International Journal of Computer Networks and Applications
Volume 2, Issue 2, March – April (2015)

REVIEW ARTICLE

Security Concerns at Various Levels of Cloud Computing Paradigm: A Review

Aarti Singh
Associate Professor, Maharishi Markandeshwar University, Mullana
singh2208@gmail.com

Manisha Malhotra
Research Scholar, Maharishi Markandeshwar University, Mullana
mmanishamalhotra@gmail.com

Abstract –Cloud computing has become a buzzword in IT industry these days and organization are getting attracted towards this magnet for expanding their infrastructure at cheaper rates. However, with all flexibility offered by cloud there are concerns about security, integrity and availability of precious information of cloud users. Conventional protection mechanisms need to be reconsidered for their effectiveness, since cloud service model is distinctly different from other internet based service models. Recently, much research efforts are being done in cloud security but still more efforts are desired. Since cloud security is a sensitive dimension affecting its wide commercial acceptance. This work explores various levels of security concerns in cloud environment and lists available mechanism for addressing them.

Index Terms – Cloud Computing, Security issues, Levels, Review

1. INTRODUCTION

Infrastructure as a Service (IaaS), specifically data storage is one of important services provided by cloud computing (CC). Individual users and business organizations are shifting their data storage on cloud because of easy availability and reduced cost offered by it [1]. However, saving data at a remote server is just like giving your money to someone, since in today's digital era, data is the backbone of processing. Thus, with all the flexibility offered by cloud, serious security concerns have also been generated. Security concerns are generating hindrance for business organizations to shift entirely into public clouds [2]. Recently, there is increased attention from research and business community towards developing effective security measures for cloud paradigm. Some organization like Cloud Security Alliance (CSA), European Network and Information Agency (ENISA) [3], Cloud Computing Interoperability Group and Multi-Agency Cloud Computing Forum are working towards providing effective and efficient controls to provide information security in cloud environment. Some important security concerns prevailing in this domain are data security, privacy, resource availability, trust management etc. However, recently lot of researchers have proposed techniques for improving information security but still there is scope for research in this direction. This work explores security issues in cloud environment and presents existing solutions for the same. Next section outlines security problems existing at various level of cloud computing. Section 3 focuses on existing solutions for those problems. Finally last section concludes this work and elaborates future research directions.

2. SECURITY ISSUES AT VARIOUS LEVELS IN CLOUD COMPUTINGCONCLUSION

CC is internet based service paradigm where users access various services from Cloud service provider (CSP) through internet. Whenever user logs in a cloud and start accessing various services, information exchange gets started between user and CSP. Figure 1 given below indicates a cloud environment.

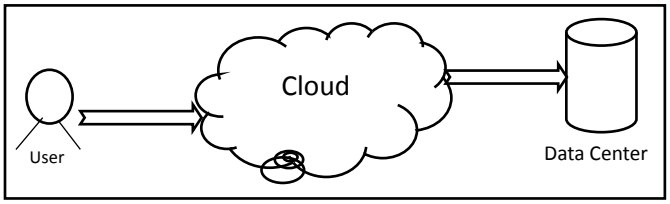

Figure 1 Cloud Environment

As far as security of information exchanged is concerned, only cloud storage is not concerned. There are in fact various levels where security breach may take place and integrity of information may be compromised. Figure 2 given below illustrates various levels of security concerns in cloud environment.

Every level contains their key points at different levels. All levels have their own importance and need equal attention for ensuring overall robust security in cloud environments. Figure 3 given below highlights various levels requiring security along with concerns underlying.

REVIEW ARTICLE

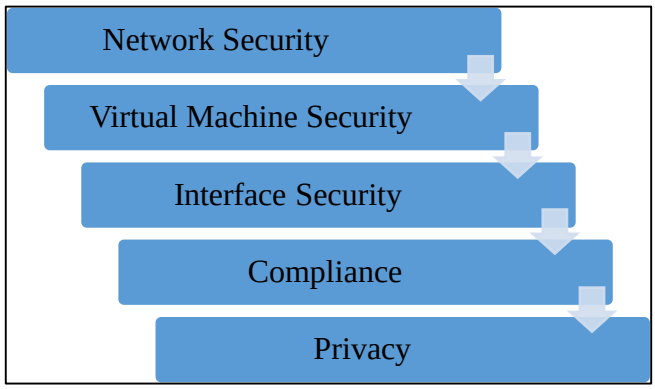

Figure 2 Various Levels of Security Concerns in Cloud Computing

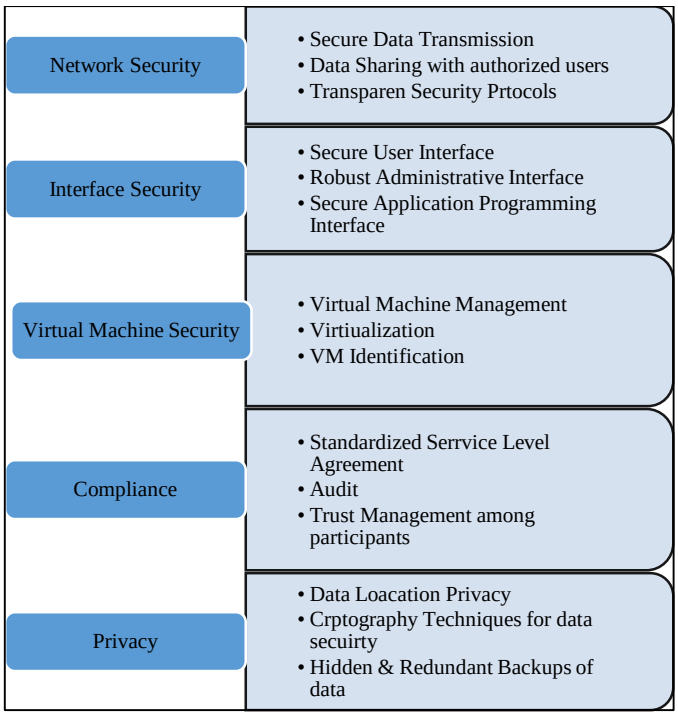

Figure 3 Security in Clouds: Levels and Concerns

Description of various security concerns are as follows:

2.1. Network Security

When information travels in the network then network security becomes a concern. Cloud service providers must ensure that robust and secure communication protocol is being adopted to avoid attacks on information while traveling in the network.

2.2. Interface Security

It is directly concerned with the interface which is provided by cloud providers and level of security offered by it. VM interface affects the inherent security features such as IBM Blue Mix is a cloud service based on Linux and Microsoft Azure is based on Windows operating system. Linux operating system is more secure as compared to Microsoft Windows. Thus interface security would be better with Linux based interface. Thus interface offered by CSP should deploy secure operating system.

2.3. Virtual Machine Security

VM security is of utmost concern amongst all security anxieties. Users make use of VM for their processing tasks. Further, a cloud makes use of Multi-tenancy technique i.e. same VM and resources are being used by different users at different point of time to improve resource utilization and cost reduction. However, this increases possibility of security breaches. Multiple users of a single virtual machine must be isolated to the extent so that confidentiality of an individual may be maintained.

2.4. Compliance

Compliance focuses on enforcing stated service level agreement (SLA). SLA is the only legal document between the user and the service provider which states the service requirements of the user and service standards to be provided by the provider. However, there is no standardization of SLA [4] which is essential to make this business model trustworthy. Weak implementation of service standards by the provider may lead to security flaws.

2.5. Confidentiality/ Privacy

Confidentiality focuses on preventing disclosure of private information to unauthorized users. In cloud computing all data is stored on geographically separated locations thus ensuring confidentiality of data becomes major issue. Applying various cryptographic algorithms, [5] is the typical solution being adopted. Data splitting [6] is another technique being used to ensure security of data at providers end. In this technique data is stored at multiple non-interacting hosts. However, both above techniques have their own inherent issues.

All above listed security concerns are of importance at different levels of communication with cloud. CSP has to ensure security at all levels, which is a tough task. Next section analyzes existing solutions for above security concerns.

3. SECURITY MECHANISM EXISTING IN LITERATURE

3.1. Towards Network Security

Arfeen et. al [7] focused on network awareness and consistent optimization of resource allocation strategies and highlighted the research issues prevailing in this field. Authors emphasized that more efforts are required to make the existing

REVIEW ARTICLE

performance models predictive and responsive. Safiriyu [8] proposed a user identity management protocol (UIDM) in cloud paradigm. It accommodates all stakeholders i,e end user and providers. It provides authentication, encryption and key management mechanism. They have tested weak, strong and very strong user identity and observed more failure in case of weak IDM. Zhen chen et. al [9] proposed a collaborative network security prototype system used in a multi-tenant data center. They have used a centralized collaborative scheme along with packet inspection at different levels of security. It protects the data center from all possible network attacks. This centralized security center is able to deploy security rules and collect data from the networks. But the proposed prototype lacks in detection of network policy violations.

3.2. Towards Interface Security

Philipp, et.al [10] has developed a platform which ensures the integrated security and improved data processing known as Virtual Fort Knox. This product is suitable for small and medium enterprises. It provides physical security like access control, protection from tampering of physical server as well as protection against failure of administrator.

3.3. Towards Virtual Machine Security

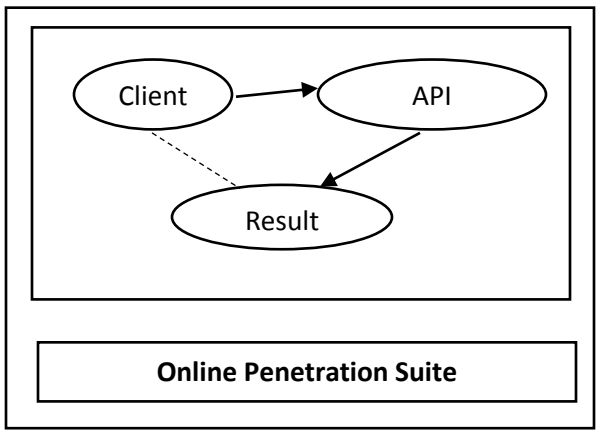

Figure 4 Update Checker Architecture [11]

Roland et.al [11] presents an architecture which increases the security of virtual machine. The architecture is divided into two parts one is update checker architecture and another is online penetration suite architecture shown in Figure 4. Update checker identifies the outdated information installed on virtual machine. Second one scans all virtual machines and boot them if there is need for it. Further, report generator is another component which generate the results of flaws (in terms of risk level) after collecting all reports from scanner. With the help of this report the error can easily be detected and removed. But both these architectures can be pertinent only on Linux environment. However, there is need of a generic architecture which can work on every environment.

Sapuntzakis et. al [12] developed a mechanism which assigns virtual machines automatically. The proposed scheme has prevented security breaks but does not allow updation of all packages of virtual machine.

3.4. Toward Compliances

Qian et. al [13] proposed a cloud data storage architecture that provides public auditable cloud mechanism which helps to examines proficiency and capabilities of data owner to assess the risk of outsource data with the help of external audit party. The proposed architecture comprises of four components: data owner, user, cloud server and Third Party Auditor (TPA). It provides a mechanism in which data owner appoint TPA to audit the cloud server in effective and cost efficient way for end users, when it is required. When it comes to security, it is not completely secure as it seems because the auditing completely relies on TPA and data owners. Here the question arise that if the owner and TPA are not delivering correct report to user, then who will be responsible for that. Funmilade et. al [14] proposed a dynamic data driven architecture which is capable to minimize the SLA violations by releasing resource provision. In the proposed architecture, the author has focused only on resource releasing but no attention about the security. Cloud Security Alliance [15] is a nonprofit organization which was established in December 2008. It checks all government strategies and audit policies for ensuring good security in cloud computing. It releases new policies with the help of National Institute of Standards and Technology (NIST) and Information Systems Audit and Control Association (ISACA).

3.5. Towards Privacy

Yuefa et. al [16] presents a study on need of security in cloud computing. Currently, most of the agencies are working on Hadoop Distributed File System (HDFS) architecture which is based on master slave node. Master node is named as name node and slave node is named as data nodes. All data is replicated thrice and stored on data nodes. According to this study, all access control of data nodes are managed by a single point i;e name node which can be a cause of failure. They presented a model with three lines of defense as shown in Figure 5. These are authentication security at first level, encryption and privacy protection at second level and fast recovery at third level. Authentication layer is used for user verification with the help of digital signature and encryption algorithm is deployed at second layer. Third layer uses rapid recovery algorithm for recovering the data.

Huiqi et al. [17] proposed Random Space Perturbation (RASP) method and Nearest Neighbor (kNN) which address the four main aspects data confidentiality, query privacy, efficient query processing and low processing cost. Authors performed an experiment under a threat model and found the results providing more efficiency at reduced cost. But this method suffered from data leakage and weak query privacy.

REVIEW ARTICLE

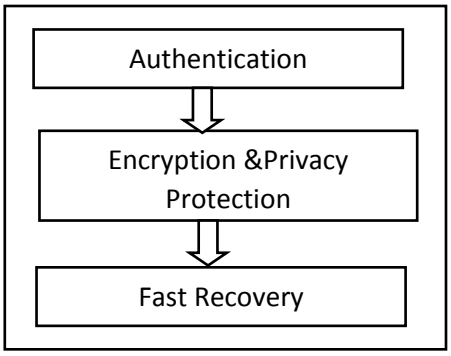

Figure 5 Data Security Model for Cloud Computing [16]

Hossein et al [18] presents Encryption as a Service (Eaas) for ensuring the security at CSP. In this approach a private cloud is being created by using Message Authentication Code (MAC) for integrity. This approach is based on multi-threading processes. Each single thread hits equivalently on a parallel region and produces team of threads after encryption. However, this mechanism will work successfully only if the program had been written in multi-threading style, otherwise the performance gets decreased. The description of this model is shown in Figure 6.

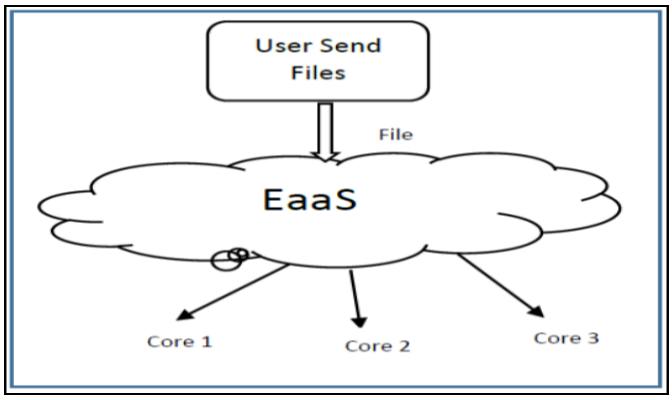

Figure 6 Encryption as a Service [18]

Xu et. al [19] proposed an agent based trust model which ensures the reliability and credibility. Authors proposed architecture Trustworthy Agent Execution Chip (TAEC) which provides high security and works on sensor node by using agent technology. Before sending the data from node A to node B, it encrypts the data by applying TAEC. Firstly node A gets the trust certificate from TAEC Manufacturer (TAECM) which contains public key, security strategy, and TAEC type. After verification of digital signature, data is transferred to node B. Due to assimilation of agents the proposed model becomes platform independent, however the usage of digital signature decrease the efficiency of model. The architecture is shown in Figure 7.

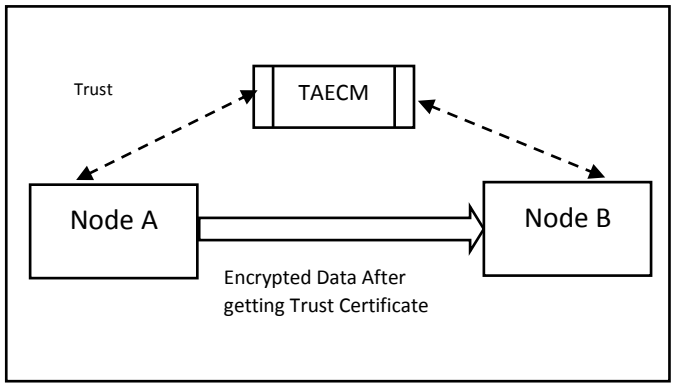

Figure 7 Trustworthy Agent Execution [19]

Wang et.al [20] proposed an auditing mechanism in cloud environment known as Public Auditing for shared data (PANDA) with efficient user revocation. The purpose behind the user revocation is that if the same user would approach to cloud then every time of revocation, the private key is generated and the data has to be re-signed with private key. Due to this computing, time increases and efficiency decreases.

Above section indicates that limited research had been carried out towards various security issues prevailing in CC. There is still ample scope of research in this dimension. Upcoming section concludes this work.

4. CONCLUSIONS AND FUTURE SCOPE

Security is one of the main aspects of cloud computing for its wide commercial acceptance. This work has tried to summarize security issues at various levels of cloud computing. However, it has been observed from this review that more or less, similar security approaches are being suggested for cloud computing as for other internet based computing techniques. Considering the distinct features of cloud applications, such as custody of user's data, multi-tenancy of infrastructure etc. really demand for specialized security mechanisms which could provide better comfort and trust while working with cloud. SLA compliance should be seriously considered by government agencies and strict laws should be formulated towards SLA violation. Future work will focus on developing reliable, secure and trustworthy mechanism for cloud environment.

REFERENCES

[1] Singh, A., & Malhotra, M.,"Agent Based Framework for Scalability in Cloud Computing" In International Journal of Computer Science & Engineering Technology 3(4), 2012, pp 41-45.

[2] Malhotra, M., Singh, A., & Juneja, D., "Security Issues in Cloud Computing: An Approach" In National Seminar "The Futuristic Approach to Ethical Hacking & Network Security, Feb, 2014, pp 1-5.

[3] Mather, T., & Kumarswamy, "Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliances" In 1st Edition 2009 of CSA Forum.

REVIEW ARTICLE

[4] Atallah, M., Frikken, K., & Blanton, M. , "Dynamic and Efficient Key Management for Access Hierarchies" In Proceedings of ACM Conference Computer Communication Security, 2005, pp. 190–202.
[5] Mladen, A., & Vouk. Cloud Computing – Issues, Research and Implementations. In Journal of Computing and Information Technology - CIT 16, pp 235–246.
[6] Jungwoo, R., Syed, R., William, A., & John, K., "Cloud Security Auditing: Challenges and Emerging Approaches". Published in IEEE Security and Privacy, 2013, pp 1-13.
[7] Arfeen, M. A., Pawlikowski, K. & Willing, A, "A Framework for Resource Allocation Strategies in Cloud Computing Environment". Published in Proceedings of 35th IEEE Conference on Computer Software and Application, 2011, pp. 261-266.
[8] Safiriyu, E., Olatunde, A., Ayodeji, O,Adeniran, O., Clement, O., & Lawrence, K. "A User Identity Management Protocol for Cloud Computing Paradigm" In nternational Journal Communications, Network and System Sciences, 4(1), 2011, pp 152- 163.
[9] Zhen, C., Wenyu, D., Hang, Li., Peng, Z., Xinming, C., & Junwei, C., "Collaborative Network Security in Multi-Tenant Data Center for Cloud Computing". Tsinghua Science and Technology,19(1),February 2014, pp82-94.
[10] Philipp, H., Rolf, W., Joachim, S., & Thomas, B., "Virtual Fort Knox: Federative, Secure and Cloud Based Platform for Manufacturing" In Proceedings of 46th Conference on Manufacturing System, indexed in Science Direct, 2013, pp 527-532.
[11] Roland, S., Matthias, S., Christian, S., Simon, M., & Bernd, F., "Increasing Virtual Machine Security in Cloud Environments" In Journal of Cloud Computing, 1(12), 2012, pp 1-12.
[12] Pointcheval, D., & Stern, J., "Security Proofs for Signature Schemes" In Proceedings of Eurocrypt, volume 1070 of LNCS. Springer-Verlag, 1996, pp 387–398.
[13] Qian, W., Cong, W., Kui, R., Wenjing, L., & Jin, L. "Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing" In IEEE Transactions on Parallel and Distributed Systems, 22(5), 2011, pp 847-859.
[14] Funmilade, F.,, Rami, B., & Georgios, T ,"A Dynamic Data Driven Simulation Approach for Preventing Service Level Agreement Violations in Cloud Federation". In Proceedings of International Conference on Computational Science, Procedia of Computer Science 2012, pp 1167-1176.
[15] CSA Security Guidance for Critical Areas of Focus in Cloud computing 2009, Cloud Security Alliance, Published on Forum of CSA. **5**
[16] Yuefa, D., Bo, W., Yaqiang, G., Quan, Z., & Chaojing, T., "Data Security Model for Cloud Computing" In Journal of International Security and Applications, 2009, pp 141-144.
[17] Huiqi, X., Shumin, G., & Keke, C.,"Building Confidential and Efficient Query Services in the Cloud with RASP Data Perturbation" In IEEE Transactions on Knowledge and Data Engineering, 26(2), 2014, pp 322-335.
[18] Hossein, R., Elankovan, S., Zulkarnain, M., A., & Abdullah, M., Z., "Encryption as a Service as a Solution for Cryptography in Cloud" In Proceedings of 4th International Conference on Electrical Engineering and Informatics, indexed in Science Direct, 2013, pp 1202-1210.
[19] Xu. X., Bessis, N., Cao, J., "An Autonomic Agent Trust Model for IoT System" In Proceedings of 4th International Conference on Emerging Ubiquitous System,2013, pp 107-113.
[20] Wang, B., Li, B., & Li, H., "Panda: Public Auditing for Shared Data with Efficient User Revocation in the Cloud". In IEEE Transaction, 2013, pp 1-14.
[21] Armbrust, M., Fox, A., Griffith, R., Joseph, A., Katz, R., & Konwinski, A. "A View of Cloud Computing". In ACM Communication, 53(4), 2010, pp. 50–58.
[22] Bellare, M., Garay, J., & Rabin, T., "Fast Batch Verification for Modular Exponentiation and Digital Signatures". In Proceedings of Eurocrypt volume 1403 of LNCS. Springer-Verlag, 1998, pp. 236–250.
[23] Ferrara, A. L., Greeny, M., Hohenberger, S., & Pedersen, M. "Practical Short Signature Batch Verification" In Proceedings of CT-RSA, volume 5473 of LNCS. Springer- Verlag, 2009, pp. 309–324.
[24] Goyal, O., Pandey, A., Sahai, & B. Waters , "Attribute-Based Encryption for Fine- Grained Access Control of Encrypted Data" In Proceedings of ACM Conference Computer Communication Security, 2006, pp. 89–98.
[25] Malhotra, M., & Malhotra, R., "Cloud Adaptive Resource Allocation Mechanism for Efficient Parallel Processing". Published in IGI Global, International Journal of Cloud Applications and Computing, 4(4), 2014, pp 1-6.
[26] Messmer, & Ellen,"Cloud Security Alliance Formed to Promote Best Practices" Computerworld, Published on Forum 2009 of CSA.
[27] Sapuntzakis, C., Brumley, D., Chandra, R., Zeldovich, N., Chow, J., Lam, M., & Rosenblum, M., "Virtual Appliances for Deploying and Maintaining Software" In Proceedings of the 17th USENIX Conference on System Administration. USENIX Association, Berkeley, 2008, pp 181–194.
[28] Singh, A., & Malhotra, M.m, "Analysis for Exploring Scope of Mobile Agents in Cloud Computing" In International Journal of Advancements in Technology, 3(3), 2012 pp 172- 183.
[29] Xiaonian W., Runlian Z., Bing, Z &Shengyuan, Z., "A Trust Evaluation Model for Cloud Computing" In Elsevier Proceedings of Information Technology and Quantitative Management, 2013, pp 1170-1177.
[30] Yang, H., & Tate, M., "Where are we at with Cloud Computing?: A Descriptive Literarure Review" In Proceedings of 20th Australasian Conference on Information Systems, 2009, pp 807-819.
[31] Zhang, Q., & Cheng, L., "Cloud computing: State-of-the-art and Research Challenges". Journal of Internet Serv Appl, 2010, pp 7–18 DOI 10.1007/s13174-010-0007-6.
[32] Zhou, L., Varadharajan, V., & Hitchens, M., "Enforcing Role-Based Access Control for Secure Data Storage in the Cloud" In Journal of Computing 54(13), 2011, pp. 1675–1687.
[33] Zhu, Y., Hu, H., Ahn, G., Wang, H., & Wang, S., "Provably Secure Role-Based Encryption with Revocation Mechanism". In Journal of Computer Science and Technology, 26(4), 2011 pp. 697–710.
[34] Zhu, Y., Ma, D., Hu, C., & Huang, D., "How to Use Attribute-Based Encryption to Implement Role-Based Access Control in the Cloud". In Proceedings of International Workshop Security Cloud Computing, 2013 pp. 33– 40.

Authors

Dr. Singh is presently working as Associate Professor in Maharishi Markendeshwar Institute of Computer Technology & Business Management running under the umbrella of Maharishi Markendeshwar University, Mullana, Haryana. She has a credible academic record, with various degrees like Ph.D.(Computer Science), M.Phil. (Computer Science), MCA, M.Sc.(Computer Science) and B.Sc. (Computer Science & App.). She also owes the credit of 37 published research papers in various national &International Journals of repute, with one paper awarded as the Best Paper in an IEEE Conference. She has also participated in many International conferences within India and abroad. Dr Singh's research interests include Semantic Web, Agent Technology, Web Mining and Intrusion Detection Systems.

Ms. Manisha Malhotra working as Assistant Professor in Chandigarh University. She is pursuing her Ph.D in area of Cloud Computing. She has the degree of MCA and B.SC (Computer Science). She is the members of many professional bodies like IEEE, IEANG. Ms. Malhotra has published more than 10 research papers in National/ International Conferences & in reputed Journals. She has attended many National & International Conference. Her area of interests in the field of Cloud Computing & Agent Technology.