ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645
Indian Journal of Science and Technology, *Vol 10(25), DOI: 10.17485/ijst/2017/v10i25/112401, July 2017*

Secure Communication Architecture for Privacy and Authentication in Ubiquitous Computing

Nitin Jain[1]*, Kirti Walia[1] and S. N. Panda[2]

[1]I. K. Gujral Punjab Technical University, Jalandhar – 144603, Punjab, India;
nitinjain15@rediffmail.com, kirti_walia@rediffmail.com
[2]Chitkara University, Patiala – 140401, Punjab, India;
panda.india@gmail.com

Abstract

Objectives: To change the conventional safety mechanism for the omnipresent condition. The security strategies must change with respect to the change in a specific situation. Thus, security approaches must be powerful as well as dynamic. **Method**: Framework of a ubiquitous computing environment consists of devices in all forms; sensors everywhere seamlessly associated to wireless networks to offer computing / communication services to the user. In this study, we have proposed an architecture that preserves the user's privacy and authenticates the devices for secure communication between the devices and service providers. **Findings**: The secure architecture discussed in this research paper uses a unique pass-key exchange with a token combination during the data exchange to protect user privacy. This mechanism not only protects the user privacy but also authenticates the user. **Application**: This architecture can be used anywhere in the ubiquitous environment for security enhancement.

Keywords: Authentication, Privacy, Secure Architecture, Secure Communication, Ubiquitous Computing

1. Introduction

The word Ubiquitous means being everywhere meanwhile – certain. This might be translated as "PCs Everywhere"[1]. Intend of ubiquitous is to bolster the clients in their everyday lives by making administrations accessible to the clients whenever, in any system and anyplace. Users trade information between themselves or with the service providers. These communications must be made safe in spite of the context in which the gadget is utilized to get to the administrations. The possibility of ubiquitous computing is making various enlisting gadgets available all through the physical environment to support predictable participation with the environment and additionally accessible resources by making these computing devices imperceptible to the user. Correspondence between devices is blended into environment without redirecting customers. Ubiquitous Computing joins context and situational information to offer administrations to the user. For secure correspondence environment A6 which are[2] Anytime, Anywhere, Any framework, Anyone, Any affiliation must be master.

Honestly, security in this kind of condition requires more complement than what has been seen in conventional frameworks. The ubiquitous frameworks environment makes new troubles in security and requires change of better approaches to manage location both existing and new security issues. Heterogeneous systems

*Author for correspondence

administration circumstances add unusualness to existing security instruments, and diverse procedures ought to be created to ensure perfect levels of security in the ubiquitous networking environment. In the event that this computing environment does not join proper validation component, then this may prompt genuine security and privacy[3] dangers. Mark Weiser generally called father of ubiquitous computing formally recognized security as one of its most noteworthy troubles. With across the board utilization of wireless network, we must be careful in securing our own data and our own systems get to. The course of action of ubiquitous processing advancement will make it difficult to isolate amidst private and public activities and can significantly influence the level of privacy overjoyed in by the clients.

With the present case in point toward networking, compromise of one PC on a network can consistently impact endless machines related with the network. The underlying move toward securing a PC structure is the ability to affirm the identity of users. The system of affirming a customer's identity is ordinarily suggested as client authentication. A key essential of any safe system is the approval of a legitimate user to the system. Access control[4] is put into play entirely when the customer is approved.

Various authentication protocols have been presented in the recent past. Some of their attributes should be enhanced so as to suit this computing environment. [5] is of the opinion that security and privacy are the greatest difficulties to Weiser's visualization of computing. [6] used information disguising thought of TCP/IP packs. This procedure can be used only for dependable verification of fire walls like security gadgets. The information whether fragile or non-delicate will be en-capsulated. By virtue of this reason computational and transmission overhead will be high in this strategy. [7] arranged single, twofold and triple verification methods. This procedure gives strong barrier moreover; it gives more sensible to use OTP's generally customary passwords. Their plan is not reasonable for portable environments. [8] introduced a cloud confirmation system. Makers utilize customers' prior behavioral data planned for confirmation. The issue is that this plan is not bolstered for a wide range of gadgets. [9] prescribed lightweight verification protocol for convenient movable cloud setting. This strategy spares bandwidth, as well as gives low latency. Significant restriction of this plan is that it devours additional time particularly in wireless interchanges.[10] propose a key agreement proposal, in which the customer is required to enroll just once and can be affirmed with no enlistment center. This framework because of its low calculation and correspondence overhead can be utilized as a part of ubiquitous situations[11].

2. Proposed Security Architecture

The proposed architecture for secure communication shown in Figure 1 consists of client devices, dynamic database, context collector and Authentication Module (AM). It is assumed in the proposed model that all the services / providers have been authenticated and registered themselves with Authentication Module Service providers after authentication and registration are given unique ID's which are stored in Super Administrator. Detailed explanation of various components of proposed architecture is as under.

(i) Dynamic Database: When the user / client requires any service, it initiates its device for that service. Service discovery protocol finds out all the services available at that point of time and are put in the dynamic database with their respective ID's. This database contains ID's and service info for all the services available at any instant. On finding its appropriate service, user sends the request to the service ID shown by dynamic database along with its own ID and device generated nonce. As soon as the user chooses service ID from the dynamic database, a similar service request is sent by the database to the

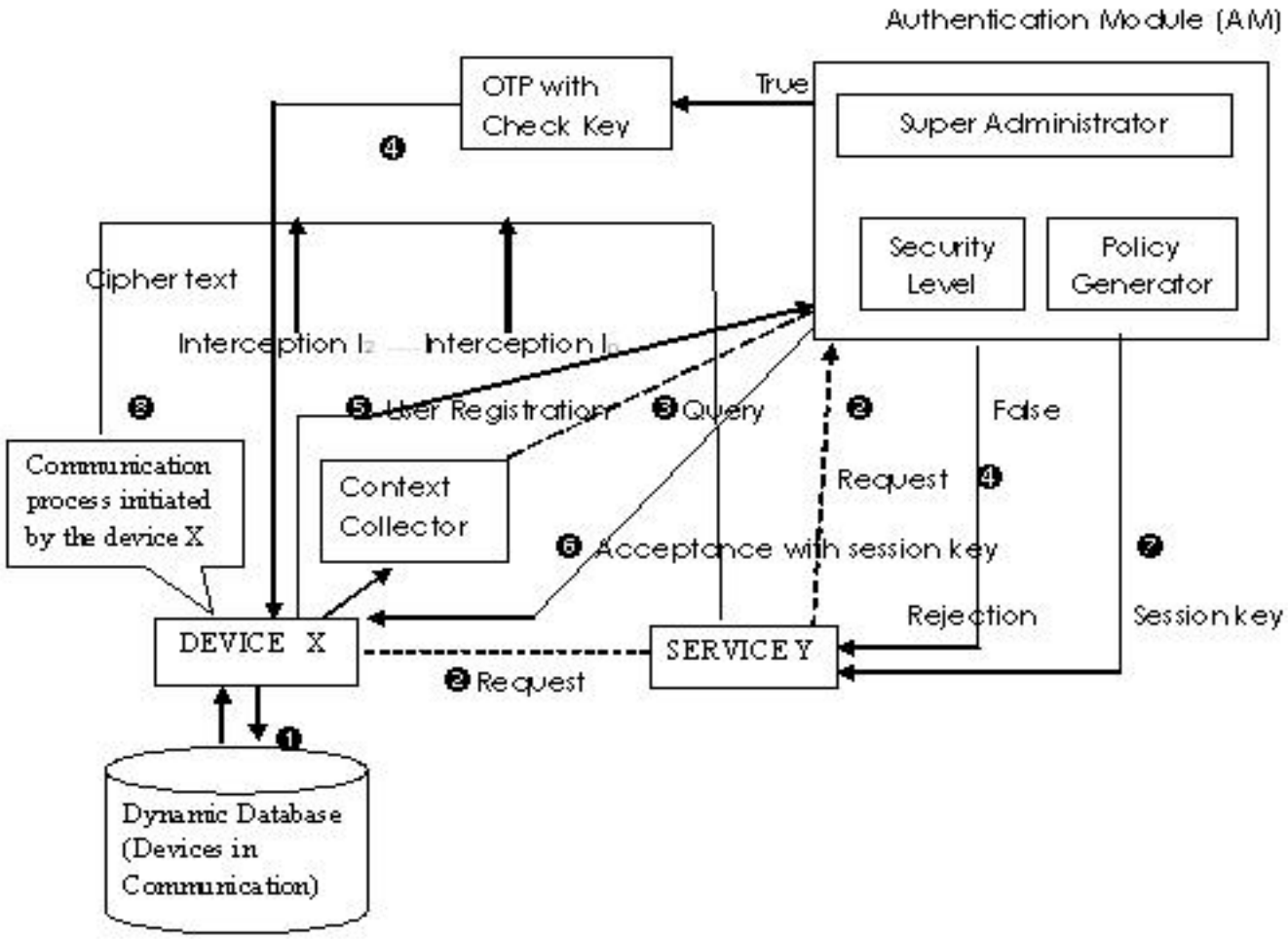

Figure 1. Proposed security architecture.

Authentication Module, which is not known to the user and the service.

(ii) Context Collector: Context and activity data which is generated by the devices (user) as a part of their use is collected by Context Collector. Authentication Module obtains a report from context collector by querying about the device. During operation, client devices periodically report to the Context Collector, and the user behavior will be tracked with the help of this data which further helps in authentication decisions. In order to protect user privacy, all collected data hashed by means of a random key at the point in time of compilation or gathering. The said key is gadget particular, which is produced and put away on the gadget, never sent out.

(iii) Authentication Module (AM): This module takes the authentication decisions. The authentication Service is a cloud service. Only the users authenticated by this module will go through user registration process and after that the secure communication between user → services takes place. AM have three sub systems namely: Super Administrator, Security Level, and Policy Generator. All the ID's, keys and nonce are stored and maintained by super administrator. Security level determines in what manner validation procedure will happen. Its setting depends on the policy rule offered by service providers to the authentication module. Proposed architecture presently has three security levels[11].

Low: AM permit access right away.

Medium: AM have to also check with a nearby authenticated device for requesting device credentials.

High: AM have to also verify with additional extra close by authenticated gadgets for requesting device testimonial.

Policy Generator sub system uploads modifies and monitors the policies given by the service providers for their services. The policy supports rules like specification of second user verification strategy, least operating system edition, suitable network settings etc. For each access request, Authentication Module retrieves the corresponding provided-policy and extracts the information collected based on the policy. Then authentication rule is applied to determine the authentication result.

2.1 Algorithmic Approach

1. Device X finds the appropriate service available with the help of dynamic database. //Service Discovery
2. X sends a request to Y (service) using its device ID and nonce D.Y redirects request with its nonce S to AM. //Access Request.
3. AM sends a request to context collector for X.// Enquiry for X
4. If report negative AM sends Y not give access to X. Else AM sends X [OTP with Check key CK] encrypted in A1 (nonce of AM). All message encrypted with D. //Authentication
5. X sends [userid, OPT with CK, Pass Key (PK)and Token T] all encrypted using public key of AM. // User Registration.
6. AM after decryption stores PK, T and sends X [registration acknowledgment, temp id, session key (K)] encrypted with D. // X Registered
7. AM sends Y {[temp id, PK-T]X, K} encrypted with S. // X authenticated to Y by AM.
8. X and Y starts packet exchange encrypted and decrypted using K.

When the device X initiates the communication, the service discovery protocol discovers all the services available at that instant of time. All available services are put into the dynamic database and the device X requests the permission to access the required service by sending its ID and device generated nonce. When service provider receives the request, it retransmits the demand to authentication module by its own nonce alongside the demand points of interest. Authentication module recovers policy for the access demand from policy generator and pull out the data that should be gathered. A query to context collector about device is sent by AM. Context collector generates a report upon receiving the inquiry and sends the same to the authentication module. AM binds verification rule given in provided policy to determine authentication outcome. If outcome is false, then AM sends a rejection message to the service provider. When the authentication result is true, authentication module informs the user to register with AM using One Time Password (OTP) with Check Key (CK) encrypted by nonce of AM; all encrypted using the nonce of the user. Now the user sends a message containing User ID, OTP with CK, Pass Key (PK) and a token T. Public key of AM is used for the encryption

of message. AM decrypting it using its private key and stores the pass key (PK) in its database. Register the user as well as set the security level for the client device with respect to the requesting service. Authentication Module sends a user registration acknowledgment, a TempID, a session key (K) everything encrypted using user's nonce. Authentication module also sends to the requesting service provider TempID, PK and token T of client device, session key (K) all encrypted by the nonce of the requesting service provider. Both the users will be using this one-time session key (K) for encryption and decryption of the messages exchanged between them. Session keys should be time bound and must expired by its own after that time period. The concept of Pass Key with token has been used to provide an extra security feature.

3. Security Assessment of Proposed Architecture

During the service discovery if some intruder acts as a service provider and where device sends an access request to fake service provider from dynamic database. That service provider does not redirect the service request to AM for authentication since the provider is fake but cannot communicate with the device because a similar service request is sent by the dynamic database to the Authentication Module with the credentials of requesting user. AM on getting the request, search the ID of service provider as all service providers has got registered with AM. When ID of service provider does not match with any stored ID's, AM sends warning to the user about fake service provider. During the connection establishment between the two users, the attacker will fail to cause any harm because the attacker would not able to decrypt the message encrypted by nonce as the attacker does not have the related private key for the nonce. When the actual communication between the device and service provider takes place, the users will cross-check corresponding Pass Key with token (PK-T) to check changes in pass key with token combination. If altered, it is confirmed that an intruder is there in the network. Intruder can only forward the packet, but will not be able to know its contents. The alterations due to intrusion will be reflected through PK-T combination. Hence the attacker will fail to cause any harm.

4. Conclusion

Secure ubiquitous communication environment for persevering user privacy and authentication is very important where users work from anywhere, anytime using any network with any mobile devices. The secure architecture discussed in this research paper uses a unique pass-key exchange with a token combination during the data exchange to protect user privacy. Further a step forward this technique authenticates the user too.

5. References

1. Mark W. The computer for the 21st century. Scientific American. 1991 Sep; 265(3):94–104. CrossRef.
2. Jain N, Panda SN, Kumar A. Future scintillation of ubiquitous computing. International Journal of Computing and Business Research. 2012 Sep; 3:1–15.
3. Campbell RE. Towards security and privacy for pervasive computing. Software Security—Theories and Systems, Springer Berlin Heidelberg; 2003. p. 1–15. CrossRef.
4. BoFu FD. User centric trust based access control management for ubiquitous computing environments. IEEE Network Operations and Management Symposium Workshops; 2008. p. 265–74
5. Kumar R. Pervasive computing. A safe walk in the woods? Survey paper [Internet]. 2002. Available from: http://www.cs.umn.edu/~richa/reports/PC. ps.
6. Liu WF. Information hiding for pervasive trusted authentication. Proceedings of IEEE Pervasive Computing Joint Conferences, (JCPC); 2009. p. 653–6.
7. Corella F, Lewison K. Strong and convenient multifactor authentication on mobile devices. 2012 Sep; 2(7):12–18.

8. Chaw R, Jakobsson M, Masuoka R, Molina J, Niu Y, Shi E. Authentication in the clouds: A framework and its application to mobile users. CCSW, ACM. 2012 Oct; 63(2):352–8.
9. Zadeh MB. Keystroke dynamic authentication in mobile cloud computing. International Journal of Computer Applications. 2014 Mar; 90(1):35–9.
10. Chang CC. A multipurpose key agreement scheme in ubiquitous computing environments. Mobile Information Systems. Hindawi Publishing Corporation. 2015; 2015.
11. Jalil KA, Rahman QBA. Authenticating devices in ubiquitous computing environment. International Journal of Cyber-Security and Digital Forensics. 2012; 1(2):75–81.