WIRELESS SECURITY ISSUES IN UBIQUITOUS COMPUTING USING BIOMETRICS

Abida Batool*

Sara Imtiaz Cheema**

Tasleem Mustafa***

ABSTRACT:

Security services, resembling verification and access control, have not only maintain user actions prepared with a variety of devices but also guarantee the security issues, privacy, and discretion for resources of ubiquitous computing.

New impression of action-based computing is used in order to prolong human actions in ubiquitous environments. Need for supporting users with wireless applications becomes essential in such kind of environments where users are using a massive quantity of diverse computing devices. Though, without taking into account fundamental protection issues, it could be widespread with vulnerabilities.

In this paper, security method is discussed which is based on biometric system. The planned method aims to boost security services on wireless devices and make easy user activities. The standard protocols that are newly and existing used for wireless security are explained.

Keywords:

Ubiquitous computing (UC), Ubiquitous (Ubi) Security, Authentication, Biometrics central control system (CC system).

* Department of computer science, University of Agriculture, Faisalabad, Pakistan

** Military college of signals, NUST, Islamabad, Pakistan

*** Chairman department of computer science, University of Agriculture, Faisalabad, Pakistan

I. Introduction

The vision of ubiquitous computing is to push the traditional or desktop interface into highly transparent environment and interface. History is full of model shifts in which human and computer relationship is perceived. Recently paradigm shift is of ubiquitous computing or UC in short. The idea of UC is proposed by weiser [7,8]. Basically the trends followed by computing are as follows Fig 1:

1) Mainframe(past)
2) Personal computers(present)
3) Distributed computing
4) Ubiquitous computing

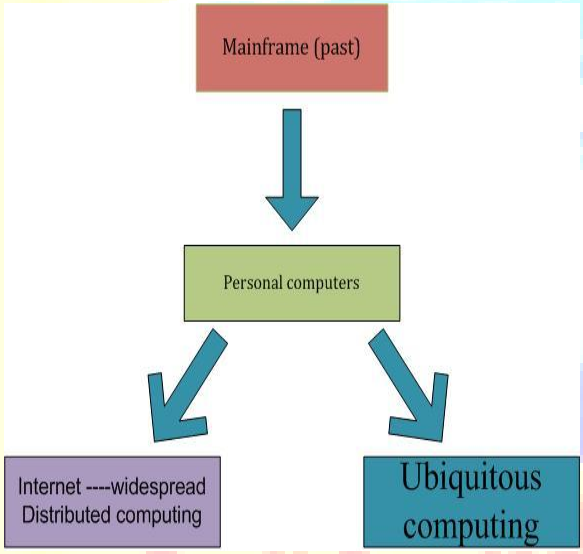

Fig .1 Major trends in computing

Ubi wireless world systems generate a number of necessities, e.g.; interoperability, mobility and compliance for Ubi systems and technologies of software. The major challenges of ubiquitous software are a adaptive and standardized technology of middleware, services interoperability, networks and set of enabling technologies.

Since ubiquitous computing deals with the amalgamation of the isolated fixed entities, it is not sufficient to launch a stand-alone solution or application. Every new theory, idea, application or service should be able to interoperate, join together and collaborate with

already available services and infrastructure. Every testing for evaluation of a fresh idea essentially needs the presence or production of a detailed environment [3].

Elements that define ubiquitous computing: [5]

1) *Ubiquity/Pervasiveness* – lots of devices.
2) *Connectedness* – the devices are networked.
3) *Context-awareness* – the system is aware of the context of users.
4) *Invisibility* – devices are apparently becomes invisible.

The technology of Ubi computing embeds in our daily life routine by giving services, information and applications over various networks with the help of different devices. UC is a precondition for insidious computing which insist on mobile data entrance and other strategies for wandering users or nomadic users.

Technology required for UC :

1) economical, VLSI technology (nanotech),
2) Very low-power computers with convenient displays,
3) Low-power, ultra-fast network for communication:
    i. wireless end-points
    ii. cellular topology
    iii. wide-bandwidth range

In this paper, main focus is on wireless security issues and also suggests possible solutions as this is one of the main parts of UC framework.

II. Problem statement

Many people and organizations have tried to build ubiquitous environment for his own use but they are failed because they are utilizing their own techniques and methods no doubt they have build some applications but these applications are only for themselves and are bounded to be used in their specific environment. While, UC is the concept of utilizing this kind of infrastructure for everyone and for anyone at any place and time.

There are so many issues regarding implementing UC applications. So, it is not possible to move further before analyzing the hurdles and issues faced by engineers until all issues are resolved. Hence, it is highly important thing to do an analysis of all UC applications made up till now so that all facing challenges can be identified. Further it is

also imperative that their current status be identified that whether they are resolved or still unresolved.

No doubt there are so many challenges in the way of UC implementation but In this paper all possible wireless security challenges found in ubiquitous computing are identified. Several wireless security challenges for UC found so far along with their possible solutions followed by the conclusion are presented below:

A. Some Security Threats of Wireless

In spite of the efficiency, ease and price tag benefit that are offered by Wireless, the use of radio waves in network of wireless generate a threat of hacking. The basic three threats are as follows:

1) Denial of Service
2) Spoofing
3) Eavesdropping

1) Denial of Service:

In such type of hit, the accessibility of the network resources is affected by legal or illogical messages or by network floods created by burglar. As radio transmission is more susceptible to hacking so there are extra probabilities of rejection of service. Comparatively short bit charge of Wireless can easily be decreased and make them undo to attacks of denial of service [9]. Radio interference can effortlessly be generated by using a dominant transceiver, which makes wireless incapable to communicate using radio path.

2) Spoofing And Session Hijacking

By assuming the distinctiveness of a legal user the invader possibly will get access to confidential data and assets present in the network. This occurs due to 802.11.The source addresses are not authenticated by network, which is MAC (Medium Access Control). MAC consists of frame address. Attackers hijack the sessions by using MAC addresses. Furthermore, an Access Point is not needed for 802.11.These help

attackers who pretend to be as AP's [4]. There is a strong need of access control which can control these threats.

3) Eavesdropping

Attack on private data that is transmitted over a network is called eavesdropping. By design wireless spread network load towards space consequently it is not viable to have power over the access to signals. Eavesdropping is the largest part of threat in these circumstances due to the attacker that can easily interrupt the broadcast slightly away from the area of company.

III. Proposed Solution

In spite of the risks and threats linked with networking of wireless, there are surely so many situations that require their usage. There is a possibility still for users to make safe their Wireless network to a satisfactory level. This can be completed by implementing the actions to reduce attacks into the core networks which are following [10]:

a) Using innovative Standards for WLAN Security enhancement:

The standards are defined previously such as 802.1x and 802.11i that can also be used for securing our wireless networks.

b) Think Like Hackers:

The second solution is to develop applications by thinking like hackers so that there are no loop holes remains to enter in our system illegally or in an un-authorized way.

c) Using Biometrics For Authorization:

Biometrics is the use of physiological and behavioral characteristics to offer the detection of individuals as applied to physical and network security within a business [4].A major feature of information security is the ability to protect a resource from internal and external threats. The field of biometrics serves as the way of protecting both the physical building of a business and the IT tools that provide as its information resource. Biometrics signatures are used in different form like[1].

1) Thumb impression
2) finger line feature
3) palm feature

4) teeth shape extraction
5) eye retina contact etc

So we can use biometrics instead of passwords for our wireless security.

d) Working

This system work by comparison of existing biometrics saved in database as existing password is matched with entered password. The system working or initialization is explained through diagram shown bellow. Fig.2

By using biometric the access to the system is provide only to those that are real authorized persons. Also these security plans definitely eradicates or minimize the hacker attacks. For the implementation of biometric security system we need tools that are already in usage.

The proposed suggestion is an effort to make the UC a real world technology and also acceptable to a common user as it minimizes the security risk.

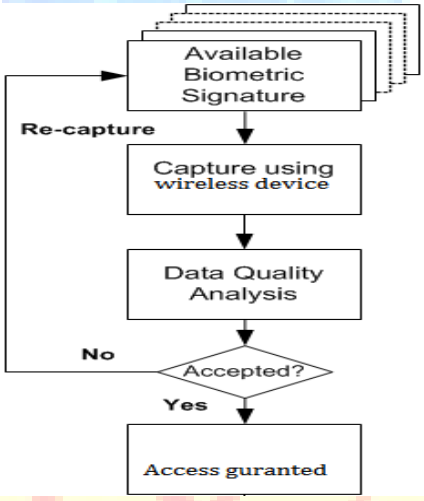

Fig.2. Authorization by pattern matching using biometric as a wireless security

e) Implementation model

The proposed implementation model for UBI—HOME which can be secured by using biometrics and specially thumb impression. Ubi-home is kind of smart home in which there is no interventions of human being .the decision are taken by itself or by following the context [2].

In proposed model all home appliances are attached to central control system (CC system) and anyone who want access to home or any appliance at home can only get access by using biometric system. The user may connect from home or remote area.

The nomadic/remote user first attached with WIFI-cloud near to home after that by using biometric system the user can get access to their home's central control system. In this way authorized person can enter to the UBI-home system only. And the risks of threats and security issues are minimized. All scenarios are shown in fig 3:

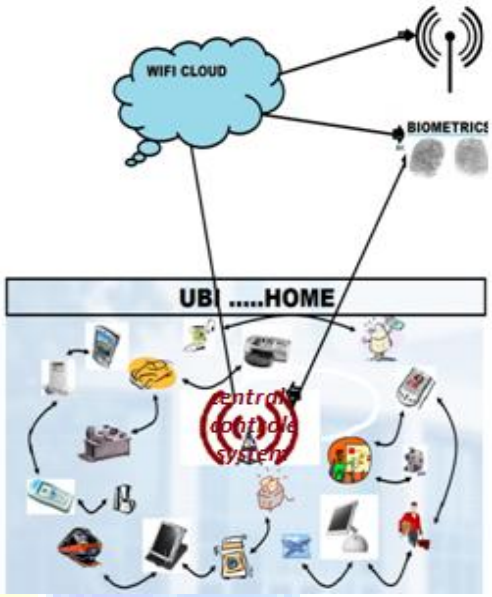

Fig.3: **Authorization by using biometric as a wireless security in ubi—home**

IV. Conclusion

In this paper, the major security concerns in the Ubiquitous Computing are analyzed. In order to handle such concerns, effective solution dealing with key security concerns are introduced and proposed. A kind of novel system is proposed for UC wireless security user verification by using biometrics. The proposed solution can be functional in diverse wireless platforms and can also used to boost protection over invasion, robbery and exploitation of UC devices.By practicing the recommended actions users of Ubiquitous Wireless can defend their networks that are mentioned in the paper which is totally based on the price tag and the altitude of security that they desire.

Reference

[1] D. Lee, K. Choi, H. Choi and J. Kim, "Recognizable-image selection for fingerprint recognition with a mobile-device camera," IEEE Systems, Man, and Cybernetics Society, vol. 38,issue 1, pp. 233 – 243, February 2008.

[2] Baris Yuksekkaya, M. Bilgehan Tosun, M. Kaan Ozcan and Ali Ziya Alkar. "A GSM, Internet and Speech Controlled Wireless Interactive Home Automation System" IEEE Transactions on Consumer Electronics, Vol.52 No. 3, pp: 837-843, 2006.

[3] E. Bardram. Activity-based computing: support for mobility and collaboration in ubiquitous computing. Personal and Ubiquitous Computing, vol.9 (5), pp.312-322, September 2005.

[4] A. Jain, A. Ross, S. Prabhakar, "An introduction to biometric, "IEEE Transaction On Circuits and System for Video Technology, vol. 14, no. 1, pp. 4 – 20, 2004.

[5] Mark Burnett, Chris P. Rainsford, Department of Defense, Australia,"A Hybrid Evaluation Approach for Ubiquitous Computing Environments. Vol. 1(2001).

[6] M. Weiser. Some computer science issues in ubiquitous computing. Communications of the ACM, 36(7):75-84, July 1993.

[7] M. Weiser. The computer of the 21st century. Scientific American, 265(3):66-75, September 1991.

[8] "An Overview of Biometrics." Computer Science and Engineering] Department. Michigan State University. http://biometrics.cse.msu.edu/info.html

[9] Knowledge Systems (UK) Ltd. "Wireless LAN Security Issues." URL:http://www.ksys.info/wlan_security_issues.htm

[10] Geier, Jim. "Guarding Against WLAN Security Threats." URL:http://www.80211planet.com/tutorials/article.php/1462031.