BIOMETRIC CRYPTOGRAPHIC AUTHENTICATION IN PERVASIVE ENVIRONMENT

Rachappa[1], DivyaJyothi M G[2] and Dr. D H Rao[3]

[1]Research Scholar, Department of Computer Science, Jain University, Bangalore
[2]Research Scholar, Department of Computer Science, Jain University, Bangalore
[3]Professor and Dean, S.G. Balekundri Institute of Technology, Belgaum

ABSTRACT

Day by day technology is moving towards advancements and pervasive computing environment is leading where the users can get services everywhere. The ubiquity of the smart spaces brings new security challenges, in which the user and the service provider have to be authenticated with the strong authentication technique. In this proposal, a very flexible common authentication scheme based on biometric encryption to protect communications between a user and a service provider is proposed. In this proposal, user's hidden authentication is achieved.

KEYWORDS

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

1. 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. Pervasive computing proposes the assurance of simplifying daily life by incorporating mobile devices and digital infrastructures into our real world. With the help of several sensors and embedded devices, active spaces can automatically be combined to users' preferences and can capture and utilize context information. Sometimes, this feature could threaten the privacy of users rigorously and raise the issues of information misuse. For example, this feature can be misused by intruders, hackers, malicious users of insiders, sometimes system administrators to thread users. Undoubtedly, for preserving users' privacy is much more difficult task in pervasive environment.

Pervasive computing technology will surround users with a contented and convenient information environment that combines physical and computing devices into an integrated environment. This feature will upsurge the productivity and interaction. Context awareness will allow this

environment to take on the responsibility of serving users, with combined activities according to the nature 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.

A pervasive computing environment unexceptionally and transparently supports the human beings with its uninterrupted computation and communication [7]. This computation power guarantees transparent interaction of the devices with the users [8][2]. In pervasive computing environment, control over collection and dissemination of information is perceived through privilege of users, which is in turn called as privacy in PCE and these users can be categorized as individuals, groups, or organizations.

Normally, the basic security mechanism involves static network or closed system with the central control, whereas the Pervasive computing environments mutual communications are unexpected and are dynamically active. The communication channel will be established between a user and a service provider. Subsequently, before to the access of services, a mutual agreement between users and service providers should be established.

Increase in location based applications guarding personal location information has become a foremost challenge. In order to resolve this matter, a set of procedures and guidelines are required which should allow users to control their location information predictably. With the major concern about privacy and security in pervasive computing environments, ample research has been conducted concentrating on various aspects [3].

2. 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. The tedious and complicated proposals of pervasive environments are embedded or they are invisible.

In pervasive computing environments, the 'invisible' computing devices are increasingly gathering personal data and deriving user context, the user will be concerned with their privacy and security. Devices may reveal and exchange personal and sensitive information (such as identity, role, preferences, credentials, etc) with the smart objects in pervasive systems. Privacy in pervasive environment will be a major issue, when the devices cannot belong to a one trusted domain. It is a critical situation to develop and create privacy sensitive services in pervasive computing systems to increase the real benefit of these technologies and decrease possible and actual risks. Since these systems gather a large amount of personal sensitive information (such as e-mail id, shopping history, location, etc.) and showing people's negligible interest in participating pervasive environments.

Henceforth, in order to maintain privacy at all times, it has become mandatory to design proper procedures and guidelines.

Privacy can be well-defined, according to Steffen et al. [4], as "An entity's ability to control the availability and exposure of information about itself". In [5], the authors identify five important

key features which make these systems very different from the current data collection systems [3]. They are:

1. Innovative and State-of-the-art computing technologies and objects will be presented in active space.
2. Data collection will be invisible and unnoticeable;
3. The gathered data will be more friendly than ever before;
4. The underlying motivation behind the data collection;
5. The necessary interconnectivity for smart devices to cooperate for providing service to users;

2.1 Anonymity

The actual identity of the user should never be disclosed from the communications exchanged between the user and a server unless it is deliberately revealed by the user.

In order to analyze the secrecy mechanisms with regard to device flexibility, the author, Zugenmaier et al. [6] proposed a new attacker model, "Freiburg Privacy Diamond Model (FPD)".

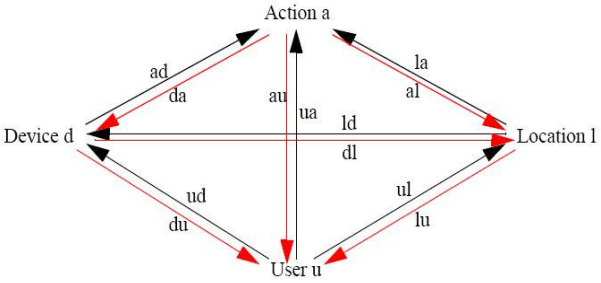

Figure1. Sample Privacy Model [9]

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.

2.2 Confidentiality and Integrity

Confidentiality refers to the need of keeping information secure and confidential. Integrity refers to the concept of protecting information from being inappropriately modified by unauthorized users.

2.3 Unobtrusive

The main aim of pervasive computing is to be anonymous and unobtrusive. The computing technology is embedded into everyday smart objects that communicate information. This concept

of embedding reduces the visibility of the pervasive computing environment and makes the technology more friendly and adequate to the user.

Consequently, the same characteristic will invade the privacy of the user without the user realizing it.

2.4 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 these information to the service provider.

2.5 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.

2.6 Data Collection

A pervasive computing application relies on an large amount, quality, and accuracy of data generated and collected. Also most of the pervasive computing technologies include wireless devices and these devices are limited to processing power, throughput, bandwidth, memory etc [14].

2.7 The Service Provider

Maintaining the privacy of data is very crucial for service provider. Chances and vulnerabilities for misuse of data is more. In reality, its difficult to ensure that all the service providers follow the rules.

The author, Langheinrich [15] measured, designing a perfect mechanism for protecting privacy would be hard to achieve. Subsequently, the author proposed a system, for alerting users about their privacy. The proposed system depends on social and legal principles of real life, rather than designing a system to ask and respect the users' privacy. The publisher named the system as, the privacy awareness system (pawS), which allows data collectors to process personal data, sensitive data and organization policies, and data manipulation tools such as adding, deleting and modifying information

The developed pawS architecture consists of two main parts: privacy proxies and a privacy aware database.

Privacy proxy:

This proxy is developed to allow the automatic interchange and auto update of privacy policies and client information. This is proxy is developed and implemented to run on a web server using group of services called Simple Object Access Protocol (SOAP) protocol. In this protocol all the user's requests are responded by the service proxies.

Privacy aware database:

This is known as pawDB. This protocol combines the users' privacy policies and their collected data elements into a sole component of storage space which then handles the data according to the usage policy.

3. ASSOCIATED WORK

Many authors have proposed numerous proposals and models to address the concerns of privacy protection in pervasive computing environment. In this paper, we propose a unique scheme for privacy preserving authentication in pervasive computing environments.

4. SYSTEM ARCHITECTURE

Biometric cryptographic authentication with RSA algorithm is used to authenticate in our scheme. 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.

4.1. 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 major advantages of biometrics are uniqueness, and need not to remember passwords. Biometrics is what you have, and it cannot be stolen or forgotten.

The Biometric technique is shown in Figure 3.

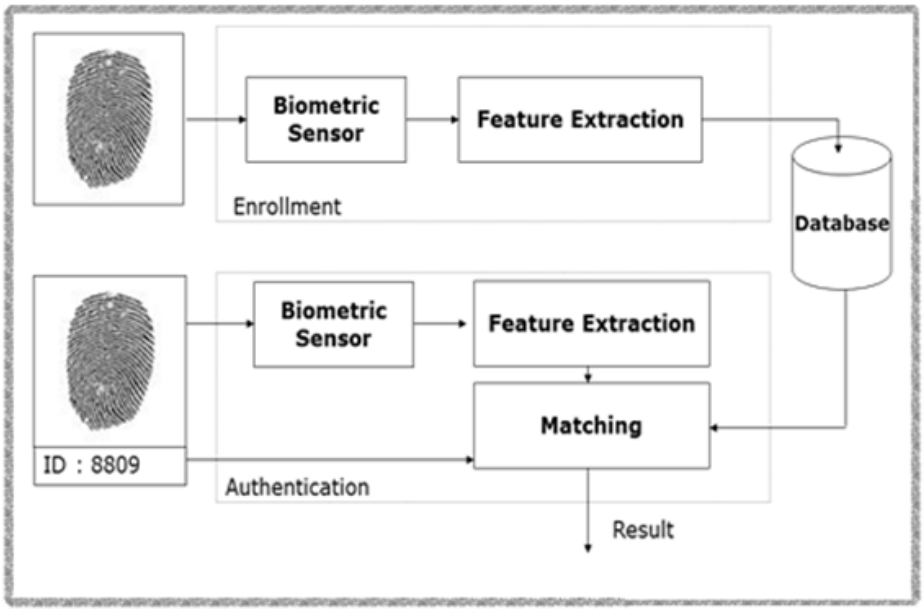

Figure 2: General Biometric System

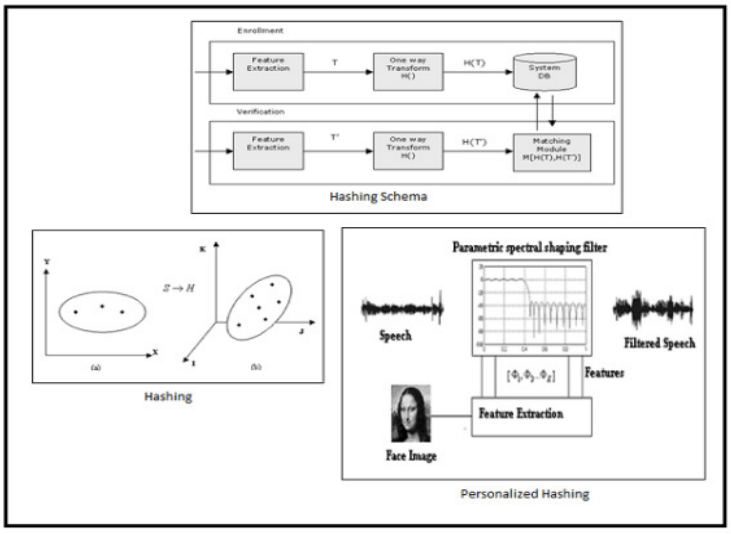

Figure 3: Biometric Hashing

In the recent days, rapid growth has been observed in mobile computing with miniature devices. [17]. The following Figure 4 depicts the pollution monitoring application using Cell Phone based Sensor Network (CPSN) developed in [18] uses short-range communication outlets such as Wi-Fi or Bluetooth

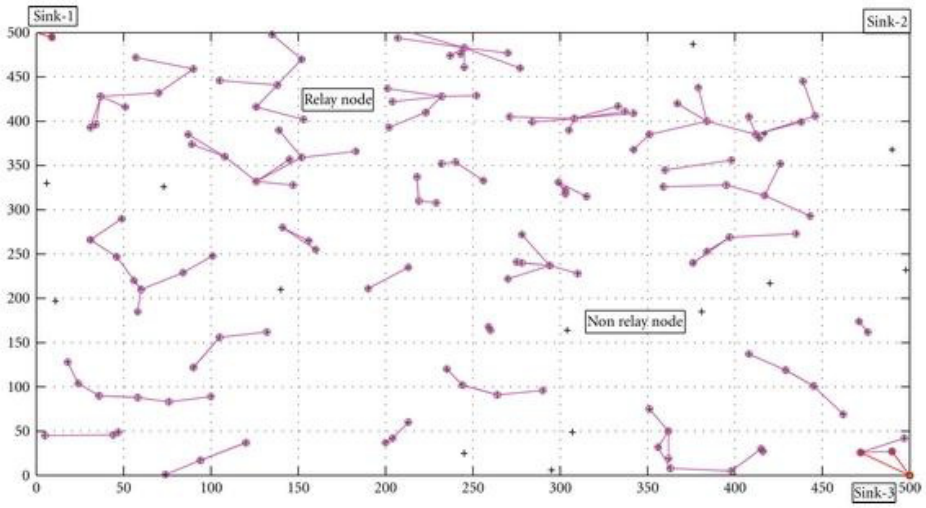

Figure 4: Cell phone based sensor network.

On the other hand, **Cryptography** is where security engineering meets mathematics. Cryptography provides numerous methods, algorithms and protocols to maintain authenticity. Possibly, it uses key enabling technology for protecting distributed systems. It mainly concerns itself with the projection of trust: with moving the trusted data from where it exists to where it is needed.

A strong combination of biometrics and cryptography in pervasive environment would have strong authentication scheme. It will be a tedious task to break the security and authenticity using stolen token.

5. 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 solution implants biometric information on the private/public keys generation process. Also the corresponding private key depends on biometric features and it can be generated when it is needed. Starting from the fingerprint acquisition, and all the behavioural biometric features, the biometric identifier is extracted, cyphered.

5.1 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:

5.1.1. 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 public, and decryption keys are private. The generated keys must have a property of non-repudiation and cannot be easily assumed from the public encryption key. The keys are to be transmitted to recipients over a secure channel.

5.1.2. 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.

5.1.3 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 original 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 cannot
   easily figure out 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.

5.2 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
5. Calculate d such that $d = e^{-1} \bmod \Phi(n)$, where d is a private exponent
6. Public Key = [e, n]
7. Private Key = [d, n]

5.3 RSA Cryptography: Selecting the Primes p and q

Firstly we need to decide the size of the modulus integer n. Let us assume that our implementation of RSA needs modulus of size B bits.

In order to generate the prime integer p;
– Generate a random number of size B/2 bits.
– Set the lowest bit of the integer generated by the above step, random number generator; this ensures that the number will be odd.
– Set the two highest bits of the integer; and ensure that the highest bits of n will be set.
–Check the resulting integer is prime or not. If the resultant integer is not a prime, then increment it by 2 and check again.

This becomes the value of p.

Follow the above steps for selecting q.

- If we get p = q, omit the generated random number, and find the new one.
- If the resulting integer is not a prime, then re generate the new random number, rather than increment by 2

5.4 Efficient encryption and decryption operations.

The RSA algorithm states that "Computing $M^e \pmod n$ requires at the most $2 \cdot \log_2(e)$ multiplications and $2 \cdot \log_2(e)$ divisions". It is important to find the amount of steps it would take a computer to encrypt the message so, it can be evaluated the performance of the algorithm. The method follows:
Step 1. Let $e_k\, e_{k-1} \ldots e_1 e_0$ be the binary representation of e.
Step 2. Set the variable C to 1.
Step 3. Repeat steps 3(i) and 3(ii) for i = k, k – 1, ..., 0:
Step 3(i). Assign $C = C^2 \bmod n$
Step 3(ii). If $e_i = 1$ then, assign C to the remainder of $C \cdot M$ when divided by n.
Step 4. Halt. Hence C is the ciphertext of M
There are many proposed procedures exists, but we found this is the better algorithm. More importantly, the decryption technique follows the similar unique procedure as encryption, and can be implemented the whole process on a few integrated chips.

As per the RSA, it claims that "the amount of encryption time per block rises no faster than the cube of the number of digits in n.

6. 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.

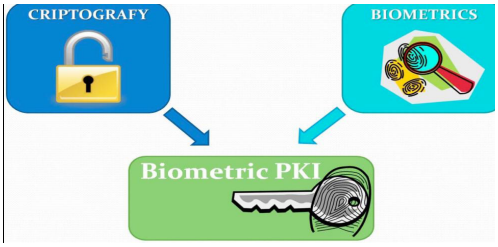

Figure: Biometric RSA System

6.1 RSA Biometric:

The method includes the following features;

i) The biometric private key is randomly generated and not stored in any device, and using the fingerprint characters stored in user smartcard during the enrolment phase.
ii) Damage proof smartcards and Cryptography provide a secure environment and protect from unauthorized access to smartcard devices,
iii) It also protects the confidentiality of the biometric information. So, the private key cannot be misplaced and stolen.
iv) Fingerprint image quality, affecting systems performance, can be checked during the enrolment phase.

In the enrolment phase, the biometric trait is acquired and processed to extract its own distinctive features.

i) Biometric trait representation is encrypted and stored in tamper-resistant device,such as, smartcard.
ii) During the authentication phase, the enrolled biometric identifier is used together with the query biometric identifier for user authentication and public/private key pair generation.
iii) The link between biometric traits and the cipher algorithm is a pair of prime number.

6.2 Signatures with RSA:

Say Bob (=B) and Dave =(D) are using RSA. In a public key cryptosystem, there is no shared key that only Obama and Cameron have. So Verda (=V) could email Bob an AES key, encrypted with Bob's public RSA key and then send Bob the message "Hello Verda, sincerely, Dave" encrypted with AES. How would Bob know whom it's from, he must demand a signature. [20]

Case 1, D sends PT msg M to B, no need to encrypt. At end signs M_2 ='Dave'. Wants to make sure B knows it is from him. C then computes $M_2^{dC} \bmod n_C = S$. Could add to end of msg. Only C can do that. The message can be verified by B, just by finding $S^{eC} \bmod n_C$ in order to get M_2. Eve can read signature too. Also L can cut and paste signature to end of his own message.

Case 2. C creates an AES key and sends $(key_{AES})^{eB} \bmod n_B$ to B. C encrypts message M for B using AES and sends CT to B. C hashes M to get H=hash(M). C computes $H^{dC} \bmod n_C = S$ and sends to B. B decrypts using RSA to get key_{AES}. B decrypts CT with AES to get M. B hashes (decrypted) M to get H. B compute $S^{eC} (\bmod n_C)$ and confirms it equals H he earlier computed. Only C could have created an S so that $S^{eC} = H$. If it does, then B knows 1) the message was sent by whoever owns the keys e_C and n_C (authentication) and that it was not tampered with by anyone else (integrity). Note that V has access to H. B and C may not want that. So C may encrypt S with RSA or AES.

Case 3. Same as case 2, but B and C do not want V to have access to hash(M) (for whatever reason - maybe C will resend M to someone else). So C encrypts S using AES.

7. RSA - THE SECURITY SYSTEM

Pervasive security environments demands high degrees of security for its deployment and RSA based hardware and software products can be very much used for the secure communication and authentication. Already RSA based security employee tokens are widely in use in various companies. The uniqueness of this token lies in the fact that the public key generated by these tokens vary every time one runs it. This along with any other biometric trait can make a strong authentication identifier.

8. 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 authentication mechanism is efficient in solving the conflict between privacy protection and authentication, which usually needs the users' sensitive information. 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.

9. ACKNOWLEDGMENTS

We would like to thank our Professor Dr. D. H. Rao for the patient guidance, encouragement, and time given during the course of our work.

10. 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

[3] 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,
[4] 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.
[5] Saadi, L., Marc, L., & Carsten, R., (2005) "Privacy and trust issues with invisible computers". Commun. ACM, 48(3), 59-60.
[6] Zugenmaier, A., Kreutzer, M., & Muller, G., (2003) "The Freiburg privacy diamond: An attacker model for a mobile computing environment".
[7] 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.
[8] 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.
[9] Zugenmaier, A., & Hohl, A., (2003) "Anonymity for users of ubiquitous computing", in the 2nd Workshop on Security in Pervasive Computing.
[11] Roy Campbell1, Jalal Al-Muhtadi1, Prasad Naldurg1, "Towards Security and Privacy for Pervasive Computing", Department of Computer Science, University of Illinois at Urbana Champaign.
[12] Alfred, K., & Jörg, S., (2003) "Privacy through pseudonymity in user-adaptive systems". ACM Trans. Interet Technol., 3(2), 149-183.
[13] 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).
[14] Chatfield, C., & Hexel, R., (2005) "User identity and pervasive computing: User selected seudonyms", in the Workshop on UbiComp Privacy: Privacy in Context,, (Tokyo, Japan).
[15] Langheinrich, M., (2002a) "A privacy awareness system for ubiquitous computing environments", in the Proceedings of the 4th international conference on Ubiquitous Computing, (Sweden).
[16] 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
[17] T. Abdelzaher, Y. Anokwa, P. Boda et al., "Mobiscopes for human spaces," IEEE Pervasive Computing, vol. 6, no. 2, pp. 20–29, 2007.
[18] 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.
[19] Evgeny Milanov, The RSA Algorithm, 3 June 2009
[20] 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
[22] 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.
[23] 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

AUTHORS

Mr. Rachappa is currently working as Lecturer at the Department of Information Technology, Al Musanna College of Technology, Sultanate of Oman. His teaching interests include Computer Security, Pervasive Computing, E-Commerce, Computer Networks, Intrusion detection System, Network Security and Cryptography, Internet Protocols, Client Server Computing, Unix internals, Linux internal, Kernel Programming, Object Oriented Analysis and Design, Programming Languages, Operating Systems, Web Design and Development, etc. His most recent research focus is in the area of Security Challenges in Pervasive Computing. He received his Bachelor Degree in Computer Science from Gulbarga University, Master of Science Degree from Marathwada University and Master of Technology in Information Technology Degree from Punjabi University (GGSIIT). He has been associated as a Lecturer of the Department of Information Technology since 2006. He has worked as Lecturer at R.V. College of Engineering, Bangalore. He has guided many project thesis for UG/PG level. He is a Life member of CSI, ISTE.

Mrs DivyaJyothi M.G. is currently working as Lecturer at the Department of Information Technology, Al Musanna College of Technology, and Sultanate of Oman. Her teaching interests include Pervasive Computing, Firewalls and Internet Security Risks, E-Commerce, Computer Networks, Intrusion detection System, Network Security and Cryptography, Internet Protocols, Client Server Computing, Unix internals, Linux internal, Kernel Programming, Object Oriented Analysis and Design, Programming Languages, Operating Systems, Image Processing, Web Design and Development, etc. Her most recent research focus is in the area of Pervasive Computing. She received her Bachelor and Master Degree in Computer Science from Mangalore University, She bagged First Rank in Master's Degree at Mangalore University. She has been associated as a Lecturer of the Department of Information Technology since 2007. She has worked as Lecturer at ICFAI Tech., Bangalore, T John College for MCA, Bangalore, Alva's Education Foundation Mangalore. She has guided many project thesis for UG/PG level.

Dr. D H Rao is Currently working as Professor and Dean, S.G. Balekundri Institute of Technology, Belgaum. He has worked as a Dean, Faculty of Engineering, VTU, Belgaum. He was Principal at KLS Gogte Institute of Technology, Belgaum and Jain College of Engineering, Belgaum. He is the Chairman, Board of Studies in E & C Engineering, VTU, Belgaum. He is a Member, Academic Senate, VTU Belgaum. He has over 100+ publications in reputed Journals and conferences. He obt ained B.E. (in Electronics from B.M.S. College of Engineering), M.E. (from Madras University), M.S. (University of Saskatchewan, Canada) Ph.D. (Univ. of Saskatchewan, Canada).