International Journal of Applied Engineering Research
ISSN 0973-4562 Volume 10, Number 3 (2015) pp. 7797-7805

http://www.ripublication.com

# Robust Security For Mobile and Pervasive Computing

**Swetha Chandra Karroti[1], Poojitha Mandava[2], Ajay Varma Nandyala[3], Hasitha Nekkalapu[4]**

[1] *K L University, Guntur Dist, Andhra Pradesh,*
[2] *K L University, Guntur Dist, Andhra Pradesh,*
[3] *K L University, Guntur Dist, Andhra Pradesh*
[4] *K L University, Guntur Dist, Andhra Pradesh*

## Abstract

In a Protection and security are two vital however apparently conflicting goals in a pervasive computing environment (PCE). From one perspective, administration suppliers need to verify true blue clients and verify they are getting to their approved administrations in a legitimate manner. Then again, clients need to keep up vital security without being found for wherever they are and whatever they are doing. In this paper we propose a novel security saving validation and access control plan to secure the collaborations between portable clients and administrations in PCEs. The proposed plan flawlessly coordinates two hidden cryptographic primitives, blind mark and hash chain, into a very flexible and lightweight verification and key foundation convention. The plan gives unequivocal common confirmation between a client and an administration while permitting the client to secretly connect with the administration. Separated administration access control is likewise empowered in the proposed plan by grouping portable clients into diverse administration bunches. The rightness of the proposed confirmation and key foundation convention is formally verified focused around BAN logic.

**Key terms:** Security, Access Control, Authentication, Pervasive Computing Environments(PCEs).

## Introduction

Pervasive computing environments (PCEs) with their interconnected gadgets and plenteous administrations guarantee incredible reconciliation of advanced framework into numerous parts of our lives, from our physical selves, to homes, offices, lanes et cetera [1], [23]. The immense number of conveying gadgets give consistent access to various elements arranges whenever from any area. As systems administration innovations get to be typical and fundamental to ordinary life, organizations, associations and people are progressively relying upon electronic intends to process

data and give applicable administrations to take preference of encompassing brainpower in PCEs [2], [4], [5], [6], [25].

Conventional confirmation which concentrates on personality verification may neglect to work in PCEs, somewhat in light of the fact that it conflicts with the objective of client protection insurance and incompletely on the grounds that the affirmation attained by substance validation will be of reducing worth [16].

In situations with significant convergence of invisible" processing gadgets assembling and gathering the characters, areas and exchange data of clients, clients ought to rightly be concerned with their protection. In the meantime, the physical effort of pervasive processing makes protecting clients' security a much more difficult assignment [9], [13], [24]. We further clear up the extent of security in PCEs as takes after. Obscurity: The genuine personality of a client ought to never be uncovered from the correspondences traded between the client and a server unless it is purposefully unveiled by the user.

## System Architecture and Cryptographic Primitives

A specimen framework building design of a yard PCE is given in Fig. 1. By and large, a PCE comprises of three sorts of substances:

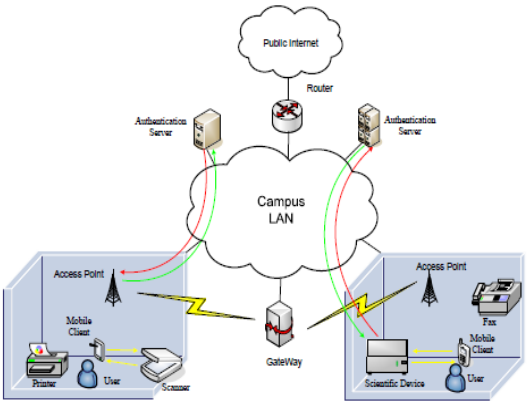


**Figure 1:** A sample pervasive computing environment

Versatile clients, administrations and back end confirmation servers, notwithstanding the fundamental wired and remote correspondence foundations. Note that remote system access is itself an administration.

Client security ought to be ensured from pariahs as well as from system administration suppliers. Our proposed access control plan is intended to secure the communications among these three sorts of substances as demonstrated in Fig. 2. All the more specifically, our plan expects to give unnamed common confirmation between the versatile client and the administration (e.g., remote administration access point for remote system access administration).

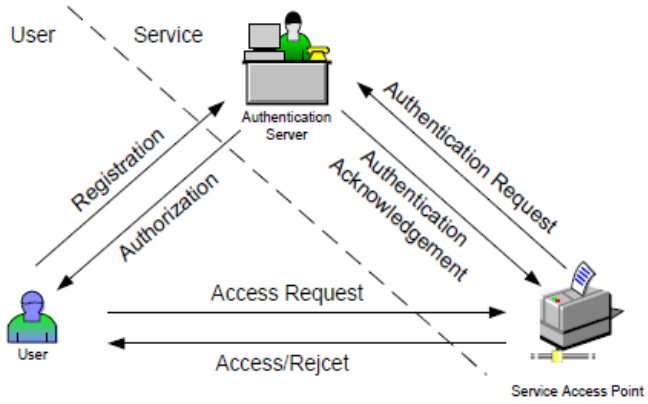


**Figure 2:** System architecture.

**Blind Signature:** Blind mark plan [14] is a variety of advanced mark plot in which the substance of a message is camouflaged from its underwriter. Blind mark plans can be actualized focused around various well known computerized mark plans, for example, RSA [22].

**Hash Chain:** One-way hash capacity h is a compelling but computational efficient cryptographic instrument, which takes a message of subjective size as its enter and yields a fixed series of digits. The "one way" implies that it's computationally infeasible to get the first enter from the yield. By applying h() more than once on a starting worth m, one can acquire a chain of yields hj(m). The idea of a hash chain was first proposed for utilization in a confirmation plot by Lamport [24] [23].

## The Proposed Scheme

This segment displays our privacy preserving confirmation and access control plan. Consider the situation that a versatile client needs to have the capacity to rapidly get to the remote or other accessible administrations in PCEs. Because of the unreliability of the remote correspondence channel, the approval of the versatile client to the specific administration she demands ought to be verified and the consequent data traffic ought to be ensured. In addition, the versatile user ought to have the full control of her setting security.

Upon the fruitful finishing of the shared Verification process, both gatherings will impart new session keys which will be utilized to secure the resulting information traffic of the session. This is carried out through the client operational convention. A question determination convention is additionally intended to tackle conceivable debate that may climb between the versatile clients and administration suppliers. Note that we expect clients are equipped for controlling the source locations of the cordial Medium Access Control (MAC) outlines. This presumption is essential for unknown correspondence generally one can without much of a stretch distinguish a client focused around her interesting MAC address. Point by point procedure on this can be found, for instance, in [17] and is out the extent of this paper.

*User Authorization Protocol:*
The reason for the client validation convention is to secure the security accreditations between portable clients and administration suppliers, which can be utilized as the security stay as a part of the ensuing shared verification forms at whatever point a versatile client endeavors to get to an administration. In our client approval convention, the versatile client and the relating administration need to validate one another first. This is regularly done through some out-of-band non-cryptographic strategy.

The proposed user authorization protocol contains two steps: 1) *credential generation*, and 2) *credential authorization*. The mobile user generates her own specific credentials as shown in Table I.

**Table 1:** Credential Generation.

| Credential Generation: |
|---|
| 1. generate two fresh nonces: $r'_U$ and $r''_U$. |
| 2. sign her own ID with a fresh nonce $r''_U$:$\{U, r''_U\}_{PriK_U}$. |
| 3. compute the anchor value $C^0$ of the credential chain as $C^0 = h(r''_U, U, \{U, r''_U\}_{PriK_U})$, |
| 4. compute the credential chain $C^j = h^j(C^0), j \leq n$, with length $n$. |
| 5. blind $C^n$ as $C_U = \{r'_U\}_{PubK_{SID}} \times C^n$. |

*The User Operational Protocol*
Appreciate various types of administrations she is approved to in PCEs at whenever, from anyplace without uncovering any of her connection data unless she is ready to do so and it is totally essential (e.g., if there should be an occurrence of question). Reasonably, the client operational convention acts as takes after. The versatile client request sends a right to gain entrance demand, which contains an administration access ability claim and an authenticator used to demonstrate her authenticity to the administration asked for, to the administration access point, for example, the remote system access point or a system printer. The authenticator incorporates an approved certification and a new nonce. The administration access point basically advances this right to gain entrance solicitation message to its back end confirmation server for verification.

*Extension for Out-of-Order Requests*
Here and there a versatile client may need to dispatch various sessions all the while. Note that if the different sessions are as for diverse administration sorts, or if the various sessions are of the same administration sort however gone to the verification server in the same request as they were started, the proposed convention can deal with them well.

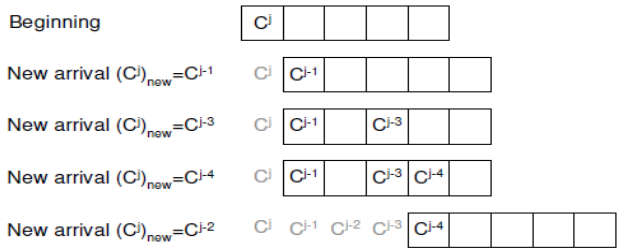


**Figure 3:** An illustration of the sliding window based credential authentication procedure (for k=5)

two values: Cn, used as the index of the hash chain, and Cj , the most recently used hash value. A submitted credential is hashed only once and compared with Cj .

## Correctness Verification of The Proposed Scheme

In this segment, we formally confirm the rightness of the proposed client operational convention, in light of the BAN rationale [11], which is a formal rationale generally used to reason about convictions, encryption, and conventions. In spite of the fact that BAN rationale does have its own particular limits, it is straightforward and has been effectively connected to numerous conventions. Convention rightness implies that, after the convention execution both of the correspondence gatherings determine that they are imparting a new session key and both are certain that the same conviction is held by the other side as well. To dispose of the representation multifaceted nature, we rearrange the two conventions into their non specific sorts. In the accompanying depiction in this area, we utilize the accompanying documentations by tradition: An and B is two substances; *K*ab is the fresh session key shared between A and B; (Ka, Ka inverse) and (Kb, Kb inverse) are the public/private key pairs of entity A and B, respectively; other notation follow those of BAN logic [12].

**Table 2:** Goals of the correctness verification

| **Verification Goals:** | |
|---|---|
| 1. $A \models A \overset{K_{ab}}{\longleftrightarrow} B$ | 2. $B \models A \overset{K_{ab}}{\longleftrightarrow} B$ |
| 3. $A \models B \models A \overset{K_{ab}}{\longleftrightarrow} B$ | 4. $B \models A \models A \overset{K_{ab}}{\longleftrightarrow} B$ |

In the user operational convention, the administration access point and the back end validation server believe the genuineness and trustworthiness of the messages traded between them, on the grounds that a protected correspondence channel is accepted between them. Thusly, without loss of simplification, we rearrange the client operational convention into the accompanying bland sort as demonstrated 8 in Table 3, which is further glorified in the same table.

## Analysis of The Proposed Scheme

### *A. Security Related Properties of the Proposed Scheme*

The proposed scheme exhibits many nice security related properties as discussed below:

**Mutual Authentication**: In the proposed plan, the portable client is verified focused around her approved qualification, as in the administration knows the client is without a doubt lawful and approved. The administration verifies itself to the client through its open key certificate and by demonstrating its information of the relating private key.

**User Context Privacy:** The clients' setting security is generally ensured by the proposed plan, just totally essential data is known to the administration, i.e., clients' administration sort, to give suitable access. Through the visually impaired mark system, the portable clients could be confirmed secretly without revealing whatever other data.

**Non-Linkability**: Ideally, non-linkability implies that, for both insiders (i.e., administration) and untouchables: 1) Neither of them could credit any session to a specific client; 2) Neither of them could connect two separate sessions to the same client [25]. In the proposed plan, perfect non-linkability is accomplished concerning pariahs.

**Data Traffic Protection**: The client operational convention creates crisp session keys to secure the communication information traffic between the portable client and the administration. Information congentility and trustworthiness can be given focused around the symmetric cryptography.

**Differentiated Service Access Control:** By arranging the versatile clients into distinctive administration sorts, separated administration access control is empowered in our plan. Distinctive portable clients are approved in like manner focused around the administration sorts to whom they have a place. Client approval is thusly, fulfilled in a separated manner.

### *B. Performance of the Proposed Scheme*

Despite the number of desirable security properties provided, the proposed scheme is extremely lightweight. We analyze the overheads introduced in this subsection.

**Management Overhead:** The proposed plan includes negligible administration overheads (e.g., human connection). The administration supplier needs to deal with one certificate for every client and the comparing client prole. Because of the elevation property, this number can be significantly lessened to that of the client bunches.

**Storage Overhead:** While the protocol is running, the back end authentication server stores two values (Cj ;Cn) for each currently in-use credential chain and one value (Cn) for each of the used but unexpired chain.

**Communication Overhead:** The client operational convention obliges two-round to fulfill common confirmation and session key foundation between the client and the administration.

**Table 3:** protocol computation overheads comparison

| | | Public Key Oper. | Sig. Veri. | Nonce Gen. | Hash Oper. | Sym. Key Oper. |
|---|---|---|---|---|---|---|
| Ours | U | 1(off-line) | 0 | 1 | 2 | 3 |
| | P | 0 | 0 | 1 | 2 | 3 |
| | S | 1(online) | 1/n | 0 | 0 | 0 |
| [21] | U | 1(off-line) | 0 | 0 | 1 | 1 |
| | P | 0 | 1(online) | 0 | 1 | 1 |
| | S | 1(online) | 1(online) | 0 | 1 | 1 |

The service access point is completely exempted from performing public key operations. We compare in Table 3 the computation overhead of the proposed scheme with the scheme proposed in [18].

## Related Work

Recently, quite a few papers have been published to address the new security and privacy challenges in PCEs [7], [8], [9], [10], [13], [16], [18], [19], [20], [21], [22], [24], [25]. However, most of these results fall in the scope of establishing general security framework and identifying general security Requirements, without providing concrete security protocols. Some of these efforts focused on designing specific security infrastructures to protect user context privacy like location information from service providers. The MIST system [7], [8] provides user anonymity through an overlay network assuming the existence of a *Lighthouse*, which keeps all information of all the users. In addition, performance degradation is unavoidable for systems that utilize MIX-network style approach [12]. A proxy-based scheme can be found in [10].

This general scheme allows users to interact with different services anonymously, using pseudonyms. Pseudonyms cannot be linked, but are formed in such a way that a user can prove to one service about his relationship with another using a .statement. Such a statement is called a credential. An in-depth description and analysis of different pseudonym systems can be found in [28]. In order to avoid leakage of user's MAC address or IP address at the lower levels, Gruteser *et al.* [20]

## Conclusion

In this paper, we proposed a privacy preserving authentication and access control scheme to secure interactions between mobile users and services in PCEs. On the one side, the proposed scheme provides explicit mutual authentication between a mobile user and a service; on the other side, it allows the mobile user to anonymously interact with the service. Hence, the proposed scheme successfully satisfies concerns of both parties- security and privacy. The scheme integrates two cryptographic primitives, blind signature and hash chain, into a highly flexible and lightweight authentication and session key establishment protocol. Differentiated service access control is also enabled in the proposed scheme by classifying mobile users into different service types.

## References:


1. Easy Living., Microsoft Research, http://research.microsoft.com/easyliving/.
2. GAIA - Active Spaces for Ubiquitous Computing., University of Illinois at Urbana-Champaign, http://choices.cs.uiuc.edu/gaia/
3. Location Privacy Protection Act and other privacy related law, http://www.techlawjournal.com/cong107/Privacy.
4. MIT Project Oxygen., http://oxygen.lcs.mit.edu/.
5. National Institute of Standards and Technology (NIST),.Pervasive Computing SmartSpace Laboratory., http://www.nist.gov/ smartspace/
6. The Aware Home., Georgia Institute of Technology, http://www. cc.gatech.edu/fce/ahri/.
7. J. Al-Muhtadi, R. Campbell, A. Kapadia, D. Mickunas, and S. Yi, .Routing Through the Mist: Privacy Preserving Communication in Ubiquitous Computing ICDCS 2002, Vienna, Austria, 2002.
8. J. Al-Muhtadi, R. Campbell, A. Kapadia, D. Mickunas, and S. Yi, .Routing through the Mist: Design and Implementation,. UIUCDCS-R- 2002-2267, March 2002.
9. J. Al-Muhtadi, A. Ranganathan, R. Campbell and M. Mickunas, .Cerberus: A Context-Aware Security Scheme for Smart Spaces., PerCom 2003, 489.
10. M. Burnside, *et al.*, .Proxy-based Security protocols in Networked Mobile Devices., ACM SAC 2002, Madrid, Spain, 2002.
11. M. Burrows, M. Abadi and R. Needham, .A logic of authentication.,Proceedings of the Royal Society of London A, 426:233-271, 1989.
12. J. Camenisch and A. Lysyanskaya, .Ef_cient Non-transferable Anonymous Multi-show Credential System with Optional Anonymity Revocation ., In Advances in Cryptology, EUROCRYPT 2001, LNCS 2045, pp. 93-118.
13. R. Campbell, J. Al-Muhtadi, P. Naldurg, G. Sampemane and M. Mickunas: .Towards Security and Privacy for Pervasive Computing., ISSS 2002: 1-15.
14. D. Chaum, .Blind Signatures for Untraceable Payments., Advances in Cryptology Proceedings of Crypto 82, D. Chaum, R.L. Rivest, & A.T. Sherman (Eds.), Plenum, pp. 199-203, 1982.
15. D. Chaum, .Security without identi_cation: transaction systems to make Big Brother obsolete., Communications of the ACM, 28(10), 1985.
16. S. Creese, M. Goldsmith, B. Roscoe, and I. Zakiuddin, .Authentication for Pervasive Computing., In Security in Pervasive Computing 2003, LNCS 2802, pp. 116-129, 2004.

17. M. Gruteser and D. Grunwald, .Enhancing Location Privacy in Wireless LAN through Disposable Interface Identi_ers: A Quantitiative Analysis, WMASH'03, San Diego, USA, 2003
18. Q. He, *et al.*, .The Quest for personal control over mobile location privacy., IEEE Communications Magzine, pp.130-136, May 2004.
19. U. Jendricke, M. Kreutzer, and A. Zugenmaier, .Pervasive Privacy with Identity Management., The 1st Workshop on Security, UbiComp 2002.
20. U. Jendricke, M. Kreutzer and A. Zugenmaier, .Mobile Identity Management., The 1st Security Workshop, UBICOMP 2002, Sep. 2002.
21. M. Langheinrich, .A Privacy Awareness System for Ubiquitous Computing Environments., UbiComp 2002, Springer-Verlag, LNCS 2498, pp.237-245, 2002.
22. K. Nakanishi, J. Nakazawa and H. Tokuda,.LEXP: Preserving User Privacy and Certifying Location Information., The 2nd Workshop on Security (Ubicomp2003), 2003.
23. A. Weimerskirch and D. Westhoff, .Zero common-knowledge authentication for pervasive networks., In Proceedings of Selected Areas of Cryprotgraphy 2003 (SAC 2003), 2003.
24. M. Wu and A. Friday, .Integrating Privacy Enhancing Services in Ubiquitous Computing Environments., Workshop on Security in Ubiquitous Computing, 4th International UBICOMP, 2002.
25. A. Zugenmaier, A. Hohl, .Anonymity for Users of Ubiquitous Computing ., Security Workshop, UbiComp 2003, Seattle, October 2003.