand the importance of the work. It takes 4 functional requirements to compare their functions. They are user centricity, flexibility, performance and security. SIP based system is proposed for some specific purposes. So it doesn't consider the users and flexibility. Security is addressed by almost all systems, although proxy-based systems create privacy issues due to storing user data in external servers and doesn't even take into account security considerations. Other works concentrates on proprietary implementations that only work within a narrow set of devices belonging to the same manufacturer or for a specific application or service. The majority of works focus on SIP-based session mobility. All reported approaches deal with few non-functional requirements. This one is fully consider the user's preferences and configure the system according to their need. Also it is flexible to users in any environment. It gives a high performance. .When compared with the SUSSO, the major advantage is privacy. Since it uses IP address and

QR code, biometric feature and digital signature, the security is fully considered But my solution PMUSYS satisfies all these and can be used for a real time application service.

V. SYSTEM ARCHITECTURE

This architecture helps to generalize the multi device single sign on by considering the privacy features also in a multi user environment. In Susso architecture[2], we can see how the context management and session transfer is performed. This is the underneath technique behind the session mobility. This architecture clearly gives an idea that how the personalization is done.

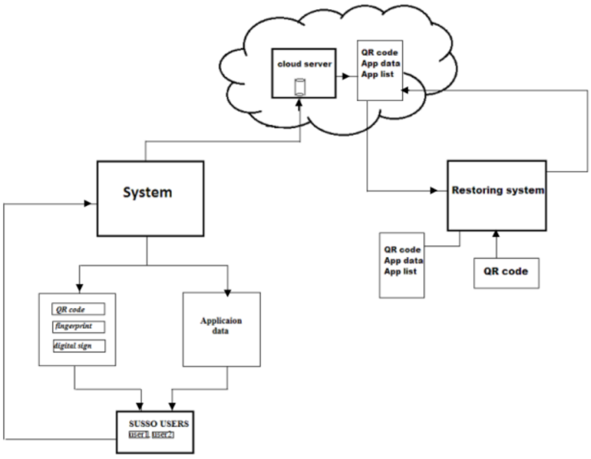

Fig 5.1. Architecture of the proposed work

PMUSYS system connected to user which is capable of playing different application. This system has a cloud interface for storage holding application data, application list, preferences etc. The switching from one system to another is possible by context management, state management, session transfer and automatic session restoring. In the base system, connected to users registration independently. Every user has profile, containing QR code generated as the attribute of user. A biometric feature of user is kept as a fingerprint template. A cryptographic key is generated as digital fingerprint. All these are used for identifying a user attached with the PMUSYS application is another environment. This profile is generated and mapped to every application for every user at the time of registration.

The switching process starts automatically or by user request (on demand). Parameter passed to cloud storage. The second phase, another system with restoration of context information takes place here. Authenticity of user is verified with cloud credentials.

For the personalization, cloud storage information for analyzing the usage cluster. The goal of the system is to filter the available items and show only those that are more relevant to the user(s), taking also into account security and privacy.

We divide this profile information into two subsets: data related to security and privacy configuration; and data for content personalization. The first subset of data is sent to the Security Manager and translated into a security policy. On the other hand, all the information that is relevant for personalization is represented based on Vector Space Model techniques [12]. Thus, when a user registers her profile, an initial *Personalization Vector* (*PV*) is created with the form:

$$PV_i = [w_1 w_2 \ldots w_n], w_i \in \{0,5\} \qquad (1)$$

Where each component *wi* represents the degree of preference that the user assigns to attribute *i*. Values of *wi* range from *0* to *5*. And the set of attributes (or corpus) is composed of a number of ordered keywords that can be used to categorize items, either these items are programs or web applications. For example, a *PV* with values *[5 4]* for the set of attributes (social network, games) means that the user likes social networking sites related items with the maximum degree of preference, and that she likes games-related items with a degree of preference equal to *4*. So, the system will put sport programs in the first place when showing recommendations for this user.

The fig 5.2 shows the modules in personalization. The user's personal details and security policies are managed perfectly for personalize the system. It works in two sides-one is client side and other at user side.

VI. IMPLEMENTATION DETAILS

PMUSYS is implemented for two streams of applications. One is a web application and other is a desktop application. Desktop application is implemented in a media player for playing videos and audios. Web application is implemented with a browser and applications like facebook and gmail. The first phase is registration. Registration is there for both web and desktop application. Thus the video or audio can be selected and played. When a dynamic change in context occurs, the session is automatically switched and played at the destination device. The switching is performed only after checking the security constraints stored during registration.

IJERT

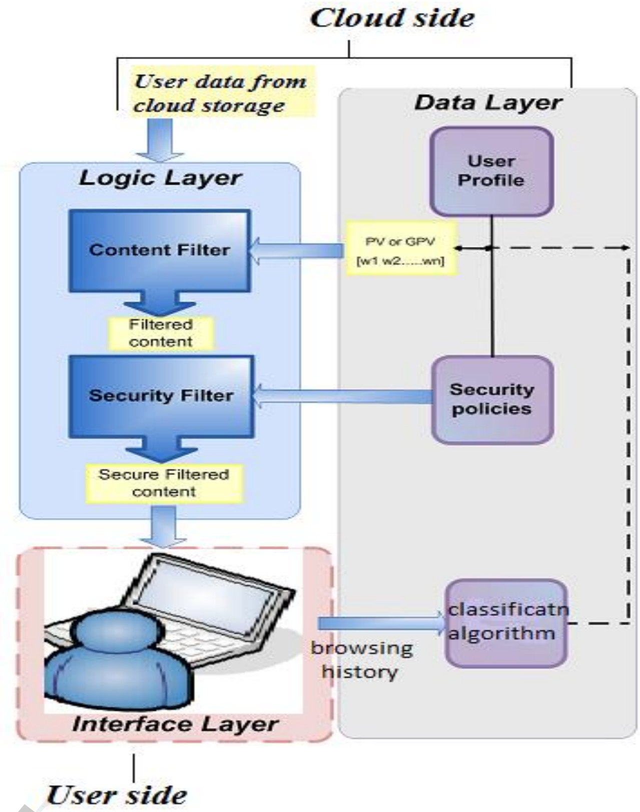

Fig 5.2 Personalization component view

In case of web application, given urls are automatically send to server. When a destination device asks for restoring, the urls send to that device after security checks. Since urls are simple text, there is no network overhead. If authentication is required for the site, it uses the credentials stored at the time of registration. Thus the required session is successfully restored at the destination device. At the time of restoration, the main aim is preservation of privacy. Here it handles this by QR Code system, biometric system and digital signature system according to the need of user.

VII. DISCUSSION

Due to personalized session transfer system, a security management system must comply with some basic factors. According to our research the most important are privacy, flexibility, transparency/seamless operation, security, and performance. PMUSYS covers all these factors as it has scalability due to its modular design. It can performs the personalization. PMUSYS has two step phases in application switching, one at the source system and another at the restoring system. PMUSYS has user configuration mode and user can select the security modes according to their gadget. This helps to share their resources and characteristics with other gadgets by applying more strict security policies. The privacy preserving features are the important ones.

VIII. CONCLUSION AND FUTURE WORK

The transfer of sessions across devices with multiple users performed successfully. The privacy feature also maintained while considering multiple users. This is a useful generic middleware architecture useful in many fields. It can maintain the continuity of the services. It is secure, flexible, user centric and high performance one. It is implemented in both desktop application and web application. A desktop application is implemented using a media player. In web application, facebook and Gmail are switched without any re-authentication. It works independent of platforms. An added advantage is the personalization in web search. This system constitutes an important step advance in the field of ubiquitous computing. The study reveals that it is feasible in all ways.

It has a disadvantage of photocopying of QR code. The future work is planning to solve this problem.

ACKNOWLEDGEMENT

Firstly I would like to thank the Almighty, that I was able to complete the project design document within the given time. I express my sincere thanks and a deep sense of humble gratitude to the Principal of this institution, **Prof. Muhammed Kasim S** for providing us all necessary facilities. I extend my sincere and heartfelt thanks to **Prof. P Mohamed Shameem**, Head of Department, Department of Computer Science and Engineering, for providing me the right ambience for carrying out this work. I also express my immense pleasure and thankfulness to my project coordinator, **Ms. Rahila N A** for her valuable advices. I am profoundly indebted to my project guide, **Ms. Beena Philipose** for her innumerable acts of timely advice, encouragement and I sincerely express my gratitude to her.

IJERT

REFERENCES

[1] Patrica Arias, Florin, Rosa 'Susso: Seamless and ubiquitous single sign on for cloud service continuity across devices' , IEEE transaction on comsumer electronics December 2012

[2] Uta Christoph, Jan von 'Context detection on mobile devices '2011.

[3] M.Adeyeye, N. venture 'SIP- based web client for HTTP session mobility and multimedia services' communications, pp-954-964,May 2010

[4] M. Barisch 'Design and evaluation of an architecture for ubiquitous user authentication based on identity management systems' IEEE international workshop on trust and identity in mobile internet, computer and communications, 2011

[5] P. Arias cabarcos , R. sanchez guerrero, F. Almenarez, D. Diaz Sanchez, A.Marin Lopez 'FamTV: An architecture for presence-aware Personalized television' IEEE transaction on comsumer electronics,Vol. 57, pp-6-13 February 2011

[6] Robin Singh Bhadoria , Deepak Sain, Rahul Moriwal (2008) 'Data Mining algorithm for personalizing user's profiles on web' International Journal of Computer technology and electronice engineering, Vol.1, issue 2

[7] Weighing Qiang, Aleksandr Konstantinov, DeqingZou, LaurenceT.Yang(2012) 'A standards-based interoperable single sign-on framework in ARC Grid middleware' Journal of Network and Computer Applications, Vol. 35,pp-892–904

[8] P. Madsen (ed)(2008) 'Liberty ID-WSF multi-device SSO Deployment guide'

[9] M. Sathyanarayanan(2001) 'Pervasive Computing: Vision and challenges'

[10] Junzhou Luo, Xudong Ni, Jianming Yong (2009) 'A trust degree based access control in grid environments' Journal Of Information Sciences, Vol.179,pp- 2618–2628

[11] Ji-Young Kwak, "Ubiquitous Services System Based on SIP," *IEEE Transactions on Consumer Electronics*, vol.53, no.3, pp.938-944, Aug. 2007

[12] S. Cantor, J. Kemp, R. Philpott, and E. Maler (Eds.), "Assertions and Protocols for the (OASIS) Security Assertion Markup Language (SAML) V2.0," OASIS Standard, March 2005.

[13] P. Madsen (ed.), "Liberty ID-WSF Multi-Device SSO Deployment Guide", 2008