International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-9 Issue-1S, October 2019

Assessing Software Risks by Implementing Cloud Readiness and Benchmarking in the Pervasive Environments

Vinita Malik, Sukhdip Singh

Abstract*: The evolution of revolutionary computational paradigms has been witnessed in terms of the pervasive systems which not only offer evolving service portfolio but also integrated sensor data from variable sources but surfaces various challenges of data interaction, integration and adaptation. This research has been provisioned with the comprehensive focus on pervasive devices user interaction, access control modeling, identity management, trust and service discovery modeling. In addition, we also proposed a deep insight into Pervasive computing characteristics, risks, and risks models, environmental, ethical and social impacts. We have explored pervasive computing environment risk models by considering social, human and environmental risks. This state of art will create a case for developing new models for access control, identity, trust, risk management in ubiquitous or pervasive computing environments. The paper has implemented the benchmarking of smart applications by a smart tool by gathering various application and business metrices to improve software performance. This research has also implemented the cloud readiness of a pervasive power reader application for PaaS environment using a smart vendor solution. The cloud readiness score is evaluated by questionnaire qualitative information and source code scan. Various boosters and roadblocks are found out to give score to cloud readiness for any application.

***Index Terms*: Pervasive/Ubiquitous Computing, Risks, Trust, Access Control, Privacy, Identity Management, Cloud Readiness, Benchmarking**

I. INTRODUCTION

The things that seem to be everywhere have been widely developed by integrating, communicating and distributing the computations in people lives, workspaces. The pervasive devices have made human life very promising by implementing moving interactions with intelligent systems with digital infrastructure. The pervasive calm technology has the ability to communicate to any device via any network without awareness of embedded technology. The self-adaptive solutions are the major attractions in ubiquitous environments which envisage complex computational environments demanding heterogeneous devices communicating with different sensitivities. The contextual data gathered about surrounding by pervasive devices helps to provide context aware non- intrusive services to users. The current most profound technologies come under Mark

Weiser's vision of pervasive or ubiquitous computing. But these devices envision so many challenges and risks which were never faced in traditional computing paradigms.

This research addresses all key aspects in pervasive computing risks, access control, user interaction, identity management, risks assessment, privacy concerns, trust management , impacts and challenges encountered.

Various search engines like Springer, Elsevier, and IEEE Explore have been unearthed to gather the relevant information. The paper is parted into various sections to introspect analysis on pervasive systems definition,

characteristics, and risks, models for risk management access control, identity, trust management, servicediscovery, privacy, impacts and challenges. In section 2, the research discusses the definition, Characteristics, risks and challenges involved in pervasive computing environment. In next section, we deal with various models for risks, access, privacy, identity, and trust and service discovery. Section 4 provides an insight into various impacts of pervasive computing. Section 5 has implemented the cloud readiness of a pervasive computing application i.e. smart power reader for PaaS environment. Next section discusses how benchmarking of a smart pervasive application is beneficial for quantitative performance improvement of the software. The last section concludes the paper by providing suggestions for future research.

II. BASICS: PERVASIVE COMPUTING

This section deals with the Pervasive computing definition, characteristics, risks, applications and challenges faced by this computing environment.

A. Definition

Mark Weiser proposed the definition of ubiquitous/pervasive computing as the methodology used to increase computer usage by building several computing resources available throughout the physical environment by making them invisible to the user [1]. The Pervasive devices are either the computing devices carried by human beings or the infrastructure devices embedded in the surrounding environments [2].Marcia Riley introduced pervasive computing as the calm technology where technology becomes virtually invisible in human lives [1].

Manuscript published on 30 October 2019.
* Correspondence Author (s)
Vinita Malik, Information Scientist, Central Library ,Central University of Haryana, Mahendergarh, India
Sukhdip Singh, Department of Computer Science and Engineering, D.C.R.U.S.T, Murthal, India

The major trends in computing includes transition from mainframe to desktop to pervasive computing. This computing utilizes embedded systems and portable devices for saturating the users with wireless environments that include actuators or sensors for interaction amongst human and machines. The technologies of pervasive capabilities are integrated into everyday life [3, 4, 5]. The complex meshed ubiquitous environment is as depicted in the Fig. 1 as shown below [6]:

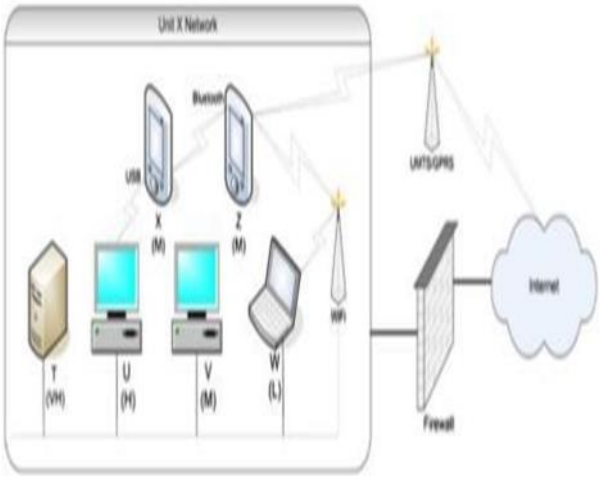

Fig. 1. Evolutionary Computing

B. Characteristics

The basic characteristics of the pervasive computing have been derived as follows [7]:

• Intelligent: The computing devices are intelligent enough to learn by user behavior and preferences. The devices are adaptable to user needs. Ambient intelligence helps to perform all work proactively.

• Embedded: Devices are implanted in user environment but stay invisible but transparent.

• Context Awareness: Operations are aware of physical and logical context in which they happen and adapt according to environment.

Autonomous: The user does not directly interact or interfere with the system delivered services.

C. Risks

Following are the potential risks screened in pervasive computing environment [8]: The risks of pervasive computing can be categorized into three categories i.e. Social, Environmental and Human risks.

Social Risks: Following are the social risks in pervasive environment:

• Undermine privacy regulations due to identification with ICT

• Computer crimes due to ICT networking

• Undermine causation principle due to uncontrolled complexity

• Loss of social contacts or isolation due to ubiquitous information access

• The economy of attention dominates over culture

• Restricted consumer freedom of choice due to pervasion of life by ICT

Environmental Risks:

• Increased usage of toxic material due to miniaturization of ICT

• Increased power consumption

• Disposal issues

• Small product service life due to virtual wear outs

• More Residential energy consumptions

Human Risks:

• Health hazard by NIR exposure

• Health issues due to physical contact with microelectronics

• Health problems by active implants

• Poor ergonomics causing stress

• The Unpredictable technical systems causing stress

D. Applications

Following are the application areas of pervasive computing:

• Communications: This area in general affects all other forms of data transmission and serves as a precondition for information technology.

• Logistics: To keep track of logistical goods and transport chain of materials.

• Motor traffic: Automobiles invisible assistance system to drivers by Networking with other vehicles and surroundings.

• Military: The development of new weapons and processing of cryptographic information for fighting against external threats.

• Production: This computing helps in developing decentralized production systems to monitor, configure and control it.

• Smart homes: The smart technology deployed in smart homes has devices for home lighting, heating, ventilation and communication.

• E-commerce: The smart objects have location based services and instructing software agents to carry out business transactions smoothly.

• Inner security: The smart cards are deployed as identification systems i.e. electronic passport for inner security. The monitoring systems are utilized for surveillance of airports and power grid.

• Medical technology: The multifunctional, miniaturized medical applications are used for intelligent implants.

E. Challenges

As various technologies like microelectronics, sensors, localization, security protocols, HCI and machine to machine communication are inherent in pervasive computing so there are various challenges faced by it which have been drawn below [7, 9, and 10]:

- Heterogeneity: In distributed systems to provide various types of devices, networks and environments pose challenge.
- Scalability: In distributed systems, increasing the number of resources and large scale deployments pose difficulty.
- Dependability and Security: In mission critical systems, provision of availability, reliability, integrity, safety is difficult to maintain.
- Privacy and Trust: In mobile computing, it's not only difficult to define the trust amongst different devices but also protecting against bad usage of data poses challenges.

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

- Interoperability: In mobile computing maintaining
- Interactions among components to permit their association are really cumbersome task.
- Mobility: It is very challenging to provide data access anywhere and anytime in mobile computing environment.
- Context Awareness: Inferring context information is a difficult task in mobile computing by user state information.
- Context Management: Adapting to current situation by modifying system behavior as per context information is cumbersome.
- Transparent User Interaction: Minimal distraction needs are raised in ubiquitous environment for merging UI with real world.
- Invisibility: It's very difficult to make computers disappear in the background in pervasive computing.

III. MODELS: PERVASIVE COMPUTING

This section of paper deals with various models of pervasive computing for risk management, access control, privacy control, identity management, trust management and service discovery.

A. Risk Management

Various models have been proposed in past for risk assessment and management. As risk management is basically an idea of how to identify the computing environment risks, how to assess them and then how to mitigate them. The computer crime and abuse survey [11] says that around 42% respondents experience mobile devices theft, out of which 6% incurs intellectual property loss. Various risk assessment strategies like OCTAVE [12], MEHARI [13], CRAMM [14] have been used for assessing risks for mobile devices. First all the asset value, threats, vulnerabilities are identified and then categorization is done. Once categorization is completed, asset value categories, threats, vulnerabilities are calculated to further mitigate them. After risk calculation, adaption through community is done to mitigate them [15]. The temporary risk matrix is provided in Table 1[15].

Table 1: Risk Matrix

Threat level \ Asset value	1	2	3	4	5	6	7	8
1	1	1	2	3	4	5	6	7
2	1	1	2	3	4	5	6	7
3	1	2	3	4	5	6	7	8
4	2	3	4	5	6	7	8	8
5	2	3	4	5	6	7	8	8

In the ubiquitous environment, the risk probability is associated with the degree of interaction amongst computing devices for which the following formula is presented [16]:

$$P^i = F(X^i) + Z^i \quad (1)$$

Where

Pi = Risk Probability Distribution Xi

Fi= Feature vector interaction which has feature elements for context specification.

Zi=Random Distribution Vector

B. Access Control

The main objective of access control on system should be putting restrictions on the actions a legitimate user performs on a given resource [17].Various models for access control include Role based access control to enforce organizational policies for large distributed environment[18,19]. The GRBAC (Generalized role based access control) used environmental roles for contextual information capture [20]. The model GTRBAC (Generalized Temporal RBAC) was used to differentiate between enabled and active role [21]. The spatial Role based access control introduces constraints based on user location and the location space is furcated into zones and an access permission is granted for satisfaction of role condition [22]. For supporting dynamic access permissions, DRBAC (Dynamic role based access control) came into picture [23]. The access role is also activated when contextual constraints gets satisfied by using state checking machine[24].The CRAAC model was designed to decouple context infrastructure and AC(access control) system for accommodating various contextual attributes[25].

C. Privacy Control

There is stringent need of privacy control in pervasive computing due to requirements of enhanced storage capability, minimization of sensors, invisible data capture and pervasive data communication. Privacy protection mechanisms include privacy awareness system[26](offers cooperation with anonym zing solutions),context driven identity management[27](anonymity level is highly situational) ,mist protocol[28](offers location privacy and connections anonymity), mix zones [29](combination of alterations of pseudonyms) ,privacy mirrors[30] (anonymity assured indirectly), privacy tagging models (high anonymity in trusted environments)[31]. The autonomous agents have been used for privacy management which requires common language for users, way to communicate privacy events, control of information flow context, negotiation of privacy control enforcements [32].

D. Identity Management

The service delivery system involves the identity information exchange. The modern system must be able to identify them in network for pervasive data exchange. The process of user identification is done by re-authentication where every individual of group re authenticate himself before getting a new key [33,34]. Other models for identity management include entity recognition by pluggable recognition module [35] and Resurrecting Duckling model where a slave device pose to be a master device by transfer of imprinting key[36].

An efficient authorization may be achieved via context and location based information on encryption [37]. As in pervasive environment it is very difficult for users to prove their identity by authentication every time so Non-intrusive assertion systems are developed to become aware of user intentions [38].The contextual attributes like location and manufacturer certificate are required to validate user level quality assurance [39].

E. Trust Management

Trust is amongst the most vital element in pervasive computations and a relation between trusted and trustee [40].Trust is used for user protection based on gathered trustworthy information [41]. The distributed trust architecture must include a clearly stated security policy, proper assignment of credentials to users, delegation of trust to trusted third party [42]. Trust models are also based on user's behavior and link it to authentication protocol. Before the service provisioning, trustworthiness needs to be evaluated [43]. The net value of trust is combination of direct and indirect trust and whenever the trust value expires, it updates itself. SSRD+ (secure resource discovery) model used the dynamic trust relationships to specify behavioral characteristics to make whole resource discovery process secure. This privacy secure model also consults the user in case of response to a higher security level service request [44]. Another trust model is TOMS (Trust computation and management system) which is able to establish trust relation between distributed nodes and involve the efficient computation system [45]. The multicast mechanism is used for dynamic and agile systems like wireless sensor networks or MANETs.

F. Service Discovery

It is a mechanism of developing dynamic infrastructure where users need particular services and service providers advertise the services. The network needs to be self- managed and healing by automatic service detection. Service location protocol (SLP) by IETF is used with IP networking for service discovery. Other protocols are BSDP(Bluetooth service discovery protocol), iSNS (Internet storage name service), XMPP service discovery(XEP-0030),UDDI (Universal Description discovery and integration), SAP(session announcement protocol for discovering RTP sessions), WPAD(Web proxy auto discovery protocol)[46].

IV. IMPACTS: PERVASIVE COMPUTING

The pervasive computing which has become ubiquitous in nature poses serious impacts on environment, health and society. The following are the impacts that pervasive/ubiquitous computing has made over years [47]:
The environmental impacts:

- Increased resource consumption: Due to increased demand of pervasive device components, total energy consumption has resulted in global resource depletion.
- End of Life treatment: Pollutants release by waste disposal causes bad impact on environment.
- Increased individual traffic: Due to support for independence from fixed locations.

The Health related impacts:

- Exposure to NIR (Non ionizing radiations): The thermal effects of NIR exposure cause negative impact on body tissues.
- Physical contact with human body: Active implants cause several side effects to human body.

The Social impacts:

- Digital divide: This computing contributes to reduced digital divide by separating social groups.
- Consumer freedom of choice: People who are not able to use technology are deprived of certain services.
- Information Overload: Users will be flooded with information with more use of ICT.
- Privacy issues: Accumulation of RFID kind technology may threaten more by eavesdropping of unsecure RF (radio frequency) interfaces.
- Security issues: Security may be undermined by technology failure.

V. CLOUD READINESS IMPLEMENTATION OF PERVASIVE APPLICATIONS

The organizations are quite challenged to manage cloud risks. The blocking factors that cause a cloud to switch to non-cloud option are privacy, technical and compliance aspects[48].First assess the potential delivery models, goals and solution for cloud sourcing. Identify all factors that may be a blocking factor in future to resolve the conflicts and continuously improve the cloud sourcing checklist. The cloud delivery characteristics include service level quality, pay per use, availability, scalability, supplier market, dynamicity and flexibility [49]. We have utilized a smart vendor [50] which indicates the application readiness for PaaS environment. The score is calculated by source code scan and information gathered by a questionnaire. The code patterns which are able to adopt PaaS environment gives positive score and the code patterns which are tweaked before doing migration, results in negative score. The code for smart power reader has been downloaded from Github [51]. We have taken Smart power Reader application and the cloud readiness results are depicted below in Fig. 2.

Fig. 2. Smart power reader application cloud ready score

The application cloud ready score is 61.2 where the questionnaire survey tells that the cloud ready score is 46.8 whereas the code scans tells that the cloud ready score is 75.6. There are 02 roadblocks and 5.4 blockers. In the Fig. 3 given below the survey questions have been answered for the application Smart power reader as follows:

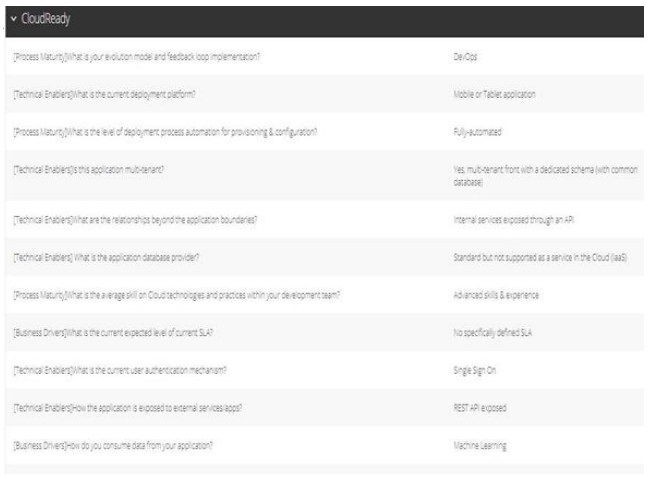

Fig. 3. Smart power reader application Cloud ready survey response

VI. BENCHMARKING IMPLEMENTATION OF A PERVASIVE APPLICATION

The benchmarking of softwares is used for the quantitative performance evaluation. The software design features are understood for building a good benchmark [52]. This section has implemented the benchmarking of a pervasive application i.e. Smartfarm, code for which has been taken from Github repository [53]. The application benchmarking has been done as per technology and application properties by a smart software vendor [54]. The vendor builds its own metrics repository by scanning the application and then dispersing the metrices over globe. The application properties are depicted as in Fig. 4 given below:

Fig. 4. Smartfarm application properties

The pervasive application has been benchmarked as per technology used in Fig. 5, 6 and 7 given below:

Fig. 5. Smartfarm application benchmarking for PhP technology

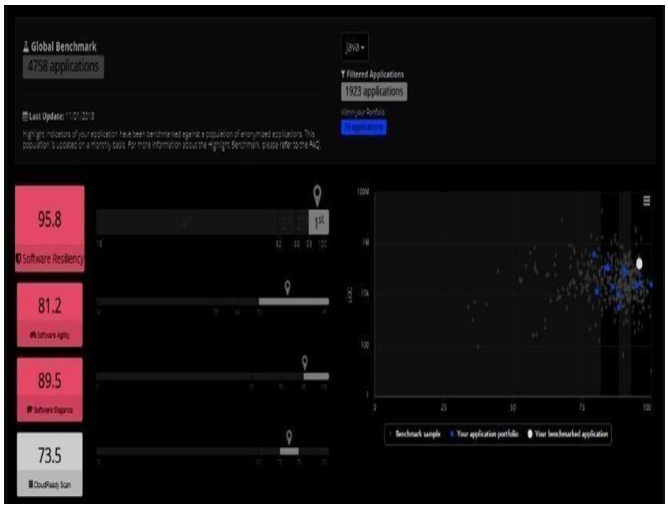

Fig. 6. Smartfarm application benchmarking for Java technology

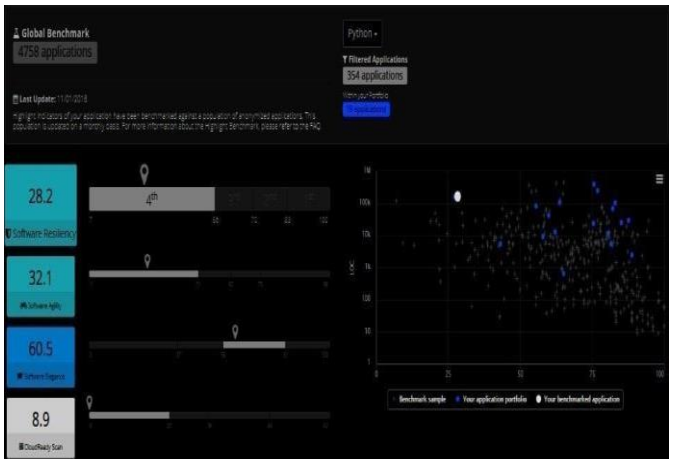

Fig.7. Smartfarm application benchmarking for Python technology

VII. CONCLUSION

Modern computing paradigms are ubiquitous in nature which has enabled a great need of deep analysis on risks inherent in such systems. The research poses explanation facility for various pervasive computing concepts like risks, access control, privacy control, identity management, trust models, challenges, service discovery and cloud readiness for migration to cloud. Various impacts of the computing on human life, health and social behavior have been described in the section 4.The research has implemented the cloud readiness for a pervasive application by a smart software vendor solution. The paper has provided strong foundation for benchmarking of smart applications as it is required for enhancing qualitative performance. This research provides the basis for proposing new models based on correlation between risk management and quality assurance in ubiquitous computing environment.

REFERENCES

1. A. A. H. Mousa, "Ubiquitous/Pervasive Computing" , International Journal of Innovative research & development , vol 2 ,pp:276-282,2013
2. M.Weiser, "The computer for the 21st century, Scientific American", 265(No. 3), pp : 94 –104,1991
3. Y.Ren, A.Boukerche., " Modelling and managing trust for wireless and mobile adhoc networks", In: proceedings of IEEE conference on Communications (ICC), 2008
4. J.M.Seigneur, " Trust, Security and Privacy in global computing" , PhD theses , Trinity College Dublin , 2005
5. S.A.Weis, " Security parallels between people and pervasive devices" , in : Proceedings of the 3rd IEEE International conference on pervasive computing and communications workshop ,pp. 105-109,2005
6. Z. Hayat, J.Reeve., "Ubiquitous security for ubiquitous computing" ,Information Security technical report ,12, pp. 172-178,2007
7. B. Abdulrazak., Y. Malik, "Review of challenges, Requirements and approaches of pervasive computing system Evaluation", IETE Technical Review, 29,6, pp.506-522,2012
8. L.M.Hilty, C.Som , " Assessing the Human, Social and Environmental risks of pervasive computing" ,Human and Ecological Risk Assessment ,10, PP. 853-874,2004
9. J.Sen, "Ubiquitous Computing: Applications, Challenges and future trends", PP. 1-41,2012
10. C.A.D Costa., "Towards a General software Infrastructure for ubiquitous Computing, Journal of Pervasive Computing" , IEEE CS , pp.64-73,2008
11. R. Richardson., "CSI Computer Crime and Security Survey", Computer security institute, 2009
12. CarnegieMellon University, http://www.cert.org/octave/download/intro.html
13. Clusif,http://www.clusif.asso.fr/fr/production/ouvrages/pdf/MEHARI-2010-Overview.pdf, 2010
14. Insight Consulting, http://dtps.unipi.gr/files/notes/ 2009-2010/eksamino_5/politikes_kai_diaxeirish_asfaleias/ egxeiridio_cramm.pdf, 2009
15. T. Ledermuller, N.L.Clarke, "Risk assessment for mobile devices", Lecture notes in computer science ,210-221,2011
16. F.Liu,Y.Chen., K.Dai.,Z.Wang, " Research on risk probability estimating using fuzzy clustering for dynamic security assessment" ,LNAI,3642,pp. 539-547,2005
17. R.Sandhu, P. Samarati, "Access control: principles and practice. IEEE Communications Magazine", 32(9),pp. 40–48.,1994
18. R.Sandhu, E.Coyne, H. Feinstein, C. Youman, , "Rolebased access control models". IEEE Computer, 29(2), 38–47,1996
19. S.Park,Y. Han, & T. Chung, , "Context-role based access control for context-aware application". In Lecture notes in computer science: Vol. 4208. High performance computing and communications (pp. 572–580). Berlin/Heidelberg: Springer, 2006
20. M.J.Covington, P.Fogla, Z.Zhan, M.Ahamad, "A context-aware security architecture for emerging applications". In Proc. 18th annual computer security applications conference (ACSAC '02), Washington, 2002 (p. 249). Los Alamitos: IEEE Computer Society, 2002
21. J.Joshi, E.Bertino, A.Ghafoor,. "Hybrid role hierarchy for generalized temporal role based access control model." In Proc. 26th international computer software and applications conference on prolonging software life: development and redevelopment (COMPSAC '02), Washington, DC (pp. 951–956). Los Alamitos: IEEE Computer Society, 2002
22. H.Zhang, Y.He, Z., "Spatial context in role- based access control .In Lecture notes in computer science", vol. 4296. Information Security and Cryptology—ICISC2006, November 2006 (pp. 166–178), 2006
23. Z.Guangsen, P.Manish, "Context-aware dynamic access control for pervasive applications", In Proc. communication networks and distributed systems modeling and simulation conference, San Diego, California (pp.219–225) ,January 2004
24. Y.Kim, C.Mon, D. Jeong ,"Context-aware access control mechanism for ubiquitous applications", In Lecture notes in computer science: vol. 3528. Advances in web intelligence (pp. 236–242). Berlin/Heidelberg: Springer, 2005
25. A. Ahmed, N. Zhang. "Towards the realization of context risk aware access control in pervasive computing, Telecommunication Systems", 45:127-137, 2010
26. M.Langheinrich., "A Privacy awareness system for ubiquitous computing environments", In: Proceedings of UbiComp, LNCS, 237-245, 2002
27. U. Jendriche, M. Kreutzer, "Pervasive privacy with identity management", In : Proceedings of the workshop on Security in ubiquitous computing , 2002
28. J.A.Muhtadi, R. Campbell., "Routing through the mist Privacy preserving communication in ubiquitous computing environment", In: Proceedings of the international conference on distributed computing systems , 2002
29. A.Beressford, F.Stajano., " Location privacy in pervasive computing" ,IEEE pervasive computing ,46-55, 2003
30. D.Nguyen, E. Mynatt., "Privacy mirrors: Understanding and shaping socio technical ubiquitous computing", Technical report, 2002
31. X.Liang, J.Landay, "Modelling privacy control in context aware systems" , IEEE Pervasive computing ,59-63,2002
32. M.Tentori. ,J. Favela., "Privacy aware autonomous agents for privacy healthcare", IEEE Computer Society, 55-62,2006
33. A. Al-Karkhi., A.Al-Yasiri, "Privacy,trust and identity in pervasive computing : A review of technical challenges and future research , international journal of distributed and parallel systems" , vol 3 ,2012
34. A.Lee, , J.Boyer, C. Drexelius, P.Naldurg,, R.Hill, Campbell, Supporting dynamically changing authorizations in pervasive communication systems, in the 2nd International Conference on Security in Pervasive Computing, 2005
35. J.M .Seigneur, S. Farrell, C.D. Jensen, , "Secure ubiquitous computing based on entity recognition", in the UBICOMP2002 - Workshop on Security in Ubiquitous Computing, (Goteborg, Sweden),2002
36. F. Stajano, R. Anderson, "The resurrecting duckling: Security issues for ad-hoc wireless networks". in Security Protocols, 7th International Workshop Proceedings, Lecture Notes in Computer Science, 172-194, B. Christianson, B. Crispo, and M. Roe (Eds.),1999
37. J. Al-Muhtadi, R.Hill, R. Campbell, "Context and location-aware encryption for pervasive computing environments", in the Pervasive Computing and Communications Workshops, PerCom Workshops2006. Fourth Annual IEEE International Conference on, (Pisa), 2006
38. A. Al-Karkhi and A. Al-Yasiri "Asserting User Identity in Pervasive Computing Environments Using a Non-Intrusive Technique", ISBN: 978-1-902560-24-3 , 2010 PGNet.
39. S. Creese, M. Goldsmith, B. Rosco, I. Zakiuddin, "Authentication for pervasive computing, in the Proceedings of the First International Conference on Security in Pervasive Computing, (Boppard, Germany), 2003
40. T. Grandison, M.Sloman, , "A survey of trust in internet applications", IEEE Communications Surveys and Tutorials, 3(4),2000
41. W.Wagealla, S.Terzis, "Trust based model for privacy control in context–aware systems", in the 2nd Workshop on Security in Ubiquitous Computing, Washington, USA,2003
42. L.Kagal, T.Finin, A.Joshi, Trust-based security in pervasive computing environments. IEEE Computer, 34(12), 154-157, 2001

43. Anas EL HUSSEINI, Abdallah M'HAMED, Bachar EL HASSAN, Mounir MOKHTARI, "A Novel Trust- Based Authentication Scheme for Low-Resource Devices in Smart Environments, "The 2nd International Conference on Ambient Systems, Networks and Technologies (ANT-2011), Niagara Falls : Canada, Procedia CS", vol.5, 362-369, 2011
44. M.Sharmin.S.I, Ahamed.., " SSRD+ : A Privacy aware trust and security model for resource discovery in pervasive computing environment" , 30th Annual international computer software and applications conference, 2006
45. A.Boukerche., Y.Ren., " A trust based security system for ubiquitous and pervasive computing environment, computer communications", 4343-4351, 2008
46. S.Singh, A.Katiyar, "Pervasive computing service discovery in secure framework environment", International research journal of Engineering and technology, (2018), 380- 387
47. A.Koehler, A.C. Som., "Effects of Pervasive computing on sustainable development", IEEE Technology and Society magazine, 15-23, 2005
48. Claudio Da Rold, Gilbert Vander Heiden, "Applying a Cloud First Checklist to ensure successful sourcing and Business IT Alignment", Gartner Inc, G00296404, pp: 1-22, 2016
49. Claudia Loebbecke, Bernhard Thomas, "Assessing cloud readiness: Introducing the magic metrices used by Continental AG", IFIP AICT 366, pp: 270-281, 2011
50. https://www.castsoftware.com/products/highlight
51. http://codeload.github.com/smartuni/smartpowerreader/zip/maste
52. S. Madan, "A benchmark for the artificial intelligence applications on parallel computers" , BEAP, Conference on Communications, Power and computing, WESCANEX 97 Proceedings; Winnipeg, MB; pp.: 82-87,1997
53. https://codeload.github.com/Smartuni/SmartFarm/zip/master
54. https://www.castsoftware.com/products/highlight

AUTHORS PROFILE

Ms. Vinita Malik received the Bachelor of Engineering degree from the Deenbandhu Chhotu Ram University of Science and Technology, Murthal, Haryana, India in 2008. She got her Masters of Software systems degree in 2012 from B.I.T.S Pilani Goa Campus. She is currently posted as Information Scientist at Central University of Haryana, Mahendergarh. Her research interests include risks management in various computing environments in software engineering. She has published more than 15 papers in the Journals and conferences of repute.

Dr. Sukhdip Singh received the Bachelor of Technology degree from the Maharishi Dayanand University Rohtak , Haryana, India in 1999 and the Ph.D. degree from Maharishi Dayanand University Rohtak ,Haryana India. He worked as a lecturer in Technological Institute of Textile Sciences Bhiwani Haryana from 2000-2002. He is currently a Professor in the Department of Computer Science and Engineering at Deenbandhu Chhotu Ram University of Science and Technology Murthal, Sonipat Haryana India. His research interests are in Software Engineering, Green Computing and Cloud Computing. Dr. Singh has published more than 35 papers in the Journals and conferences of repute. He serves as advisory committee member in various conferences. He is a life time member of the ISTE.