A Secured and Efficient Biometric Cryptographic Authentication in Pervasive Computing

K.Swetha, P.S.A.Pavan Kumar Reddy, S.Maneesha Durga, A.V.Gautham

Abstract- In pervasive computing environments, clients can get benefits anytime and anywhere, but the inescapability and versatility of the circumstances bring present day security challenges. The client did know about the service provider and vice versa. They have to authenticate each other before starting the service. The cloud has to identify or authenticate the client or user by his/her identity i.e, fingerprint. Here the two important things that we can consider were about privacy and security. In this case, the client should not expose any private information to the cloud such as his physical location, ID and so on when being authenticated. In this paper, we provided a authentication scheme based on biometric encryption to enclose the data transferring between a client and cloud. In this proposal, client's authentication was hidden.

Keywords- Privacy, Security, Biometric encryption, Pervasive Computing, RSA, RSA cryptography, Biometry and Cryptography

I. INTRODUCTION

Computer technology increasingly advances and it come into everyone's lives more and more as they perform better and we can do several tasks faster with them. Day by day as a result of computing devices becomes increasingly smaller, tiny and powerful, the embedded technology leads the role. The aim is to meet the claim of "anywhere, always, everywhere" for data processing and communication through the ubiquity of information and communication technologies. Towards Mark Weiser's vision [1][2][7][8][22], pervasive computing is the next generation of computing environments with information and communication technology anywhere, anytime for all. Inescapable processing is the up and coming age of figuring conditions with data and correspondence innovation anyplace, whenever for all. Inescapable registering proposes the attestation of rearranging day by day life by incorporating cell phones and advanced foundations into our genuine. With the assistance of a few sensors and implanted gadgets, dynamic spaces can naturally be joined to clients' inclinations and can catch and use setting data. Once in a while, this component could undermine the security of clients thoroughly and raise the issues of data abuse. For instance, this component can be abused by interlopers, programmers, vindictive clients of insiders, now and then framework executives to string clients. Undoubtedly users privacy is much difficult task in pervasive environment. Unavoidable registering innovation will encompass clients with a mollified and helpful data condition that consolidates physical and figuring gadgets into a coordinated situation. This component will upsurge the profitability and connection. Setting mindfulness will enable this condition to assume on the liability of serving clients, with consolidated exercises as per the idea of the physical space. The stated setting is called as "active space", [7][8][11] in which, users can relate with number of applications which may follow the user orders, and control the numerous flexible applications that may obey the user, define and control the active space. An unavoidable registering condition unexceptionally and straightforwardly bolsters the people with its continuous calculation and correspondence [7]. This calculation control ensures straightforward communication of the gadgets with the clients [8][2]. In unavoidable figuring condition, control over gathering and spread of data is seen through benefit of clients, which is thus called as protection in PCE and these clients can be sorted as people, gatherings, or associations. Ordinarily, the fundamental security instrument includes static system or shut framework with the focal control, though the Pervasive processing situations shared interchanges are startling and are dynam ically dynamic. The correspondence channel will be built up between a client and a specialist organization. Hence, before to the entrance of administrations, a shared assention amongst clients and specialist organizations ought to be built up. Increment in area based applications guarding individual area data has turned into a preeminent test. With a specific end goal to determine this issue, an arrangement of systems and rules are required which ought to enable clients to control their area data typically. With the primary worry about protection and security in unavoidable registering conditions, adequate research has been sorted out focusing on different angles [3].

Manuscript published on 28 February 2018.
***** Correspondence Author (s)

K.Swetha*, Computer Science, Koneru Lakshmaiah Education Foundation, Guntur, India, Email: swetha.k@kluniversity.in

P.S.A.Pavan Kumar Reddy, Computer Science, Koneru Lakshmaiah Education Foundation, Guntur, India, Email: *p.akhilreddy1289@gmail.com*

S.Maneesha Durga, Computer Science, Koneru Lakshmaiah Education Foundation, Guntur, India, *maneeshadurga8@gmail.com*

A.V.Gautham, Computer Science, Koneru Lakshmaiah Education Foundation,Guntur,India, *avenkatagautham@gmail.com*

II. PRIVACY IN PERVASIVE COMPUTING ENVIRONMENTS

Privacy in Pervasive Computing is a major issue. Numerous models have been proposed and come up with several solutions to address privacy challenges. The successful project proposal needs the desires and consciousness of the users' requirements.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)
© Copyright: All rights reserved.

The tedious and problematic proposals of pervasive environments are embedded or they are unseen. In inescapable figuring conditions, the 'imperceptible' processing gadgets are progressively assembling individual information and determining client setting, the client will be worried about their protection and security. Gadgets may uncover and trade individual and touchy data, (for example, character, part, inclinations, qualifications, and so forth) with the keen questions in unavoidable frameworks. Privacy in pervasive environment will be a major issue, when the devices cannot belong to a one trusted domain. It is a basic circumstance to create and make protection touchy administrations in inescapable registering frameworks to expand the genuine advantage of these advances and lessening conceivable and real dangers. Since these frameworks accumulate a lot of individual touchy data, (for example, email id, shopping history, area, and so forth.) and demonstrating individuals' unimportant enthusiasm for taking an interest inescapable conditions. Henceforth, in order to maintain privacy at all times, it has become mandatory to design proper procedures and guidelines. Protection can be very much characterized, as indicated by Steffen et al. [4], as "An element's capacity to control the accessibility and presentation of data about itself". In [5], the creators recognize five essential key highlights which make these frameworks altogether different from the present information gathering frameworks [3].They are:

1. Innovative and State-of-the-art computing technologies will be presented in active space.
2. Information gathering will be imperceptible and unnoticeable;
3. The assembled information will be more cordial than any time in recent memory;
4. The central motivation driving the data collecting;
5. The fundamental interconnectivity for keen gadgets to collaborate for giving administration to clients;

A. *Anonymity*

The genuine personality of the client ought to never be unveiled from the correspondences traded between the client and a server unless it is purposely uncovered by the client. So as to examine the mystery instruments as to gadget adaptability, the creator, Zugenmaier et al. [6] proposed a new attacker model, “Freiburg Privacy Diamond Model (FPD)”.

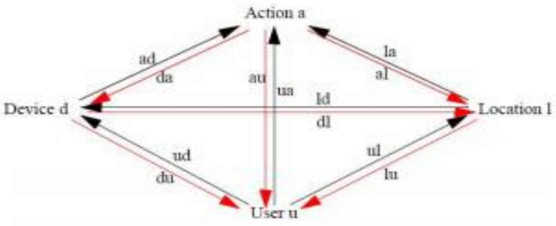

Figure1. Sample Privacy Model [9]

The sample privacy model will perform four types of entities to distinguish information about secrecy, that are - the performed action ‘a’, the device ‘d’ used for performing the action, the user ‘u’ that performs the action and the location ‘l’ of the device, as depicted in Figure 1. The authors are clearly described the relationship of each entities, and the attacker familiarization with the existing relationship to break the secrecy/anonymity.

B. *Confidentiality and Integrity*

Classification alludes to the need of keeping data secure and secret. Honesty alludes to the idea of shielding data from being improperly altered by unapproved clients.

C. *Unobtrusive*

The primary point of unavoidable figuring is to be mysterious and unpretentious. The registering innovation is implanted into ordinary savvy protests that convey data. This idea of inserting lessens the perceivability of the unavoidable registering condition and makes the innovation all the more cordial and satisfactory to the client. Thusly, a similar trademark will attack the protection of the client without the client acknowledging it.

D. *Location Dependency*

The Pervasive computing technologies make use of location information such as traffic reports, navigation maps, news, locating nearest restaurants, nearest clinics, etc. [12]. The users have to provide this information to the service provider.

E. *Context Dependency*

The Pervasive computing tools are dependent on context information, such as the type of wireless device used, user profiles, user preferences, current time, GPS coordinates etc. [13] [23]. Protecting context information is a tedious task, as they deal with different sets of information with context aware systems.

F. *Data Collection*

An inescapable registering application depends on a huge sum, quality, and exactness of information produced and gathered. Also most of the pervasive computing technologies include wireless devices and these devices are limited to processing power, throughput, bandwidth, memory etc [14].

G. *The Service Provider*

Maintaining the privacy of data is very crucial for service provider. Chances and vulnerabilities for misuse of data is more. As a general rule, its hard to guarantee that all the specialist organizations take after the principles. The creator, Langheinrich [15] estimated, outlining an ideal instrument for ensuring protection would be difficult to accomplish. Consequently, the creator proposed a framework, for cautioning clients about their security. The proposed framework relies upon social and lawful standards of genuine living, as opposed to outlining a framework to ask and regard the clients' protection. The distributer named the framework as, the security mindfulness framework (pawS), which enables information authorities to process individual information, touchy information and association strategies, and information control instruments, for example, including, erasing and changing data.

The created pawS engineering comprises of two principle parts: protection intermediaries and a security mindful database.

III. SYSTEM ARCHITECTURE

Biometric cryptographic verification with RSA calculation is utilized to confirm in our plan. This approach is different from the existing conventional approaches. In this approach we integrate the techniques of cryptography and biometrics effectively for maintaining privacy and secrecy of the data.

2.1. Biometry and Cryptography

Many researchers have studied and proposed the interface between two corresponding technologies, biometrics and cryptography. Biometrics is about determining unique personal features, such as a face recognition, voice recognition, fingerprint, signature, hand geometry, or iris. The general Biometric system [16][21] is described in Figure 2. As illustrated in the picture, its authentication has to be transparent and trusted. The significant focal points of biometrics are uniqueness, and need not to recall passwords. Biometrics is the thing that you have, and it can't be stolen or overlooked.

The Biometric technique is shown in Figure 2.

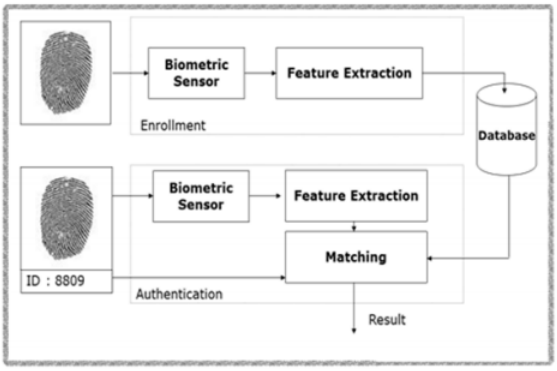

Figure 2 Biometric System

IV. THE PROPOSED SYSTEM

We proposed system which aims to provide mutual authentication between user and Pervasive computation devices. The scheme integrates Biometric Encryption and RSA key exchange algorithm for authentication and key generation. The scheme holds most of the security properties, such as anonymity, confidentiality etc. system uses the RSA algorithm for key generation. The arrangement inserts biometric data on the private/open keys age process. Additionally the comparing private key relies upon biometric highlights and it can be produced when it is required. Beginning from the unique mark obtaining, and all the behavioural biometric highlights, the biometric identifier is removed, cyphered.

V. RSA ALGORITHM

The cryptographic algorithm was introduced by (RSA) Ron Rivest, Adi Shamir, and Leonard Adleman, in 1978. RSA algorithm implements on a public key cryptosystem, and digital signatures. Basically, RSA is inspired by the published work of “Whitfield Diffie” and “Martin Hellman” for quite a long ago, they introduced new method of distributing cryptographic keys, and it was known as Diffie–Hellman key exchange. RSA algorithm implemented two key concepts:

A. *Public key encryption*

This encryption mechanism introduces the concept of involving two keys - one for encrypting, and the other for decrypting; only the user with proper decryption key can decrypt and encrypt the message, since in RSA encryption keys are open, and decryption keys are private. The generated keys must have a property of non-repudiation and cannot be easily assumed from the open encryption key. The keys are to be transmitted to recipients over a secure channel.

B. *Digital signatures*

It is a mathematical scheme for authenticating a message or documents. The received message to be verified by the user, whether the transmitted message is generated by the sender. A valid digital signature provided the originality of the message transmitted by sender and provided authenticity that the message was not modified during the transmission. Normally this technique is used to implement electronic signatures. The security of the RSA algorithm is validated, and mostly no attempts were able to break it, since it is difficult to find out the two large primes p and q, from the number n=pq.

C. *Public-key cryptosystems*

Let us assume that, each user has their own encryption and decryption procedures, En (public key) and Dn (Secret key). In RSA algorithm, these two procedures are denoted as two numbers. Let us assume that Msg is a message to be encrypted. We follow four statements which are essential to a public-key cryptosystem.

a) Deciphering an enciphered message gives you the first message, symbolically Dn(En(Msg)) = Msg

b) Reversing the procedures still returns M En(Dn(Msg)) = Msg ….. (2)

c) En and Dn are easy to compute.

d) The publicity of En does not compromise the secrecy of Dn, meaning you can't undoubtedly make sense of Dn from En.

With a given En, we are still not given an efficient way of computing Dn. We know that, if Ct = En(Msg) is the cipher text, then computing Dn and to satisfy the Msg in En(Msg) = Ct is arbitrarily difficult. The above properties prove that, it is trap door one way permutation, For example, the users ALC and BOB (Alice and Bob) on a two user public key cryptosystem, with their keys: EALC, EBOB, DALC, DBOB.

RSA Cryptography: Key Generation in Pervasive environment the following steps to be followed for RSA key generation:

1. Produce two prime numbers p and q
2. Find $n = p \times q$
3. Find $\Phi(n) = (p - 1) \times (q - 1)$
4. Select e, such that $1 < e < \Phi(n)$ and $\gcd(\Phi(n), e) = 1$, where e is an exponent

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

5. Calculate d such that d = e−1 mod Φ (n), where d is a private exponent
6. Public Key = [e, n]
7. Private Key = [d, n]

VI. BIOMETRIC RSA SYSTEM

Example Scenario in Pervasive Environment: The proposed system is used to generate key. In this proposal, we combine the features of biometrics based on RSA algorithm. Basically it is composed of fingerprint authentication module, asymmetric cryptography module. It is depicted in the following Figure.

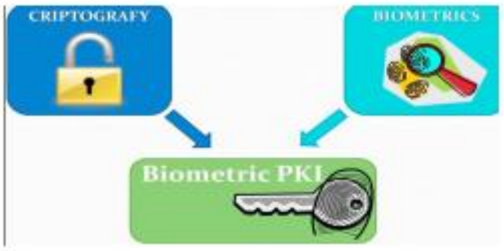

Figure: Biometric RSA System

RSA Biometric: The method includes the following features;

i) The bio metric private key is generated at random and not stored in any device, and using the fingerprint characters stored in user smart card at the enrolment phase.

ii) Damage proof smart cards and Cryptography provide a secure environment and protect from unauthorized access to smart card devices.

iii) It likewise secures the privacy of the bio metric data. Along these lines, the private key can't be lost and stolen.

iv) Unique mark picture quality, influencing frameworks execution, can be checked amid the enlistment stage. In the enlistment stage, the bio metric characteristic is obtained and handled to extricate its own particular unmistakable highlights.

v) In the verification stage, the selected bio metric identifier is utilized together with the inquiry bio metric identifier for client confirmation and open/private key combine age.

VII.CONCLUSION

In this paper, we propose a biometric authentication using RSA cryptographic algorithm. We discussed the key establishment scheme using biometrics for Pervasive computing environments. The proposed verification instrument is effective in tackling the contention between security assurance and validation, which generally needs the clients' delicate data. Explicit mutual authentication is achieved among the service providers and users by following this approach. This scheme is effective in maintaining the anonymity and confidentiality of the user. As a result, the approach proposed can serve very well in pervasive computing environments.

REFERENCES

1. M. Weiser. The computer for the twenty-first century. Scientific American, 265(3): 94-104, 1991. [2] Juan Ye and Simon Dobson. “Pervasive Computing needs better situation –awareness” , doi:10.2417/3201201.003943
2. Ameera Al-Karkhi1, Adil Al-Yasiri2 and Nigel Linge, “Privacy, Trust and Identity in Pervasive Computing: A Review of Technical Challengesand Future Research Directions” Department of Computing, Science and Engineering, University of Salford,
3. Steffen, S., Bharat, B., Leszek, L., Arnon, R., Marianne, W., Morris, S., et al., (2004) “The pudding of trust”. IEEE Intelligent Systems, 19(5), 74-88.
4. Saadi, L., Marc, L., & Carsten, R., (2005) “Privacy and trust issues with invisible computers”. Commun. ACM, 48(3), 59-60.
5. Zugenmaier, A., Kreutzer, M., & Muller, G., (2003) “The Freiburg privacy diamond: An attacker model for a mobile computing environment”.
6. Divyajyothi M G, Rachappa and Dr. D H Rao,” Techniques of Lattice Based Cryptography Studied On A Pervasive Computing Environment,” International Journal on Computational Science & Applications (IJCSA), Vol.5, No.4, August 2015.
7. Divyajyothi M G, Rachappa and Dr. D H Rao, “A Scenario Based Approach for Dealing with Challenges in A Pervasive Computing Environment,” International Journal on Computational Sciences & Applications (IJCSA), Vol.4, No.2, April 2014.
8. Zugenmaier, A., & Hohl, A., (2003) “Anonymity for users of ubiquitous computing”, in the 2nd Workshop on Security in Pervasive Computing.
9. Roy Campbell1, Jalal Al-Muhtadi1, Prasad Naldurg1, “Towards Security and Privacy for Pervasive Computing”, Department of Computer Science, University of Illinois at Urbana Champaign.
10. Alfred, K., & Jörg, S., (2003) “Privacy through pseudonymity in user-adaptive systems”. ACM Trans. Interet Technol., 3(2), 149-183.
11. Jason, I. H., & James, A. L., (2004) “An architecture for privacy-sensitive ubiquitous computing”, in the 2nd international conference on Mobile systems, applications, and services, (Boston, MA, USA).
12. Chatfield, C., & Hexel, R., (2005) “User identity and pervasive computing: User selected seudonyms”, in the Workshop on UbiComp Privacy: Privacy in Context,, (Tokyo, Japan).
13. Langheinrich, M., (2002a) “A privacy awareness system for ubiquitous computing environments”, in the Proceedings of the 4th international conference on Ubiquitous Computing, (Sweden).
14. Khusvinder Gill, Shuang-Hua Yang, Fang Yao, and Xin Lu,”A ZigBee Based Home Automation System”, IEEE Transactions on Consumer Electronics, Vol. 55, No. 2, MAY 2009
15. T. Abdelzaher, Y. Anokwa, P. Boda et al., “Mobiscopes for human spaces,” IEEE Pervasive Computing, vol. 6, no. 2, pp. 20–29, 2007.
16. D. Chander, B. Jagyasi, U. B. Desai, and S. N. Merchant, “Spatio-temporally adaptive waiting time for cell phone sensor networks,” International Journal of Distributed Sensor Networks, vol. 2011, Article ID 962476, 21 pages, 2011.
17. Evgeny Milanov, The RSA Algorithm, 3 June 2009
18. Edward Schaefer, “ An introduction to cryptography and cryptanalysis”, Santa Clara University [21] M Varaprasad Rao1 and Prof N Ch Bharta Chryulu2, “ SECURED SMART SYSTEM DESING IN PERVASIVE COMPUTING ENVIRONMENT USING VCS International Journal of UbiComp (IJU), Vol.6, No.2, April 2015
19. Yao Lin, Kong Xiangwei, Wu Guowei, Fan Qingna, Lin Chi, “A Privacy Preserving Authentication Scheme Using Biometrics for Pervasive Computing Environments”, Journal of Electronics(China), 2010.
20. Pankaj Bhaskar and Sheikh I Ahamed, “Privacy in Pervasive Computing and Open Issues”, Proceedings of the International Conference on Availability, Reliability and Security (AReS), IEEE CS Press, Vienna, Austria, April 2007

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)