# Implementing Risk Management in Pervasive and IoT Environments

**Vinita Malik, Sukhdip Singh**

***Abstract*: *The pervasive nature of networked things envision various risks as these digital devices generate high volume of data with variable nature. The technological growth is also a product of highly interrelated complex data, so it becomes a strong argument for risks management in pervasive and internet of things environments. This research analyzes many risks present in pervasive and IoT environments. The paper elaborates various risk analysis strategies in the pervasive and IoT environments which are highly configurable in nature. The paper has implemented risk management in pervasive applications by providing risky code insights by a smart software. The risky regions of software code are analyzed by the software and managed on priority. The state of art constructs a strong case for establishing interrelationships between risks management and quality assurance in big computation environments.***

***Keywords: Attacks; Internet of Things; Risks; Risk Management; Pervasive***

## I. INTRODUCTION

The pervasive devices with connected networks have made the life easier by mobile interactions with digital devices. This technology has enabled the communications to other digital devices without context awareness. The ubiquitous environments own self adaptive nature and envisage quite complex computations which require risk management. The IoT i.e. internet of things permits wide pervasive platforms that involves the coupling of cyber physical systems. The variable relationships in automation, density and time invites requirement of risk management in the initial stages of software evolution.

The research explores pervasive and Internet of Things environments risks, strategies for risk management and challenges involved. The research has been furcated into various sections to deal with risks, attacks and their mitigation strategies in pervasive and IoT environments. Section 1 deals with Pervasive environment risks, applications and challenges. Next section elaborates Internet of things architecture, risks, attack vectors and challenges. Section 3 deals with risk management strategies in both environments.

Next section has implemented risk management in pervasive environments by providing code alerts with the help of a smart software. Last section, the research conclusions are explained with future scope.

## II. PERVASIVE COMPUTING

This section has discussed definition, risks, applications and challenges involved in pervasive computing environments.

### A. Definition

The definition of pervasive/ubiquitous computing has been proposed by Mark Weiser the methods used for increasing computer use by making various computing resources available and making the resources invisible to the user [1]. The Pervasive devices may be either the computing devices which can be carried by human beings or the infrastructure devices which may be embedded in the surrounding environments [2]. Marcia Riley has defines the pervasive computing as the calm technology in which the technology becomes virtually invisible in human beings lives. The major trends in computations today include getting transition from mainframe to desktop to again pervasive computing. This computing uses the embedded systems as well as portable devices for user's saturation with wireless environments that may include actuators/ sensors for interaction amongst human and machines. The pervasive computing capabilities have been integrated into day today life [3, 4, 5]. The complex meshed pervasive/ ubiquitous environment has been depicted in the Fig. 1 as given below [6]:

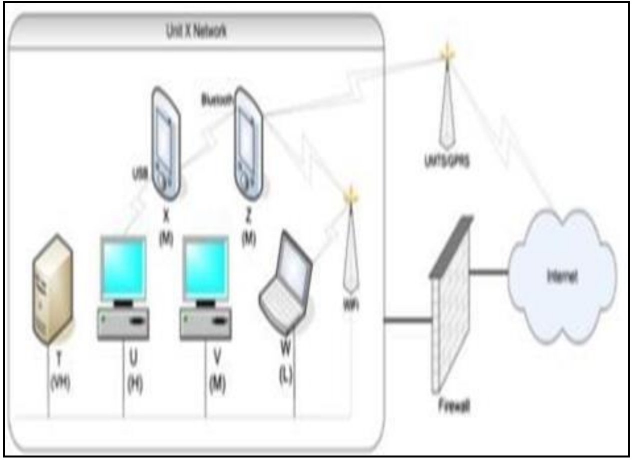


Fig.1. Environment: Evolutionary Computation

Revised Manuscript Received on October 15, 2019.

* Correspondence Author
**Vinita Malik***, PhD Scholar, D.C.R.U.S.T, Murthal & Information Scientist, Central University of Haryana, Mahendergarh, India
Email: is@cuh.ac.in
**Sukhdip Singh**, Professor, CSE Dept., D.C.R.U.S.T, Murthal, India
Email: sukhdeepsingh.cse@dcrustm.org

### B. Risks

Following are considered as the potential risks identified in pervasive computing environments [7]:

The pervasive computing risks are categorized into three main categories i.e. Social risks, Environmental risks and Human risks.

*Social Risks:*

Following are the main social risks involved in the pervasive environment:

•Undermining the privacy regulations due to ICT Identification

• ICT Networking originated computer crimes

• Isolation issues by ubiquitous information access

• ICT pervaded life for restricted consumer freedom

*Environmental Risks:*

• Miniaturization of ICT resulting into increase in toxic materials

• Power consumption increase

• Disposal Problems

• Virtual wear outs causing small product service life

• Increased Residential energy consumptions

*Human Risks:*

• NIR exposure causing health hazards

• Microelectronics causing health issues

• Active implants causing health problems

• Stress due to poor ergonomics

• Stress due to the unpredictable technical systems

### C. Applications

The application areas of pervasive computing are given as follows [8]:

•Communications: Here the pervasive technology is connected with all data transmission forms and build a precondition for information technology.

•Logistics: These are used to keep track of logistical goods and transport mechanisms.

•Motor traffic: Drivers use automobiles invisible assistance System by internetworking with other vehicles.

•Military: Used for new weapons building and cryptographic information processing by fighting with external threats.

•Production: The decentralized production systems are developed to monitor and control it.

•Smart homes: The smart homes smart technology has various devices for home lighting, heating, ventilation as well as communication.

•E-commerce: The smart objects in pervasive computing have location based services and instruct the software agents for carrying out the business transactions.

•Inner security: The smart cards are used as the identification systems i.e. in electronic passport; inner security system uses pervasive computing and in the surveillance of airports.

•Medical technology: The miniaturized, multifunctional and the medical applications are used for the smart implants.

### D. Challenges

As pervasiveness of ubiquitous technology encompasses various technologies i.e. microelectronics, sensors so there are various challenges inherent in it which have been drawn as below [9, 10]:

•Heterogeneity: For different device types, networks and environments.

•Scalability: As the number of resource increases the large scale deployments pose difficulty. Dependability and Security: It’s really difficult to maintain the reliability, safety in the mission critical systems.

• Privacy and Trust: The trust amongst mobile devices is difficult to maintain.

• Interoperability: In the pervasive computing it is cumbersome to maintain interaction among various components.

• Mobility: Providing data access anywhere anytime is a challenging task.

• Context Awareness: By user state information, finding the context information is very difficult task.

• Context Management: As per context information, modifying the system behavior by adapting to current scenarios.

• Transparent user Interaction: Very little distraction Needs are raised in pervasive environment for merging the user interface with the real world.

• Invisibility: It’s really very difficult to make computers disappear in the background in the pervasive computing.

## III. INTERNET OF THINGS

This section describes IoT (Internet of things) definition, architecture, risks, attacks and challenges.

### A. Definition

NIST defines IoT as the connected objects in networked infrastructure which interact with the physical world by sensors. This kind of infrastructure further enables data processing, storage and transportation [11].

IoT capabilities encompass various data processing, storage, transmission by interfacing and sensing. ITU-T expounds IoT as the universal framework for the whole society which enables the resources by virtual interconnections and by the help of interoperable data communication technology [12].

### B. Architecture

The architecture for IoT should be open using protocols to support various network applications. The IoT architecture must be adaptable, secure and data integration promoted [13].

The architecture is made of the following layers:

• Perception-Layer: It has embedded sensor technology, Nano technology, embedded intelligence for objects identification and information gathering from outside world.

• Network-Layer: It comprises of wireless sensor technology, fixed networks, 2G/3G communications, and IP networks. Information from various devices/sensors is transferred to information processors from this layer.

• Support-Layer: This layer is quite close to application layer and comprises of information processors.

- Application-Layer: All practical applications are developed as per user requirements.

The architecture for internet of things is given below in the Fig. 2 as below[14]:

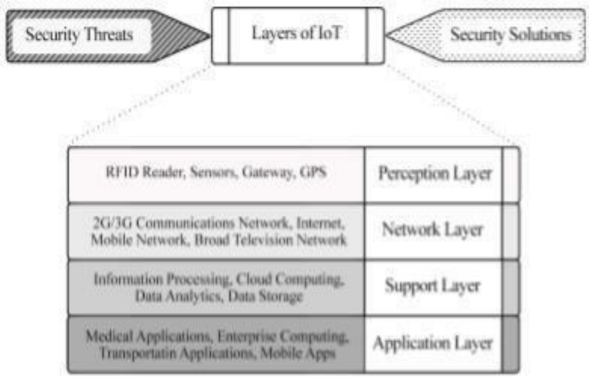

Security Threats
Layers of IoT
Security Solutions
RFID Reader, Sensors, Gateway, GPS
Perception Layer
2G/3G Communications Network, Internet, Mobile Network, Broad Television Network
Network Layer
Information Processing, Cloud Computing, Data Analytics, Data Storage
Support Layer
Medical Applications, Enterprise Computing, Transportatin Applications, Mobile Apps
Application Layer

Fig. 2: Architecture: IoT (Internet of Things)

### C. Risks

The IoT risk factors are described as below [15]:

- Forge Attacks
- Network Routing
- Buffer Overflow
- DoS attack
- Defect Expose
- Information Leakage
- Channel block
- Node Access
- Network Vulnerability
- Password Vulnerability
- Physical Attacks

### D. Attacks

Following attack vectors or threats exist in IoT environment [16]:

- Viruses
- Phishing
- Credential Harvesting
- Web attacks
- Weak Passwords
- Zero day
- Hypervisor Breach BIOS/Hardware
- Weak Cryptography
- Spear Phishing
- Network Breach (Firewall, Router)
- Two Factor Compromise

### E. Challenges

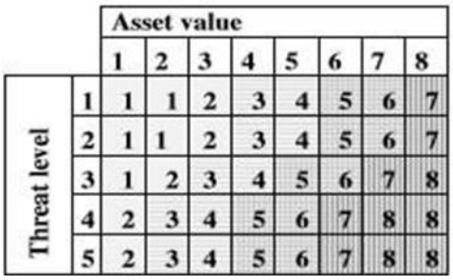
Various types of challenges i.e. Efficiency, reliability, scalability, availability, interoperability, storage and security challenges exist in internet of things [17]. The scalability challenges have poor response time and bad analytics. As the interconnected devices increase in number and the technology changes frequently the IoT scalability issues arise which are bad process linkages at organizational level, unclear information transmission, data exchanges and the legislation issues, transmission protocols, infrastructure and device linkage issues. Reliability challenges encompass bad system architecture, underdeveloped system and transfer level issues [18]. Efficiency challenges are linked to incompetent machine learning procedures and real time data analysis issues. Availability challenges needs to satisfy the need of connecting any network, any place, any service, any time and anything [19]. Data storage issues in IoT have virtualization, variability, veracity, velocity, volume, value, validity, volatility and variety issues. IoT security assurance, the care of information, operational, physical and IT security issues are taken [20].

## IV. RISK MANAGEMENT STRATEGIES IN PERVASIVE & IOT ENVIRIONMENTS

This section describes risks management in pervasive and Internet of things environment.

Various types of models have been proposed in past for risk assessment and management in pervasive environments. As risk management tells how to identify the computing environment risks and how to assess them , finally how to mitigate risks. The computer crime and abuse survey indicates that 42% (around) respondents experience mobile devices theft, out of which 6% incurs intellectual property loss [21]. Various risk assessment methods i.e. MEHARI, CRAMM and OCTAVE have been used for risks assessment for mobile devices [22-24]. First, the asset values, threats and vulnerabilities are identified and then further categorization is done. Once categorization process gets completed the asset value categories, threats, vulnerabilities are calculated to further mitigate them. Once risk calculation process is over, adaption through community is done to mitigate them [25]. The temporary risk matrix has been given in the Table 1[25].

Table 1: Risk Matrix



| | | Asset value | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| Threat level | 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 pervasive environment, the risk probabilities are associated with the degree of interaction amongst the computing devices for which the following formula is given [26]:

$$Pi = F(Xi) + Zi \quad \ldots\ldots\ldots\ldots \quad (1)$$

Where

Pi = Risk Probability Distribution Xi

Zi=Random Distribution Vector

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

The IoT complex data nature asks for continuous risk assessment. The IoT generated data is considered as private and requires more attention as well as privacy controls [27]. The security and privacy risks should be managed by best risk management strategies. The todays risk management methodologies are not sufficient for IoT because of very less periodic assessment, less knowledge and not targeting the unknown aspects of system. Risk management in IoT is dealt in four steps. First is the risk assessment building where all the system characteristics are identified? Second is to find all the risks/ vulnerabilities and third is by calculating risks by finding asset risks as well as the propagation probability. Once all the risks levels obtained then risk control recommendations have been followed properly. Risk management strategies in IoT has Encryption & Authentication, RFID 2 way Authentication , cloaking greedy algorithm, K- anonymity, EBIOS ,OM-AM model, HMG ISI method, Block chains, RPL protocol, DRAMIA method, adaptive risk aware privacy aware RBAC and the algorithm of association rules.

## V. IMPLEMENTATING RISK MANAGEMENT FOR A PERVASIVE/SMART APPLICATION

This section describes how risks may be managed for a pervasive application by smart software after identifying code alerts and risky code regions. The pervasive application Prophet has been taken from GitHub repository [28]. A smart vendor has been utilized for identifying the riskiest items of the application scanned [29]. The smart application is scanned first by the smart software and the risk distribution is found as per technology, software resiliency, agility and elegance as depicted in the Fig. 3 below:

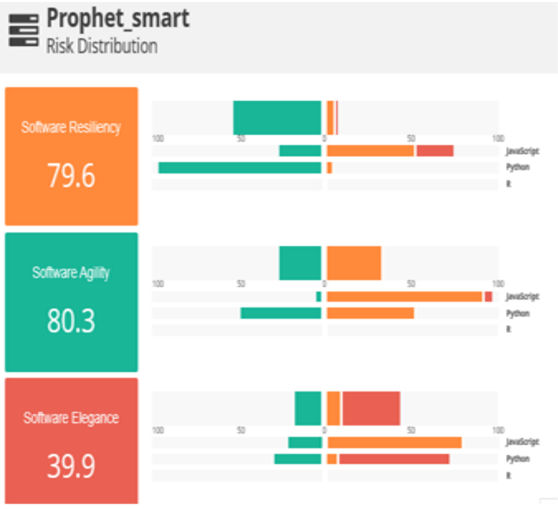
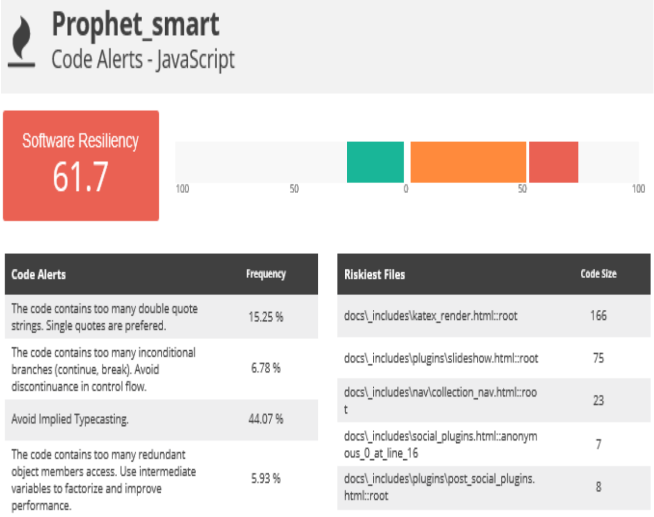


Fig. 3. Risk distribution technology wise

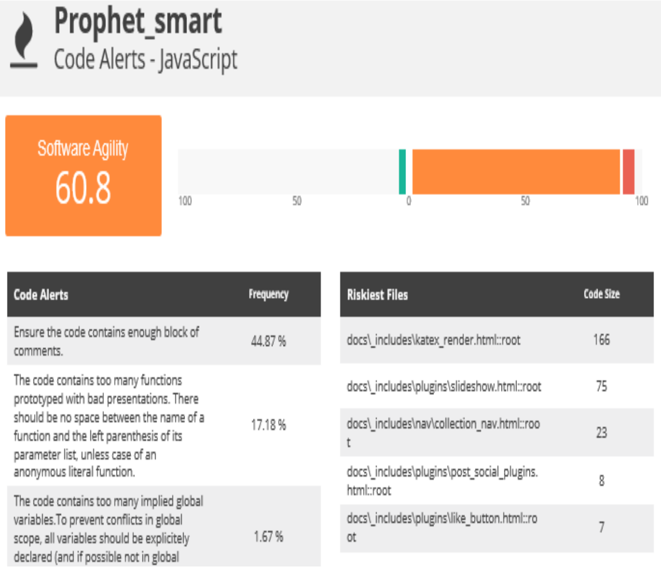
Once the risks distribution is identified, the riskiest items of application scanned are identified by code alerts. The code alerts for various technologies used in the application scanned, have been depicted in Fig.4, 5, 6 as per software resiliency , agility and elegance.



| Code Alerts | Frequency |
|---|---|
| The code contains too many double quote strings. Single quotes are prefered. | 15.25 % |
| The code contains too many inconditional branches (continue, break). Avoid discontinuance in control flow. | 6.78 % |
| Avoid Implied Typecasting. | 44.07 % |
| The code contains too many redundant object members access. Use intermediate variables to factorize and improve performance. | 5.93 % |

| Riskiest Files | Code Size |
|---|---|
| docs_includes\katex_render.html::root | 166 |
| docs_includes\plugins\slideshow.html::root | 75 |
| docs_includes\nav\collection_nav.html::root | 23 |
| docs_includes\social_plugins.html::anonymous_0_at_line_16 | 7 |
| docs_includes\plugins\post_social_plugins.html::root | 8 |

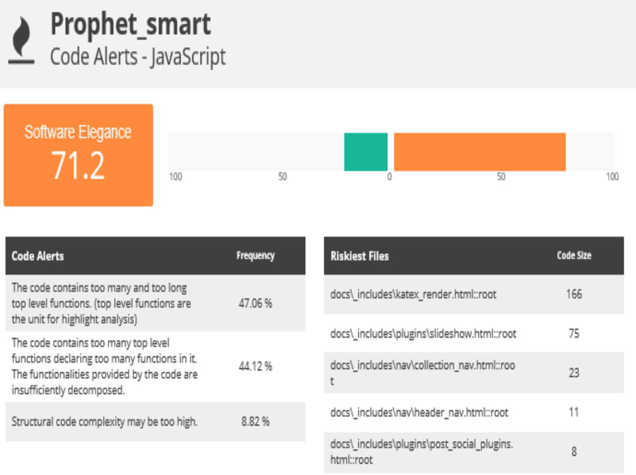
Fig. 4. Code Alerts as per software resiliency and JavaScript Technology



| Code Alerts | Frequency |
|---|---|
| Ensure the code contains enough block of comments. | 44.87 % |
| The code contains too many functions prototyped with bad presentations. There should be no space between the name of a function and the left parenthesis of its parameter list, unless case of an anonymous literal function. | 17.18 % |
| The code contains too many implied global variables.To prevent conflicts in global scope, all variables should be explicitely declared (and if possible not in global | 1.67 % |

| Riskiest Files | Code Size |
|---|---|
| docs_includes\katex_render.html::root | 166 |
| docs_includes\plugins\slideshow.html::root | 75 |
| docs_includes\nav\collection_nav.html::root | 23 |
| docs_includes\plugins\post_social_plugins.html::root | 8 |
| docs_includes\plugins\like_button.html::root | 7 |

Fig. 5. Code Alerts as per software agility and JavaScript Technology



| Code Alerts | Frequency |
|---|---|
| The code contains too many and too long top level functions. (top level functions are the unit for highlight analysis) | 47.06 % |
| The code contains too many top level functions declaring too many functions in it. The functionalities provided by the code are insufficiently decomposed. | 44.12 % |
| Structural code complexity may be too high. | 8.82 % |

| Riskiest Files | Code Size |
|---|---|
| docs_includes\katex_render.html::root | 166 |
| docs_includes\plugins\slideshow.html::root | 75 |
| docs_includes\nav\collection_nav.html::root | 23 |
| docs_includes\nav\header_nav.html::root | 11 |
| docs_includes\plugins\post_social_plugins.html::root | 8 |

Fig. 6. Code Alerts as per software Elegance and JavaScript Technology

Here once the code alerts and their frequency are identified, the location of riskiest files which need to be handled on priority are taken care off, thus reducing the application risks.

## VI. CONCLUSIONS & FUTURE SCOPE

The research has successfully explored risks, attacks, risk management strategies in pervasive and internet of things environment. Due to ubiquitous and mobile nature of these software's, it's essential to manage the software risks to assure their quality. The paper has used a smart vendor solution for identifying the riskiest items of a pervasive application and therefore can reduce the risks by either removing those files or reducing the frequency of risky code size. This research will prove a foundation for establishing interrelations between risk management and quality assurance in the ubiquitous and highly networked environments i.e. Internet of things.

## REFERENCES

1. A. A. H. Mousa, "Ubiquitous/Pervasive Computing" , International Journal of Innovative research & development , vol 2 , 2013, pp. 276-282
2. M.Weiser, "The computer for the 21st century, Scientific American", 265(No. 3),1991, pp.94 –104
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, 2007, pp. 172-178
7. L.M.Hilty, C.Som , " Assessing the Human, Social and Environmental risks of pervasive computing" ,Human and Ecological Risk Assessment , 10, 2004, pp. 853-874
8. J.Sen, "Ubiquitous Computing: Applications, Challenges and future trends", 2012, pp. 1-41
9. B. Abdulrazak., Y. Malik, "Review of challenges, Requirements and approaches of pervasive computing system Evaluation", IETE Technical Review, 29,6, 2012, pp.506-522
10. C.A.D Costa., "Towards a general software Infrastructure for ubiquitous Computing, Journal of Pervasive Computing", IEEE CS, 2008, pp.64-73
11.https://csrc.nist.gov/CSRC/media/Presentations/NIST-Cybersecurity-for-IoT-Program/images/media/NIST%20Cybersecurity%20for%20IoT%20Program.pdf, 20th August,2018, pp. 1-8, 2018
12. E. Leloglu, "A review of Security concerns in internet of things", Journal of Computer and Communications, 5, 2017, pp. 121-136
13. J.An. , X.L. Gui, X. He, "Study on architecture and key technologies for Internet of things", Advances in Biomedical Engineering, 11, 2012, pp. 329-335
14. E. Leloglu, "A review of Security concerns in internet of things," Journal of Computer and Communications, 5, pp.121-136, 2017
15. W.Tianshu, Z. Gang, "A novel Risk assessment model for privacy security in internet of things", vol 19, no 5, 2014, pp.398-404
16. G. Sorebo, "Managing the unmanageable : A risk model for the Internet of Things", RSA Conference, https://www.rsaconference.com/writable/presentations/file_upload/grc-r01- managing-the-unmanageable-a-risk-model-for-the-internet-of-things.pdf, 2015, pp.1-20
17. M. Mircea, M. Stocia, Ghilic-Micu, "Using Cloud computing to address challenges raised by internet of things", Computer communications and networks, Connected environments for internet of things, springer, 2017, pp.63-82
18. J. Kempf , J.Arkko , N. Beheshti, K. Yedavalli, "Thoughts on reliability in the internet of things", March 2011. https://www.iab.org/wp-content/IAB-uploads/2011/03/Kempf.pdf, accessed 3 Feb 2017, 2011, pp.1-4
19. B. Bagula , "A: Internet-of-things and big data: promises and challenges for the developing world", http://unctad.org/meetings/en/Presentation/ecn162016p16_BagulaUWC_en.pdf. Accessed 3 Feb 2017, 2017, pp.1-20
20. R. Liwei, " IoT security: problems, challenges and solution", http://www.snia.org/sites/default/files/DSS-Summit-2015/presentations/LiweiRen_Iot_Security_Problems_Challenges_revision.pdf. Accessed 20 Jan 2017, 2017, pp.1-32
21. R. Richardson., "CSI Computer Crime and Security Survey", Computer Security institute, 2009
22. Carnegie Mellon University, http://www.cert.org/octave/download/intro.html
23. Clusif, http://www.clusif.asso.fr/fr/production/ouvrages/pdf/MEHARI-2010-Overview.pdf, 2010
24. Insight Consulting, http://dtps.unipi.gr/files/notes/2009-2010/eksamino_5/politikes_kai_diaxeirish_asfaleias/egxeiridio_cramm.pdf, 2009
25.T. Ledermuller, N.L.Clarke, "Risk assessment for mobile devices", Lecture notes in computer science, pp.210-221, 2011
26. F.Liu, Y.Chen., K.Dai., Z.Wang, " Research on risk probability estimating using fuzzy clustering for dynamic security assessment" ,LNAI,3642,pp. 2005, 539-547
27. https://www.gartner.com/smarterwithgartner/make-privacy-a-top-priority-for- your-iot-project/, 25th August 2018
28. Prophet, https://codeload.github.com/facebook/prophet/zip/master, 2018
29. Cast Software, www.castsoftware.com, 2019

## AUTHORS PROFILE

**First Author** Ms. Vinita Malik did the Bachelor of Engineering degree from M.D.U, Rohtak, India in 2008. She completed Masters of Engineering in 2012 from B.I.T.S Pilani University, Rajasthan. She is currently working as Information Scientist at Central University of Haryana, Mahendergarh. She is also pursuing PhD in Computer Science && Engineering from D.C.R.U.S.T, Murthal. Her research interests include Software engineering – Risks Management and Testing. She has published 17+ papers in the reputed Journals and conferences.

**Second Author** Dr. Sukhdip Singh did the Bachelor of Technology degree from the M.D.U, Rohtak, Haryana, India in 1999 and the Ph.D. degree from Maharishi Dayanand University Rohtak, Haryana India. He is currently working as a Professor in the Department of Computer Science and Engineering at D.C.R.U.S.T, Murthal. His research interests include Software Engineering, Green Computing and Cloud Computing. Dr. Singh has published 35+ papers in the reputed Journals and conferences. He is a life time member of the ISTE.