ISSN 2047-3338

Data Security of Heterogeneous Devices in Ubiquitous Environment

Binish Raza[1], Muhammad Fuzail[2], Anum Aftab[3] and Muhammad Omer Mushtaq[4]
[1,2,3,4]Department of Computer Science and Engineering, UET Lahore, Pakistan
binish155@yahoo.com[1], m.fuzail@ymail.com[2], anumaftab772@gmail.com[3], engr.omermushtaq@gmail.com[4]

***Abstract*— Today, the growing interest for mobile devices is a call for advanced researches in the emergence of 'Ubiquitous Computing'. A Ubiquitous Computing is "a paradigm shift where a technology becomes apparently invisible in our life". Intuitively it can be defined as making computer systems persistent in enhancing user interaction with the environment, as impeccably as possible. Its main objective is to provide computing to a user from anywhere and anytime. For this, computing systems are developed that provide services at any time and anywhere throughout the physical world. The words anywhere and anytime are attractive but more appealing for the security of this computation that can be of a precious data. So the need of security on such protocols cannot be overlooked. This paper discusses the security issues and various existing technologies on security of heterogeneous devices.**

***Index Terms*– Ubiquitous Environment, Security Issues, Ubiquitous Environment and Techniques**

I. INTRODUCTION

TODAY, an unbelievable diversity of computers and applications, covering the whole world, has deep and important influences on all parts of society. Computer technology advancements has entered in human lives because they can perform difficult tasks faster and easily or certain tasks automatically.

In the world of Ubiquitous Computing, computers and humans can be regarded as units of a single system and they are said to influence each other. In other words Ubiquitous Computing is computing in which both Humans and Computer surrounding each other everywhere and interacts with each other by removing time and location barrier [1]. The ultimate target of Ubiquitous Computing is required to be distraction-free. Due to latest developments in computer technology especially development in computer hardware computing technology leads to the idea of Ubiquitous Computing.

It comprises communication between different networks from different operators with different technologies and controls. This increases the interest of user to enter in ubiquitous environment because it provides freedom to select the applications, access and services [11].

The usage of mobile devices is increasing with the passage of time because in current era of latest technologies these are considered as much more powerful hardware devices that enable data connectivity and different software's integrity that are efficiently invisible to the user. They are considered as most convenient computing devices. Such devices, also referred as handheld computers, having features of running applications on the platform with some software and operating system.

Certainly, numerous researchers have admitted that security is one of the major and evolving problem in this environment. However, security and privacy issues in such surroundings have not been investigated thoroughly. The characteristics that make Ubiquitous environments expedient and dominant on other side make them at risk to confidentiality and authentication threats. Security systems and strategies that are used conventionally may not supply sufficient security to deal with the new exposure and susceptibilities. Ubiquitous environment is susceptible to both active and passive attacks, such as modification of message contents, replay, eavesdropping and release of message contents etc.

The system must have the ability to prevent from any malicious effect; this will protect the system and did not cause any harmful effect to the complete system.

This is the motivation of moving towards contextual information, where we are free for the usage of any input/output device, any heterogeneous devices and other mobile users: all are connected with such computational environment (Fig. 1).

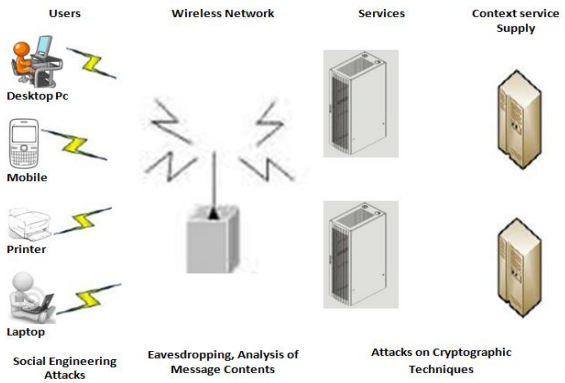

Fig. 1: Ubiquitous Environment with Security Issues

Next section gives an overview ubiquitous computing. Third section describes the design goals of Ubiquitous computing. Fourth section explains the security issues and its solution. Fifth section describes technical background of researches already made in this area. And sixth section describes the conclusion of our paper.

II. UBIQUITOUS COMPUTING

Ubiquitous computing is one of the latest paradigms of 21st century. It can be defined as "*existing or being everywhere at the same time"*, situations take place in this computing are very similar to the real world [9]. In this computing the systems and appliances are embedded and incorporated with computing, communication and wireless capabilities that can process and provide information.

It facilitates the systems and appliances that should change themselves according to the user environment rather than users have to do this. Subsequently users cannot realize the presence of ubiquitous computing systems because these devices and systems are integrated with the user's environment so overwhelmingly.

In today's research, researchers are focused to introduce the concept of human computer interaction in ubiquitous environment. The usage of folk's devices leads us towards a new intelligent environment, where all devices can interact easily from wherever to somewhere. Such intelligent environment can take decision by itself with the help of other devices.

In some cases devices are communicating within a boundary area, which is a problem. Consider a device that communicates within 100 km of its connected system. Under the bounded area device can easily communicate but, as soon as it cross its territory communicating with the system will cause some problem [2].

III. HISTORY OF UBIQUITOUS COMPUTING

Father of Ubiquitous computing, Mark Weiser at Xerox lab as a chief technologist during his research used the phrase "Ubiquitous Computing". ''Ubiquitous' is a Latin word meaning 'anytime and anywhere' or 'exist simultaneously.' He wrote some initial papers on developing ideas of Ubiquitous computing. Mark Weiser have influence by several fields like phenomenology, philosophy, sociology and psychology other than the computer sciences. He concentrated on understandings the influence of these fields on life of users while sharing of computing power to everyday life [9].

The "media cup" also called a "Smart Coffee Cup" is a model of ubiquitous system. This cup is equipped with sensors, networking, elements and processors that communicate with the owner of the cup. By using sensors and processor and networking elements it store information about the owner.

The research theme of ubiquitous computing consists of computerized capture, access and integration. Different institutions develop different experimental applications on the bases of this theme. At Georgia Tech institute Classroom 2000, application was designed to facilitate students to provide recording lectures and have access to the lectures, so that they can focus on lecture rather than wasting time on writing notes. This can be accomplished by electronic boards that are provided to the teacher to record and capture the lecture effectively.

IV. DESIGN GOALS

There are three overarching goals: "adaptability, deployability and aggregation", adaptability and deployability are the central points of ubiquitous computing. In such environment heterogeneity, legacy component and incremental evolution are not considered in exception case [14] (Fig. 2).

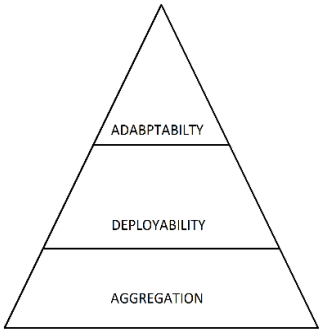

Fig. 2: Design Goals of Ubiquitous Computing

Adaptability

Software's handle dynamic emergence of devices in system evolves context and user preference at different level. Having the feature of dynamic changes adaptability is considered as the basic concept of ubiquitous computing. Adaptive system introduces the basic concept of the requirements which are accepted at different level in the system. This feature may lead us toward the user requirement what he wants in his system, and explicitly controlled by the users. It requires different approaches as:

i). *Laissez-faire approach* states adaptation in a system is totally depends upon the users, that what he wants from the system without any manual involvement. This is much difficult to deploy in any system. The reason behind this is the size of file may be too large or too short; which is difficult to handle.

ii). *Transparent approach* provides all basic needs which system require for making an application adaptable. Due to this, system is responsible to handle all aspects of user demands [15].

Deployability

To interact with a system we require some interface through which user can easily interact, for the deployment in context environment there are some requirements and specifications:

i). Flexibility the system should not force the users to follow the same pattern through which the system is designed, in order to introduce the new appliances for the network.

ii). Management of the deployer is responsible to manage all the resources for application specification, mapping to resource and gathering all resources.

Aggregation

Generally refers as, "a function in data processing". This function leads us towards the joining of different data packets from a network and makes it possible to transmit it on a network as a single media. This feature is the base constraint of some application running on the system.

V. SECURITY ISSUES AND SOLUTIONS

Time and locality is the two important consideration for security design .In ubiquitous computing both time and locality is enhance in multiple computing explicitly. Authentication of security mechanisms and controlled access in the systems created by manufacturer can be implementing with powerful protection methods. Slack of authentication and control protocol improve the role of security. The systems to become extraordinarily secure systems, it should be the system that identifies all things that is happening or going on. Security from user's perspectives is the safety of its data from unknown person. The system security can be described as server and client side security. The system security includes the protection of user data on its server storage and the client side security depend on the user itself [4].

The security in ubiquitous computing should be applied by more reliable and suitable method by convenient ways. The strategies used in network are managed by security tools that are based on the functions that repeat among low-level interface to change the values of system variables.

Policy management software manages the whole database of the results generated by these devices and interfaces [10]. The security tools used to manage these tasks are rapidly upgraded to handle new applications and hardware resources otherwise the system becomes hard to manage.

Majority of security policy tools handled low level interfaces so the admin of the system often have no idea of results generated by these management policies.

Enslavement between the items can lead to astonishing results and unwanted behaviour. Moreover, the invention of new security strategies leads to the breakage of security. Such as to identify that the system is inspected by attacker is truly secret. As a result illegal persons could not judge the strategies that is using in these confident situations.

Security in a ubiquitous environment should be assurance of correct and precise working of the essential characteristics. These characteristics are specifically *integrity*, *confidentiality*, *availability*, non-repudiation and authorities [3]. These mechanisms must assure the providence of different parameters such as reliability and robustness that is more important. Limited user interruption confines user validation each instant when the data is accessed due to the interaction between device and building trust mechanisms.

Security mechanism should refuse to accept any attacks. Attacks could be varying as of uncomplicated denial of service to faulty system. The security issues can be determined as network and system security. There are already various protocols, that are used to secure the system from attackers and their attacks, and implemented in different security system architectures and this implementation is still on the way. Another way to implement the security is cryptographic mechanisms that provide security and authentication to users and allow them to access the actual information.

Mark Weiser recommended secure message transfer from one ubiquitous device to another device using cryptographic technique [9]. And this information is stored in system network privately. Michel Collins recommended that when data is being substitute between devices the security of the system should be explored at the design of frameworks itself and the data should be encrypted using some cryptographic technique. These cryptographic techniques are useful for future applications, but encryption techniques are applied within the legacy systems that appear to be more real.

By using such satisfactory secure techniques we can allow the user to access some applications and services without creating new log in identity or restrict the attacker to open the system in any way. This can be accomplished only when we have such a secure and reliable methods to implement security in ubiquitous computing environment. To implement the security in this environment cryptographic techniques can be used because it provides security and authentication for different heterogeneous devices very effectively.

The security issue is resolve by creating a centric data intrusion deduction approach which gathered the user data and mechanism and then apply intrusion detection mechanism on this data. Other approach to resolve this is the verification of data from trusted third party.

We address a solution of security issue that works by ignoring the distance limit, through which devices can communicate at anywhere. The detection of such devices will be done by sensors, which will sense the devices having different operating system, and also their location at the time of connectivity and also provide security during the communication.

VI. RELATED WORK

To secure the communication in ubiquitous computing

Roshan K,Ravi Sandhu [12] explore the challenges to implement models, protocols and architecture for security in ubiquitous computing that uses socio-technical issues as a starting point. In the categories of protocol different challenges are highlighted such as the integration of socio-technical perspectives, security strength and balancing non-intrusiveness, with context awareness .To implement the models for security authentication, access control, privacy and dissemination control challenges are briefly presented .A comparison between the socio-technical view and computing-system view is presented that is the starting point to implement these implementations. Different protocols designs are discussed to realize these models. In multiple personas addressing and security profile protocol the challenges is describe to implement high level persona in ubiquitous environment. Then protocols issues for movement, portative and transparencies of authentication, adaptability or disconnected operations, privacy preservation and scalability

challenges are presented. The security strategies are expressed by abstract models that are provided by security protocols and architecture that go parallel to implement security in ubiquitous computing. The architectural challenges are discussed that providing security infrastructure for ubiquitous computing.

Chan Yeob Yeun[8] proposed an overview of ubiquitous computing, its evaluation, security architecture and protocols that is fast and require less memory resources. The authentication strategies are based on two mechanisms, symmetric key and single sign-on mechanism. The technique securing both application and user authentication in ubiquitous computing. It is provided by authentication, access control and key negotiation. This model and algorithm comprises three stages to secure the ubiquitous network users and applications. The stages consist of validation, access control and key exchanging that provide security in ubiquitous computing. However this technique requires more improvement and further enhancement that addressing the allocation and revocation problems in access rights.

Fan Yang,Qingcong Lv, Qiying[6] proposes a protocol for ubiquitous computing. The protocol consists of both symmetric and asymmetric key algorithm to provide more security in ubiquitous computing. This technology provides data authentication and data freshness also. For wireless communication symmetric key is used and to build security protocol for wire communication asymmetric algorithm is used. In SPUC with base station S,SI there are various rooms and a sensor node A that move from one base station to other base station. A protocol for message freshness and authentication is described that not relying on synchronized clock. In this protocol the session key is acquired by the sensor without observing what is happening in background.

Le Xuan Hung [7] proposed a scheme that integrates MDS, TEA and Diffie-Hellman key agreement protocol to enhance the security service on mobile devices. The scheme is based on Activity authentication manager and active recognition manager. The architecture of security is based on access rights, authentication, key organization, privacy and truthfulness. This architecture is only novel based. Authentication is provided in the form of image to resolve the problems of easily deducing passwords, network intrusive and key-logging. Access control is managed by activity-oriented access control model. By showing samples and implementation it shows that the system that is proposed is correctly working. One drawback of this system is that, how the user activity recognize on the bases of contextual information.

Dong Hu and Hansheng Lao[4] proposes a new technology by implementing a prototype that is based on neural cryptography. This paper describes the security issues, challenges and their requirements in Ubiquitous Computing. Neural cryptographic prototype technology includes the exchange of shared key that are generated by complex physical dynamics method. These shared keys are easily applied on all protocols. The attacker could only listen the communication but not the weight of the partner's that are generated by complex physical process of dynamics. So this is the secure communication to much extent.

Stefan Ransom, Christian Werner [13] proposes the concept and technologies of data-centric security. Data is continuously increasing, both in range and volume. Growing quantity of private data in digital form is exclusively challenging for applying security. It is commonly saved outside the control of user by external companies or websites and for proper data handling users have to trust these companies or websites. Sensitive or confidential data handling like customer information, designs of new technologies is also challenging in organizations and on need this data is shared with other organizations during collaboration or assistance or during the comparison of operations leaving its protected haven.

Now-a-days private data can be easily found by Google search which indicates that security of data is not proper. This leads to the research about the security of data in homogeneous devices in ubiquitous computing. Particularly organizations should pay more attention to security of data.

Large number of devices increases network complexity and with regard to security it difficult to manage on device level. Devices communicate randomly by offering different high level services and this communication leads towards the modification in network structure. This wipes out the traditional network boundaries and decreases the application areas where security is responsible. So achieving security among device communication is very difficult to manage. In IT infrastructure is the real asset is the data not the devices that gather and process it.

Tim Kindberg Hewlett [5] proposes a technique to overcome the issue of limit for communicating devices, for this an impulsive network apply as a replacement of ad-hoc network so that devices can freely cooperate with each other in all environments and being anywhere. When the devices spontaneously interoperate with each other they will enable to share information. The devices connect to the network through some central media, which will act as a server (but no actually a server). It will help the devices having Android Operating System to freely interact with each other and devices having heterogeneous operating systems to connect with network by doing some additional checks. Central device will detect first location of device and then scan it for any malicious attack; it will let it to communicate with other devices and resources on the network. When the device having different operating system detected by central media, it will acknowledge to connected device via TCP protocol.

The central media's operating system should be capable enough to detect heterogeneous operating system of device, by embedded sensors, and versions of application available on it. This will make device able to upgrade its versions so; it could exchange information with other upgraded devices. Here the important issue is how devices keep their private data secure while interacting with other devices available on network.

The operating system of central media will provide security to devices of open source operating system by performing security checks while interacting with heterogeneous operating systems. Ubiquitous computing makes devices closer to human nature. Their aptitude of making decision according to environment and user mood makes it more attractive for daily life. It made device much portable and

enable to keep more and more information on our finger tips than PCs.

VII. CONCLUSION

With the passage of time, the field of ubiquitous computing has motivated centre-stage. For ubiquitous environment smart systems have produced that embedded into this environment. To produce these smart systems people in fields like human-computer interaction, sensor networks, context-aware computing, and middleware, together with those in the more traditional areas of wireless communications, applications, artificial intelligence and so on, have now worked together to produce these smart systems. The evolution of ubiquitous computing has enabled the interaction of heterogonous devices, networks and operating systems to communicate .This dynamic heterogonous and distributed environment has increased the new security challenges. This paper has described the evaluation, history and design goals of Ubiquitous computing environment and also discussed the issues of security when heterogeneous devices communicate in this environment. We have also discussed the different existing technologies and challenges facing the development of models, protocols and architectures that provide security and privacy in the world of Ubiquitous computing. However, these security protocols, models and schemes have required further improvements and enhancements. By observing existing technologies we concluded that future work should be done on techniques to merge the ubiquitous devices, small communicating devices with low computing and battery power, to the infrastructure network. We have addressed a solution of security issue, which is to ignoring the distance limitation and using sensor with neural cryptography two resolve this.

REFERENCES

[1]. Prof. Ashok Agrawala, "Ubiquitous Computing", CMSC 818Z, Fall 2003.

[2]. Mika Raento, Antti Oulasvirta, Renaud Petit, and Hannu Toivonen "ContextPhone: A Prototyping Plateform for Context-Aware Mobile applications" University of Helsinki and Helsinki Institute for Information Technology 2005 IEEE.

[3]. Frank Stajano, "Security Issues in Ubiquitous Computing", University of Cambridge Computer Laboratory, Cambridge, United Kingdom.

[4]. Dong Hu, Hansheng Lao, "Privacy Research on Ubicomp Computing with Neural Cryptography", The 3rd International Conference on Grid and Pervasive Computing – Workshops, pp. 978-0-7695-3177-9/08.

[5]. "System Software for Ubiquitous Computing" Tim Kindberg Hewlett-Packard Laboratories Armando Fox Stanford University 2002 IEEE S. Usha, "A secure triple level encryption method using cryptography and steganography", International Conference on Computer and Network Technology, Vol. 2, pp. 1017-1020, 2011.

[6]. Fan Yang, Qingcong Lv, Qiying Cao, "SPUC: Security Protocol for Ubiquitous Computing", 2007 International Conference on Computational Intelligence and Security Workshops, pp. 0-7695-3073-7/07

[7]. Le Xuan Hung, Hassan J, Riaz A.S , S.M.K. Raazi, Y. Weiwei, NT Canh, P.T.H. Truc, Sungyoung Lee, Heejo Lee, Yuseung Son, Miguel Fernandes, Miso (Hyoung-IL) Kim, Yonil Zhung, "Activity-based Security Scheme for Ubiquitous Environments", pp. 978-1-4244-3367-4/08

[8]. Eng Keong Lua and Jon Crowcroft, "Security for Emerging Ubiquitous Networks", pp. 0-7803-9152-7/05

[9]. Weiser M, The Computer for the 21st Century. Scientific American. (1991) 94-100.

[10]. Kevin Eustice, Amir Mohsen Jourabchi, Jason Stoops, and Peter Reiher "Improving User Satisfaction in a Ubiquitous Computing Application" pp. 978-0-7695-3393-3/08

[11]. Yong Liu, "Towards an Open Ubiquitous Computing Environment" pp.978-1-4244-3304-9/09

[12]. Roshan K. Thomas and Ravi Sandhu," Models, Protocols, and Architectures for Secure Pervasive Computing:Challenges and Research Directions", Proceedings of the Second IEEE Annual Conference on Pervasive Computing and Communications Workshops (PERCOMW'04) 0-7695-2106-1/04 ,2004 IEEE

[13]. Stefan Ransom and Christian Werner, "Towards Data-Centric Security in Ubiquitous Computing Environments", 20th International Workshop on Database and Expert Systems Application

[14]. Shankar R. Ponnekanti, Brian Lee, Armando Fox "ICrafter : A service Framework for ubiquitous Computing Environments" Pat Hanrahan, and Terry Winograd Stanford University, 2001.

[15]. Zohaib Sibte Hassan "Ubiquitous Computing and Android" National University of Computer and Emerging Sciences, Lahore, Pakistan.2008 IEEE.