# Privacy & Security of Mobile Cloud Computing

Manmohan Chaturvedi[*,1] , Sapna Malik[2], Preeti Aggarwal[3] and Shilpa Bahl[4]
Ansal University, Sector 55,Gurgaon- 122011, India
[1]mmchaturvedi@ansaluniversity.edu.in [2] sapnadhankhar@gmail.com
[3] preetaggarwal@gmail.com,[4] gerashilpa@gmail.com

## Abstract

The Indian government, like governments elsewhere in the world, has chosen mobile device as preferred platform to engage with citizens while offering various e-Governance services. Likewise there is huge market for mobile based e-Commerce applications across the globe. However uptake of these services is challenged by the security and privacy concerns of the end user. The limited processing power and memory of a mobile device dependent on inherently unreliable wireless channel for communication and battery for power leaves little scope for a reliable security layer. Thus there is a need for a lightweight secure framework that provides security with minimum communication and processing overhead on mobile devices. The security and privacy protection services can be achieved with the help of secure mobile-cloud application services. Taking support from a proximate cloud a security service could be devised for a mobile device which works as an interface and adaptively provides optimum security solutions based on communication channel capacity, available system resources both hardware and software and user-defined QoS parameters. We plan to explore and experiment with available options to recommend security and privacy enhancing approaches that may meet the security need for mobile application using automated sensing of the context.

**Key Words:** Mobile Security, Adaptive Security, m-governance, m-commerce, Privacy and Security

## 1. Introduction

Mobile Cloud Computing (MCC) is combination of two terms, mobile computing and cloud computing. Mobile computing is provision of applications on mobile devices. Cloud computing refers to getting paid services either in the form of infrastructure, platform or software through internet based cluster of distributed servers. Mobile cloud computing is provision of mobile applications using cloud to give more power to mobile devices towards computing, in spite of resource limitations in mobile devices. Mobile cloud computing is a concept that has been in use since 2009 and is still evolving.

There are various known challenges in the field of MCC viz. handover delay, bandwidth limitation, task division for offloading, reliability, integrity of data delivered, scalability of MCC without degradation in performance or change in infrastructure, security of data in mobile device within a cloud and in the communication channel, identity privacy, location privacy, etc. These challenges are the biggest obstacles in growth of mobile cloud computing. According to the literature [1,2] 74% of IT Executives and Chief Information Officers are not willing to adopt cloud services due to the risks associated with security and privacy. In MCC the security threats are likely in various segments viz. mobile device, communication channel or the cloud itself. So one has to provide protection from these threats by having secure cloud application services in mobile devices and cloud, secure routing protocols in communication channel and secure virtualization in cloud architecture. According to review of the current approaches in MCC [3], the security framework for MCC is divided into two categories; Data Security framework and Application Security Framework. Data Security frameworks are compared on the basis of their basic theory –mathematical principle or cryptographic principle, data protection –protection of data created or manipulate on device or data created or manipulate on cloud, data integrity, scalability, assumption of components-fully trusted, semi trusted or distrusted, data access automated or semi automated and authentication of originator of file. Application security framework can be compared on the basis of application type, security features like data security, integrity, identity privacy, location privacy, authentication, secure data access

[*] Corresponding author : MM Chaturvedi (email :mmchaturvedi@ansaluniversity.edu.in , +919871078151 (m) )

management or secure routing, assumption of component trust levels, scalability of framework. Each security framework must be viewed with its security strength and resource usage. In security strength we take care of confidentiality, integrity, authentication parameters. In resource usage we consider memory usage, processing time and network overhead parameters [4].

In this paper, section 2 reviews the related literature on cloud computing, MCC and various security aspects of mobile and cloud computing. Section 3 deals with the overall architecture of the proposed plan elaborating on need of cloud computing in 3.1, features of mobile cloud computing in 3.2, objective in 3.3. Section 4 describes the possible validation approaches to test the design objective. Section 5 lists out the challenges involved in the research objectives whereas section 6 concludes the paper highlighting the possible outcome of this research work.

## 2. Related Work

Security and privacy issues of MCC have been discussed by many researchers. J. Oberheide et al [5] proposed Cloud AV platform, malware detection system for mobile device by moving detection capabilities to network service or cloud. Zhang et al [6] present security framework for elastic mobile application model by dividing an application into easily configurable weblets. Xiao and Gong [7] proposed scheme for mobile cloud environment to generate a dynamic credential for mobile user for their identity protection from hackers. Wang and Wang [8] have proposed privacy preserving framework for mobile devices while using location based scheme by spatial cloaking. Huan et al [9] presents framework –MobiCloud to enhance the functionality of MANET and cover security aspect in terms of risk management and secure routing. G. Portokalidis et al [10] proposed scheme for threat detection in a smart phone with Mobile Cloud Computing. H.Zhang and X Mingjun [11] proposed distributed spatial cloaking protocol for location privacy. P.Zou et al[12] propose Phosphor, a cloud based mobile digital right management scheme with Sim Card by designing License state word . R.Chow et .al [13] present policy based cloud authentication platform using implicit authentication for solving privacy issues. Itani et al.[14] proposed an energy efficient framework for mobile devices by using incremental message authentication code to ensure integrity of mobile users. Jia et al[15] presents proxy re-encryption (PRE) scheme and identity based encryption (IDE) scheme to achieve secure data service. Huangs et al.[16] proposed secure data processing framework for MobiCloud addressing issue of authentication on cloud. Hsueh et al [17] Proposed authentication mechanism to ensure security and integrity of mobile users files stored on cloud server. Yang et al.[18] extended the public provable data possession scheme with Diffie Hellman Key Exchange, Bilinear mapping and Merkle Hash Tree (MHT). Chen et al [19] present security framework for location based grouped scheduling services for identity privacy and authentication. Ren et al [20] proposed three schemes; encryption based, coding based and sharing based to ensure the confidentiality and integrity of user's file stored at cloud. Zhou and Huang [21] proposed a privacy preserving framework by offloading the processing and storage intensive encryption and decryption on cloud based on Cipher text Policy attribute. Current research initiatives seem to address only one or two parameters of security from the comprehensive set of authentication, integrity, confidentiality and privacy. These research approaches favor static security algorithms without considering changing demand for security, quality of service, and resource usage of mobile users.

## 3. Architecture of the model proposed to be explored

### 3.1 Cloud Computing

The Cloud Computing is gaining popularity with its main advantage of reducing the computational burden of the client and thus reducing the complexity and other infrastructure requirements at the client end. However, it is important to realize that the market is still deprived of cloud service providers because of following important issues:

- Data replication
- Consistency
- Limited scalability
- Unreliability
- Unreliable availability of cloud resources
- Portability
- Trust
- Security
- Privacy

The commonly accepted definition of Cloud computing is an IT service being provided to users on demand and being paid for depending upon amount of usage. It can also be termed as a dynamic service being provided to users that can

add on to the available capacity and capabilities of user entity. Some of the key services of Cloud Computing as depicted in Figure 1 are:

- Infrastructure as a Service (IaaS)
- Data storage as a Service (DaaS)
- Communication as a Service (CaaS)
- Security as a Service (SecaaS)
- Hardware as a Service (HaaS)
- Software as a Service (SaaS)
- Business as a Service (BaaS)
- Platform as a Service (PaaS)
- Virtualization

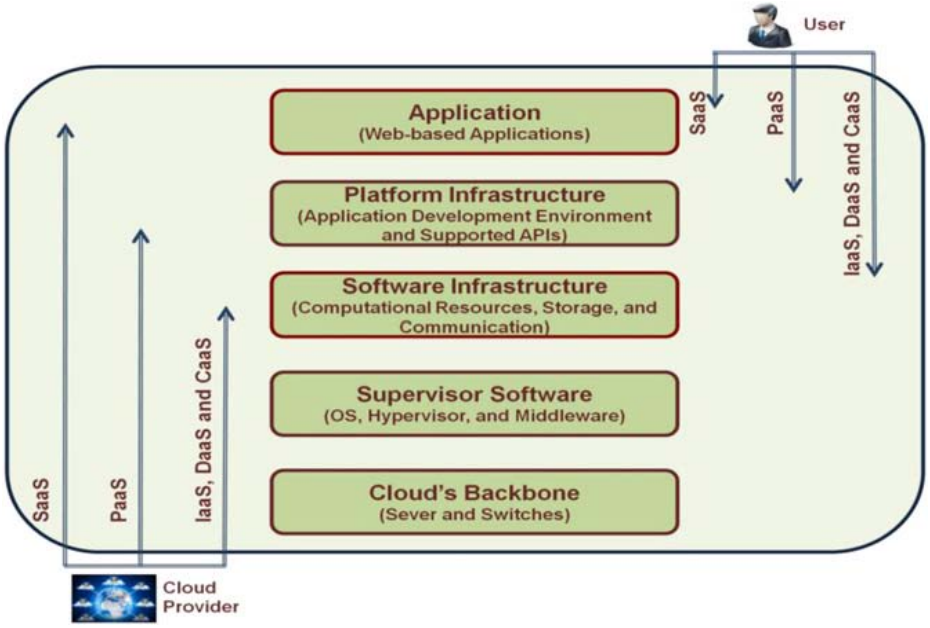


Fig. 1. Layered Architecture of Cloud Computing [3]

### 3.2 Mobile Cloud Computing

The application of cloud is possible in many domains. One of the domains of our current interest is that of mobiles. Hence, we will be focusing on utility of cloud computing environment for mobile usage and how can a cloud add value to the overall functionality and performance of mobile devices? According to Khan et al [3] as depicted in figure 2, MCC is a service that allows resource constrained mobile users to adaptively adjust processing and storage capabilities by transparently partitioning and offloading the computationally intensive and storage demanding jobs on traditional cloud resources by providing ubiquitous wireless access.

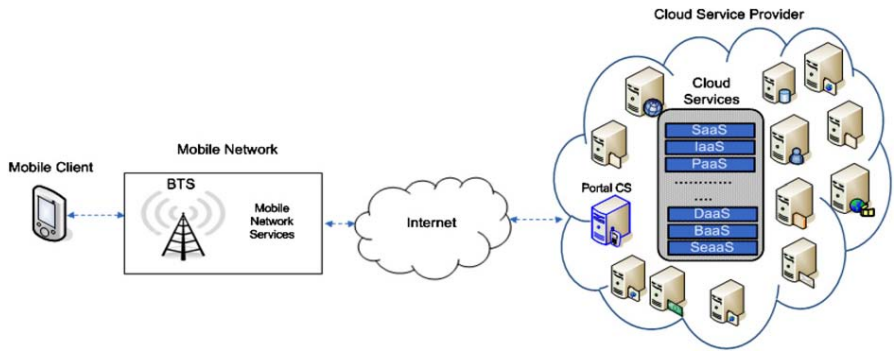


Fig. 2. Mobile Cloud Computing Architecture [3]

Some of the limitations of mobile devices which drive use of Cloud Computing for mobile devices are:

- Limited battery
- Limited processing power
- Low storage
- Less security
- Unpredictable Internet connectivity
- Less energy

### 3.3 Research Objective

Our research objective is to propose and develop a system in which security protocols can be decided for a mobile entity dynamically in a cloud. For this, we will be focusing on not just the mobile security parameters but also on the cloud security related issues and respective parameters. As suggested by Khan et al [3], the security and privacy protection services can be achieved with the help of secure cloud application services. Figure 3 describes the security services necessary at various layers of the supporting cloud. In addition to security and privacy, the secure cloud application services provide the user management, key management, encryption on demand, intrusion detection, authentication, and authorization services to mobile users. There is a need for a secure communication channel between cloud and the mobile device. The secure routing protocols can be used to protect the communication channel between the mobile device and cloud.

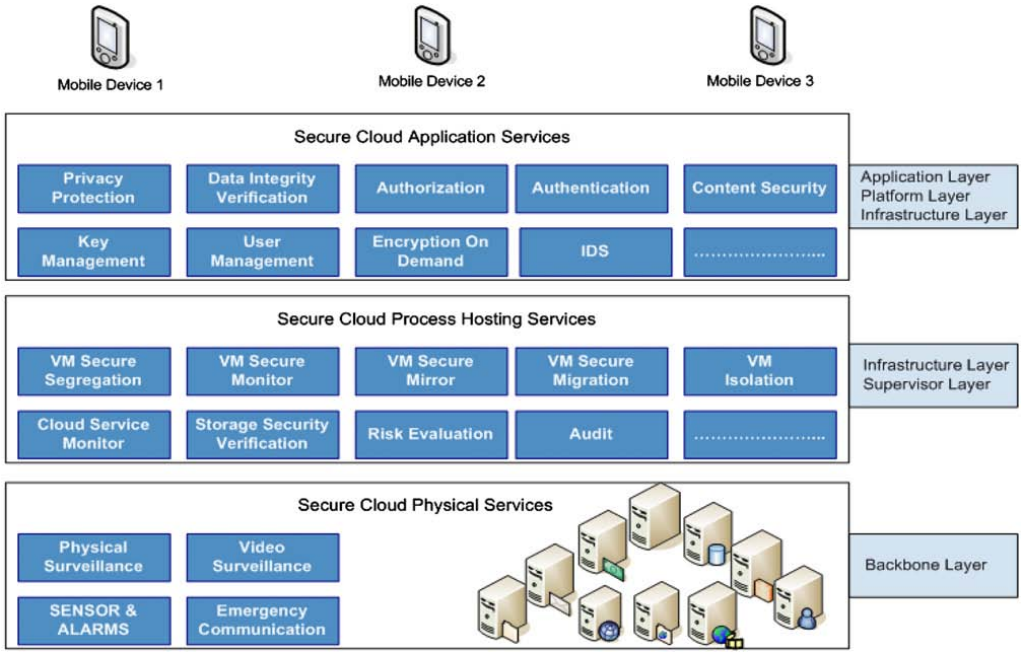


Fig. 3. Security services on different layers [3].

The key illustrative areas of proposed research are:

- Preparation of semantic data for security parameters
- Cloud Security attributes
- Mobile Security features and respective parameters
- Security protocols under different security requirements
- Platform Independent Security Architecture.

In the work of Khan et al [3], frameworks of various aspects of security features have been described in detail. As suggested by Rocha et al [4], a security service can be devised which works as a middleware with the ability to change the security protocols dynamically between two peers. In their work, domain is of independent mobile users.

We propose to expand this concept to a cloud where a number of mobile users will be acting as members of the cloud and will exchange information within the cloud. For this we need to define various levels of security. A mobile may require different levels of security at different times depending upon the service being used and the sensitivity of the data exchanged with the peer.
Broadly the proposed research could address following questions:

a) What could be semantic data for mobile and cloud security?
b) How the Protocol Selection Procedure can be made intelligent with option for static protocol selection when necessary?
c) How workload could be partitioned between mobile and cloud after factoring various related issues?

The following options need to be evaluated to arrive at a possible mix to answer the framed research questions:

a) As proposed by Zissis & Lekkas [22], a trusted third party could be tasked with assuring specific security characteristics within a cloud environment.
b) Identification of appropriate security parameters for a mobile and cloud with their dependency matrix to suggest a security metric towards security of a mobile cloud computing application.
c) Generation of semantic data which facilitates selection of the security protocol by the middleware. Intelligent protocol selection process would help conserve resources. This would permit use of already selected protocol if the semantic data values are unchanged.
d) If the security requirement between two peers is same over a period of time, then repeated overhead of security parameter collection and protocol selection for every information exchange can be avoided by choosing the relevant security protocol for stipulated time duration before entering dynamic protocol selection mode as necessary.
e) Security related work could be partitioned between the mobile and the cloud with computationally light tasks handled by the mobile itself and heavy tasks outsourced to the cloud.

## 4. Proposed Validation approaches

Validation is done at the end of the development process and takes place after verifications are completed i.e. determining if the system complies with the requirements and performs functions for which it is intended and meets the stated goals and user needs [23].
The validation of the proposed research is to establish that it is adaptive in nature for several contexts and leads to benefits both in performance and ease to use and according to the type of user dependent data transfer. The designed software should permit the application to determine different semantic values for each part of the data to be transmitted, and thus addresses the main concern of the user viz. enhanced security.

*Cloud based Mobile Computing Testing practices:-*

It is important to take into consideration the additional time and/or personnel needed to perform exhaustive tests on all the devices eg according to Rocha & Costa[4] in the proposed middleware which is a system software responsible for managing the transparent execution and interaction among the jobs running on the cloud servers, it is mandatory to test these system software like OS and Hypervisor of the cloud .So the types of testing that is to be planned for the cloud system software are, Performance Testing, Capacity Testing, Fail-over Testing, Browser testing[24]

- **Application security testing**. This type of testing is done to secure application software that is running on or being developed in the cloud.
- **Governance Risk Compliance (GRC) testing.** Its main focus is to list threats, vulnerabilities and risks that are associated to all three parts of Cloud Computing – Infrastructure as a Service (IaaS), Platform as a Service (PaaS) & Software as a Service (SaaS) and suggest controls which have been assimilated from the best practices prevailing in the Industry.
- **Latency Testing.** Cloud testing is utilized to measure the latency between the action and the corresponding response for any application after deploying it in the cloud.

*Issues and Challenges in Cloud Testing*

There are a number of issues and challenges in testing clouds and cloud-based software. Here we discuss them from the following four areas.

- *On-demand test environment construction* – How to set up a testing environment systematically (or automatically) for on-demand testing services in a cloud? Although the current cloud technologies support automatic provision of required computing resources for each SaaS (or application) in a cloud, there are no supporting solutions to assist engineers to set up a required test environment in a cloud using a cost-effective way. It is necessary to provide an on-demand test environment for TaaS customers, Iaas customers, Daas customers etc.

- *Scalability and performance testing* – Although many published papers discuss system performance testing and scalability evaluation in the past two decades, most of them address issues and solutions in conventional distributed software or web-based software systems. According to our recent literature survey on this subject, most existing papers focus on scalability evaluation metrics and frameworks for parallel and distributed systems.

- *Testing security and measurement in clouds* – Security testing has becoming a hot research subject with many open questions in current software testing community. Since security becomes a major concern inside clouds and security services become a necessary part in modern SaaS and cloud technology, engineers must deal with the issues and challenges in security validation and quality assurance for SaaS and clouds.

## 5. Key Challenges in the proposed research

The key challenges that we anticipate are:

a) During experimentation the simulator being used should acquire necessary information from both the OS and through the wireless medium.
b) Balance between security and maintaining communication quality and system performance.
c) We should provide a single security layer for different contexts of hardware, software and communication modes.
d) Need for the data semantics so as to determine different sensitivity levels of the data being transmitted, facilitating strong security mechanism only when they are actually needed rather than on the whole data.
e) In the proposed approach the appropriate metrics and the parameters should be defined to facilitate objective evaluation of our approach.
f) Design of a Platform Independent Security Architecture so that we can deploy lightweight part of security Framework on any Mobile device could pose interface issues.

## 6. Concluding Remarks

This paper has attempted literature review of various approaches for effective deployment of secure mobile cloud computing paradigm.
Challenges and possible options have been delineated while we try to explore and characterize an adaptable and dynamic framework providing configurable security interface at the application layer.
Issue connected with validation and testing of proposed solution have also been considered to help us formulate dependable testing and benchmarking of a security firmware in the context of mobile cloud computing.
The fallout of the proposed research is expected to be of interest to both E-governance and E-commerce applications. The challenges in this evolving field of research are many and we plan to proceed in phases with first phase attempting to characterize the problem in formal terms and propose a lightweight mobile interface having limited dynamic capability. Later phase may attempt expanded objectives.

## References

1. Subashini,S. ,Kavitha,V.: A survey on security issues in service delivery models of cloud computing, Journal of Network and Computer Applications 34 (1) 1–11 (2011).
2. Buyya,R.,Yeo C.S.,Venugopal,S., Broberg,J.,Brandic I.: Cloud computing and emerging IT platforms: vision, hype, and reality for delivering computing as the 5th utility, Future Generation Computer Systems 25 (6) (2009) 599–616
3. Khan,A.,N.,Mat Kiah,M.,L., Khan S.,U.,Madanic,S.A. :Towards secure mobile cloud computing: A survey, Future Generation Computer Systems 1-22 (2012)
4. Bruno P.S.Rocha,Daniel N.O.Costa,RandeA.Moreira,ristianoG.Rezende,Antonio A.F.Loureiro, Azzedine Boukerche : Adaptive security protocol selection for mobile computing, Journal of Network and Computer Applications (2012)
5. Oberheide,J., Veeraraghavan,K., Cooke, E., Flinn, J., and Jahanian, F.. :Virtualized in-cloud security services for mobile devices, in Proceedings of the 1st Workshop on Virtualization in Mobile Computing (MobiVirt), pp. 31-35, (June 2008).
6. Zhang, X., Schiffman, J. , Gibbs ,S., Kunjithapatham, A., Jeong, S.: Securing elastic applications on mobile devices for cloud computing, in Proceeding ACM workshop on Cloud computing security, CCSW ’09, Chicago, IL, USA,( Nov. 2009.)
7. Xiao, S., Gong, W.: Mobility can help: protect user identity with dynamic credential, in: Proc. 11th Int. Conference on Mobile Data Management, MDM ’10, Missouri, USA,(May 2010)
8. Wang, S., Wang, X.S.: In-device spatial cloaking for mobile user privacy assisted by the cloud, in: Proc. 11th Int. Conference on Mobile Data Management,MDM ’10, Missouri, USA,( May 2010).
9. Huan,D., Zhang, X., Kang ,M., Luo ,J.: MobiCloud: building secure cloud framework for mobile computing and communication, in: Proc. 5th IEEE Int. Symposium on Service Oriented System Engineering, SOSE ’10, Nanjing, China,(June 2010).
10. Portokalidis,G.,Homburg,P.,Anagnostakis,K., Bos,H.: aranoid Android: versatile protection for smartphones, in Proceedings of the 26th Annual Computer Security Application Conference (ACSAC), pp. 347-356, (September 2010).
11. Zhangwei ,H. and Mingjun ,X., : Distributed Spatial Cloaking Protocol for Location Privacy, in Proceedings of the 2nd International Conference on Networks Security Wireless Communications and Trusted Computing (NSWCTC), vol. 2, pp. 468,( June 2010.)
12. Zou,P., Wang,C., Liu ,Z., and Bao ,D.,: Phosphor: A Cloud Based DRM Scheme with Sim Card, in Proceedings of the 12th International Asia-Pacific on Web Conference (APWEB), pp. 459, (June 2010).
13. Chow, R., Jakobsson, M., Masuoka, R., Molina, J., Niu Y., Shi ,E., Song, Z. :Authentication in the clouds: a framework and its application to mobile users, in: Proc. ACM Cloud Computing Security Workshop, CCSW ’10, Chicago, USA,(Oct. 2010.)
14. Itani,W., Kayssi,A., Chehab, A.: Energy-efficient incremental integrity for securing storage in mobile cloud computing, in: Proc. Int. Conference on Energy Aware Computing, ICEAC ’10, Cairo, Egypt, (Dec. 2010.)
15. Jia,W., Zhu ,H., Cao, Z., Wei, L., Lin, X.,:SDSM: a secure data service mechanism in mobile cloud computing, in: Proc. IEEE Conference on Computer Communications Workshops, INFOCOM WKSHPS, Shanghai, China,(Apr. 2011).
16. Huang,D., Zhou,Z., Xu,L., Xing,T., Zhong,Y:Secure data processing framework for mobilecloud computing, in: Proc. IEEE INFOCOM Workshop on Cloud Computing, INFOCOM ’11, Shanghai, China, (June 2011.)
17. Hsueh ,S.,C., Lin ,J.Y., Lin, M.Y.,: Secure cloud storage for conventional data archive of smart phones, in: Proc. 15th IEEE Int. Symposium on Consumer Electronics,ISCE ’11, Singapore, (June 2011.)
18. Yang ,J., Wang, H., Wang, J., Tan, C., Yu1, D.: Provable data possession of resource constrained mobile devices in cloud computing, Journal of Networks 6 (7) 1033–1040 (2011).
19. Chen,Y.,J., Wang,L.,C.: A security framework of group location-based mobile applications in cloud computing, in: Proc. Int. Conference on Parallel Processing Workshops, ICPPW ’11, Taipei, Taiwan, (Sep. 2011.)
20. Ren,W., Yu,L., Gao,R., Xiong,F.: Lightweight and compromise resilient storage outsourcing with distributed secure accessibility in mobile cloud computing, Journal of Tsinghua Science and Technology 16 (5) 520–528 (2011).
21. Zhou,Z., Huang, D.: Efficient and secure data storage operations for mobile cloud computing, IACR Cryptology ePrint Archive: 185, (2011).
22. Dimitrios Zissis, Dimitrios Lekkas,: Addressing Cloud Computing Issues, Future Generation Systems (28) 583-592 (2012).
23. ISTQB Exam certification .com Webpage-http://istqbexamcertification.com/what-is-validation-in-software-testing-or-what-is-software-validation/
24.Belatrix cloud testing best practices, Belatrix Software Factory-White papers http://www.belatrixsf.com/index.php/outsourcing-case-studies/131

## About The Authors

**Manmohan Chaturvedi** is a retired Air Commodore from Indian Air Force with PhD in Information Security domain from IIT Delhi. He has about 35 years of experience in managing technology for IAF. An alumnus of National Defense College, New Delhi, he has held various appointments dealing with operational and policy dimensions of Information and Communication Technology. He graduated from Delhi College of Engineering and completed post graduation from IIT Delhi. Currently he is a Professor at School of Engineering and Technology, Ansal University with research interests in vulnerability of evolving ICT infrastructure and protection of Critical Information Infrastructure.

**Sapna Malik** is a Ph.D. candidate at the School of Engineering and Technology, Ansal University,India. She holds a M.Tech in IT from GGSIPU, New Delhi,India and B.Tech in CSE from Mayarishi Dayanand University,India.She is working as Assistant professor in department of Computer Science Engineering in Maharaja Surajmal Institute of technology ,Delhi,India.Her
Research interest includes Cloud computing, Network Security and Virtualization.

**Preeti Aggarwal** holds an M.Tech in IT from GGSIPU, New Delhi, an M.Sc in Informatics and a B.Sc (H) in Electronics from University Of Delhi and is currently pursuing Ph.D. in Data Mining and Information Security from Ansal university, Gurgaon. She is working as an Assistant Professor in department of Computer Science Engineering in KIIT College of Engineering, Gurgaon. She is also a member of Computer Society of India.

**Shilpa Bahl** holds M.Tech in IT from UIET, Krukshetra university ,Kurukshetra and B.Tech in Electronics & communication From Kurukshetra university and is currently pursuing Ph.D. in Software testing and Information Security from Ansal university, Gurgaon. She is working as an Assistant Professor in department of Computer Science Engineering in KIIT College of Engineering, Gurgaon, having Six years of teaching experience in Computer Science department