International Journal of Advanced Computer Technology (IJACT)

ISSN:2319-7900

ENABLING SELF AUDITING FOR MOBILE CLIENTS IN CLOUD COMPUTING

V.Saravanan, AP, IT Department, P.S.V. College of Engineering and Technology, Krishnagiri, India.
S.Thirukumaran, AP, MCA Department, Adhiyamaan College of Engineering, Hosur, India.
M.Anitha, AP, MCA Department, Adhiyamaan College of Engineering, Hosur, India.
S.Shanthana, PG Scholar, CSE Department, P.S.V. College of Engineering and Technology, Krishnagiri, India.

Abstract

Cloud is a rising technology that works over the Internet and it permits the user to urge the service from anyplace and at any time with pay per usage theme. Cloud computing makes the business environment easier by offering huge storage capacity, processing power and infrastructure with the elastic demand. The cloud is helpful in reducing the cost of service and in increasing the availability which is essential for a successful business. But, the lack of control and security are the big issues in the cloud computing. For this security problem, additional solutions have to be developed to make the cloud computing a grand success in the future. In this paper we have proposed a method to enhance the file integrity, which is very effective in security and very easy to implement. The proposed method is suitable for mobile clients and it helps to improve the file integrity and reduce the complexity.

Introduction

Cloud is a rising technology that works over the Internet and it permits the user to urge the service from anyplace and at any time with pay per usage theme. The cloud user wants an online enabled device with browsers to access the services. Cloud makes the business surroundings easier by giving vast storage capacity, processing power and infrastructure with the elastic demand. The cloud is useful in reducing the cost of service and in increasing the supply that is crucial for a successful business. Any corporate with cloud can scale back the cost. The servers within the cloud offers numerous services and these servers can be physical machines or virtual machines. A cloud application uses massive datacenters and powerful servers for pretty much unlimited storage and higher machine power. These datacenters and servers can host vast range of Internet applications and Internet services. Anyone with net association can access these cloud applications.

Cloud parts are classified in to two groups particularly frontend and backend. The visible parts to the cloud user like browser, laptop and network used to access the Internet are aforementioned to be frontend. The parts needed to deploy the cloud like storage devices, computers and servers that gives numerous services are classified as backend. The cloud can be deployed in three models namely private cloud, public cloud and hybrid cloud [30, 31, 32]. The cloud that operates for a particular organization is assumed to be private cloud. This kind of cloud is deployed internally or outwardly and managed internally or by third-party. The private cloud is better in security, regulative necessities and enterprise management over preparation and use. The cloud users can share and use all the resources and applications provided by the cloud supplier. The cloud that operates not for a specific organization is alleged to be public cloud. Here any users can ready to access the cloud via interfaces with pay-per-use theme [41]. This enables the cloud user to settle on right service with correct quantity of their time to scale back the IT expenditure. The mixture of personal and public cloud can form a hybrid cloud. Here the private clouds and be connected with one or additional public cloud services and managed as one unit. This enables heterogeneous users to access the resources over net with secure management over the information, and therefore the services is scaled up or down as per the demand.

The service offered by the cloud is classified in to Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS) [6, 33, 34, 35, 38]. The cloud can give resources like virtual machine disk images, firewalls, virtual native space networks and software system collections [8, 10]. The network elements like firewall, router and other may be deployed using virtual environment. By obtaining infrastructure as a service from the cloud, the price and time can be reduced dramatically. Conjointly, maintenance is really easy, since most of the elements within the cloud are virtual and on demand resources. We ask authors to follow these guidelines and make the paper look exactly like this document. The easiest way to do this is simply to download this template and replace the content with the text of your manuscript.

Advantages and Disadvantages of Cloud Computing

Starting from tiny corporations to huge organizations, the investment value is saved [23, 24, 36, 42] by avoiding the hardware purchase, hardware maintenance, pricy software system license, software system maintenance, cooling products, storage and backup devices, value for electricity usage, operational value, upgrading value etc. Apart from this value saved, the cloud has few other advantages like high responsibility and convenience, backup and recovery, device & location independence, easy accessibility to info and fast preparation. All these advantage makes the cloud computing a grand success. Cloud has several benefits and conjointly it has few disadvantages. The two big disadvantages of cloud are; Technical Problems and Security. Even though the cloud offers a lot of facility to the users and build their life straightforward, some technical problems might produce inconvenience to the users. To access the cloud, Internet usage is should and therefore the problems associated with the network might have an effect on the performance of the cloud severely. If the user uses mobile devices then several reasons like signal strength, Bandwidth, battery backup and frequent handoff might degrade the performance of the cloud dramatically [47, 48]. The security could be a huge downside within the cloud computing. Because, all the sensitive information's of an organization or company should be transferred over the Internet which might be a big risk.
As shown in figure 1, the clients are ambiguous in choosing whether the cloud is used or not, since cloud has both benefits and downsides. Cloud helps the client to scale back the operational value, preparation time and maintenance value. This reason makes the cloud computing a preferred one and plenty of corporations shifted to the cloud usage. However the large issue within the cloud computing is lack of management and security. For this security downside, extra solutions need to be developed to form the cloud computing a grand success within the future.

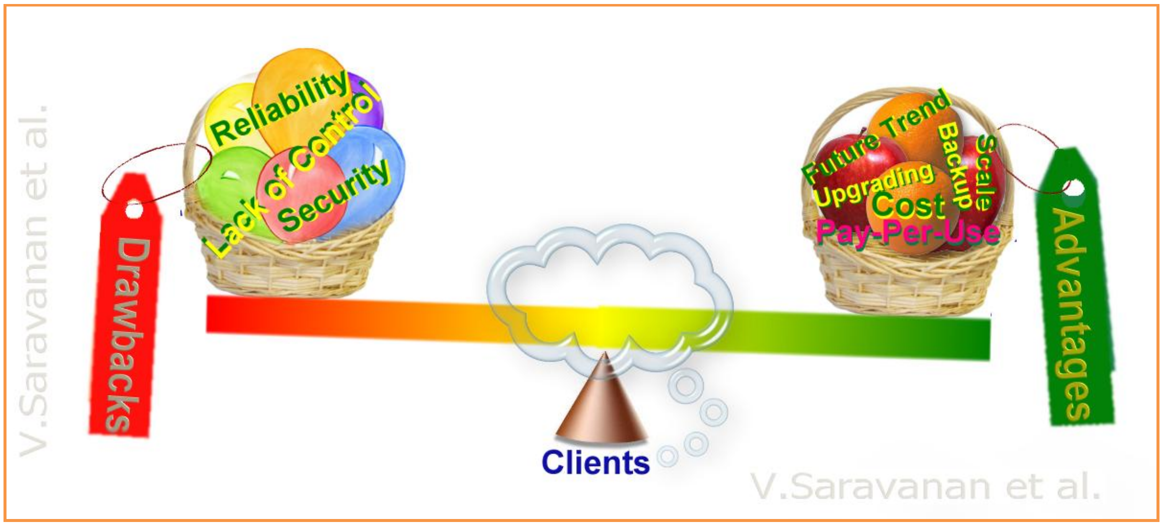

Figure 1: Cloud advantages and disadvantages

Literature Survey

Internet is acting as a lane, where various technologies drive on it. Out of that cloud is the most recent technology and almost all the large scale organizations enter into it. The cloud has too many advantages as discussed in the previous section and out of that, hardware and maintenance cost, accessibility around the globe, flexibility and highly automates process are most important for the clients, since the hardware or software up gradation seem to be a everyday headache for the clients.

The execution environment required for a client to develop a web based application requires expensive hardware and software support and this may require more time to setup. But by using the cloud one service can continue his work without the expensive purchase and time consuming setup by using PaaS of the cloud [7, 8, 17]. The infrastructure and execution environment can be used by many clients simultaneously and managed by third party [10, 11, 18, 23].

To make everything (Services) possible, available, manageable and reusable in the cloud, the virtualization technique plays a vital role. A single server in the cloud can provide multiple services in parallel to huge number of clients via the virtualization technique [12, 13, 23]. The tools like VMWare, Micorsoft Virtual PC, VirtualBox, Parallels, QEMU etc. helps in virtualization of Operating Systems. The cloud enables the centralization of resources, which is unsafe since the chances for cyber attacks increases. The possibility for the attack is more in cloud side because, the user of the cloud needs to send his identity over the Internet frequently for accessing the services.

The data security is also a challenging issue in cloud computing since all the data of an individual or organization are centralized and kept in remote servers [14, 15, 19]. To ensure the data security, the strong encryption algorithms has to be developed to overcome the security threads on storage security. The cloud service provider has to limit the access over the file by allowing few actions related to managing the files without any strict process and should be strict in actions like updating, reading and deleting of file. This will optimize the performance as well as security. To keep the cloud running smoothly, the multi level security is compulsory at various levels i.e., network level [16], host level [25] and application level [14, 26, 27]. The basic security models such as SQL Injection attack prevention, Cross Site Scripting (XSS) attack prevention, Man in the Middle attack prevention [20, 21, 32, 32, 37, 44] are not sufficient for the cloud to run seamlessly.

In the Internet, it is common to have denial of service attacks [2, 3, 4, 18, 22, 23, 28] and cookies poisoning attacks [43]. To distinguish the human and machine virus in the Internet, the concept of captcha [5] was used by most of the servers. but recent virus and spams have the ability to break the captcha. So it is clear that, continuous research in this field is must to protect the future Internet oriented services.

It is true that certain loopholes in the architecture make the cloud computing vulnerable to the security threads in high probability [45, 46]. There is no guaranty that the cloud service provider could maintain our files on a single server or storage. The files may be split into many parts and distributed over multiple servers to improve the speed via parallelism. This scenario makes the cloud more vulnerable to the security related threads.

Apart from security, cloud has other disadvantages like performance, latency [29] and reliability [24, 39]. The reason for the latency, poor performance and unreliability in the services is as follows;

a) The complicated or time consumable encryption and decryption algorithms used in the cloud computing environment.

b) The unreliable and low bandwidth Internet connectivity.

c) Unreliable network with high conjunction and packet losses.

d) Allowing too many users to access the services beyond the limit because of high demand from the client's side.

e) Mobile clients running with extremely high shortage of resources.

However from the survey we can say that, even after several research and development the security and file integrity problems are keep on persist in the Internet based services, specifically on the cloud. So we need different solutions for different situations and requirements over time.

File Integirity Model

Checking file integrity is a challenging task in cloud computing. In the classical method for checking the correctness of a file the client has to maintain a copy to compare the received copy. This is meaningless, because if the client has enough storage to store the data in the local system, then it is not necessary to use the cloud service to store the file in remote location. The clients, those are not having enough resources alone may prefer the cloud services.

From the literature we can have hundreds of file integrity models which are suitable for cloud storage service. Some models are lack in providing security and few are poor in performance. Also, some of the existing models are good in security but poor in execution time. The methods should be compact enough to run smoothly on the light weight mobile devices, since most of the cloud clients are mobile in the recent years.

Our proposed model of file integrity is as follows. The entire file has to be split into number of macro blocks (M1,M2,M3,M4, …, Mn). All the macro blocks should be of unique size. If the Last block contains no sufficient bits to form the block with fixed size, then padding bits can be merged with the original data. Each Mi should be processed and the corresponding hash code has to be generated using our proposed method.

The hash code for each block can be calculated using our proposed method as follows;

Step1: Create eight variables I1, I2, I3, I4, I5, I6, I7 and I8 of length one byte each.

Step2: Initialize all the variables with any fixed value (vi), that should be shared between both client and Cloud Service Provider.

Step3: Calculate variable O1, O2, O3, O4, O5, O6, O7 and O8 as follows; O1=I4 Œ I5. O2=I5 Œ I6. O3= (I6 Œ I7) Œ (ƒ1(I1 Œ I2, I2 Œ I3, I3 Œ I4, NOT(I4 Œ I5))). O4=(I7 Œ I8) Œ (Datai Œ ƒ2(I5 Œ I6, I6 Œ I7, I7 Œ I8)). O5=Datai Œ ƒ2(I5 Œ I6, I6 Œ I7, I7 Œ I8). O6=I3 Œ I4. O7=I2 Œ I2. Where Œ is the bit wise X-OR operation, ƒ1 is the function performs bit wise AND operation between first two parameters, with the result, the OR operation is performed with third parameter and finally one more operation is performed between the fourth parameter and the result. ƒ2 is the function that takes three parameters and perform bitwise AND operation between first and second parameter. With the result, OR operation is performed with third parameter. Datai is the ith ($1 \leq I \leq$ macro block size) byte of the macro block.

Step4: Repeat step 3 until all the bytes of the macro block is used completely. The O1, I2, O3, O4, O5, O6, O7 and O8 are considered to be the I1, I2, I3, I4, I5, I6, I7 and I8 respectively for the next round.

Step5: Stop the process and take O1, O2, O3, O4, O5, O6, O7 and O8 as the hash value for the current macro block.
The hash codes have to be encoded with the client's private key to form a signature. The signature is of size 64 bits. The signature has to be calculated for the entire macro blocks stating from M1 to Mn. The set of all macro block and the respective signatures has to send to the cloud service provider. The cloud provider may once again check for the correctness and if there is no error, then it can be accepted.

Auditing

If the client wants to audit its own data, then the entire file needs not to be downloaded. Only few specific randomly selected blocks can be requested from the cloud service provider. The request contains the block number, key to process the block and initial value to start the hash rounds. The Cloud Service Provider has to calculate the hash value for the currently requested block and send it with the respective signature to the client. The client can decrypt the signature or encrypt the received hash to compare with each other. If both received hash and decrypted signature matches then the auditing reports the correctness, otherwise reports the rejection.

File Updating

If the client needs to update a specific block then the client send the new modified macro block, block number, key, initial value and newly calculated signature to the cloud service provider. The cloud service provider and authenticate the request and it can replace the new block and signature in the corresponding places. Then the cloud service provider has to calculate the hash value using the received key and initial value. The newly calculated hash value and corresponding signature has to be returned to the client. The client once again checks for the integrity and accepts it or rejects, based on the comparison result as discussed above.

Performance analysis

The big problem in cloud computing is the auditing process. As discussed earlier, most of the cloud clients are mobiles. These mobile devices are limited in resources [47, 48, 49, 1] and it is a big overhead to the clients to perform auditing which consumes more resources. The solution for this problem is the Third Party Auditing (TPA). In TPA the client need to send the key, block number and initial value to the third party auditor, so that the auditor can request to the cloud service provider to send the specific block of file with its signature. In some cases the client send key alone to the third party auditor and the auditor may request the cloud service provider to send a specific block (The block can be selected randomly) with its respective signature. Then the auditing report can be send back to the client. The big problem in this scheme is, the client has to send the key over the internet to the auditor, which is not safe.

In our proposed model, the TPA is not required, since the calculation of hash code is done in the cloud side and not in the client side. The client work is to just encrypt the specific block using its key and compare it with the received signature. This work of encrypting a small block will not consume too much of resource.

Thus our proposed algorithm has the following advantages.

1 The self auditing process consumes very limited resource and thus it is suitable for mobile clients.
2 The TPA is not necessary.

3 File update is very effective and easy, since the block size is very limited.

4 Easy to understanding and implementation.

Conclusion

In this paper we did a detailed study on cloud computing and its services. We have analyzed the advantages and disadvantages of the cloud and identified the issues in cloud computing related to file integrity. Also we have proposed a method to calculate the signature, which is very effective in security and very easy to implement. The proposed method is suitable for mobile clients and it helps to improve the file integrity and reduce the complexity.

Acknowledgments

Our sincere thanks to our honourable Chairman **Dr.P.Selvam M.A., B.Ed., M.Phil., Ph.D., D.Litt.**, P.S.V. College of Engineering & Technology, Krishnagiri, for giving this opportunity. We express my profound gratefulness to our **Secretary Mr. S.Vivek M.A., M.B.A.,** and our Principal **Dr.K.Rangasamy M.E., M.B.A., Ph.D.**, P.S.V. College of Engineering & Technology for his continuous encouragement in publishing technical papers. Our special thanks to **Prof. R.Srinivasan M.E., (Ph.D.,),** HOD/IT and our system admin **Mr. T.Shankar B.E.**, for their timely help in providing required software and hardware.

References

[1] V.Saravanan and A.Neeraja, 2013. Security Issues in Computer Networks and Stegnography, in Proceedings of 7th International Conference on Intelligent Systems and Control (ISCO 2013), Coimbatore, Tamilnadu, India, January 4-5, 2013. pp. 363-366, DOI: 10.1109/ISCO.2013.6481180.

[2] Ruiping Lua and Kin Choong Yow, 2011. Mitigating DDoS Attacks with Transparent and Intelligent Fast-Flux Swarm Network. IEEE Network, 25(4): 28-33. DOI: 10.1109/MNET.2011.5958005.

[3] Ruiping Lua and Kin Choong Yow, 2011. Mitigating DDoS Attacks with Transparent and Intelligent Fast-Flux Swarm Network. IEEE Network, 25 (4): 28-33. DOI: 10.1109/MNET.2011.5958005.

[4] K. Vieira, A. Schulter, C. B. Westphall, and C. M. Westphall, 2010. Intrusion detection techniques for Grid and Cloud Computing Environment. IT Professional, IEEE Computer Society, 12 (4): 38-43. DOI: 10.1109/MITP.2009.89.

[5] J. Yan and A.S. El Ahmad, 2009. CAPTCHA Security: A Case Study. IEEE Security & Privacy, 7(4): 22 – 28. DOI: 10.1109/MSP.2009.84.

[6] Yarter L. C., 2012. Private cloud delivery model for supplying centralized analytics services. IBM Journal of Research and Development, 56 (6): 1 – 6. DOI: 10.1147/JRD.2012.2216331.

[7] Wenbo Zhang, Xiang Huang, Ningjiang Chen, Wei Wang, and Hua Zhong, 2012. PaaS-Oriented Performance Modeling for Cloud Computing. IEEE - Computer Software and Applications Conference (COMPSAC), pp: 395-404. DOI: 10.1109/COMPSAC.2012.59.

[8] F. Paraiso, N. Haderer, P. Merle, R. Rouvoy and L. Seinturier, 2012. A Federated Multi-cloud PaaS Infrastructure. 2012 IEEE 5th International Conference on Cloud Computing (CLOUD), pp: 392 – 399. DOI: 10.1109/CLOUD.2012.79 .

[9] Z. Rehman, O.K. Hussain, F.K. Hussain, 2012. Iaas Cloud Selection using MCDM Methods. 2012 IEEE Ninth International Conference on e-Business Engineering (ICEBE), pp: 246 – 251.

[10]Montero.R.S, 2012. Building IaaS Clouds and the art of virtual machine management. International Conference on High Performance Computing and Simulation (HPCS), pp: 573. DOI: 10.1109/ICEBE.2012.47.

[11] Ji Ho Kim, Sang Min Lee, Dong Seong Kim and Jong Sou Park , 2011. Performability Analysis of IaaS Cloud. Fifth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS). pp: 36 – 43. DOI: 10.1109/IMIS.2011.117 .

[12] Jun Huang, Yanbing Liu and Qiang Duan, 2012. Service provisioning in virtualization-based Cloud computing: Modeling and optimization. Globecom Communications QoS, Reliability and Modelling Symposium, pp: 1728-1733. DOI: 10.1109/GLOCOM.2012.6503361.

[13] He, Zongjian and Liang Guanqing, 2012. Research and Evaluation of Network Virtualization in Cloud Computing Environment. Third International Conference on Networking and Distributed Computing (ICNDC), pp: 40 – 44. DOI: 10.1109/ICNDC.2012.18.

[14] P. Pradhan, P.S. Kumar, G. Mahapatra and R. Subramanian, 2012. Distributed verification protocols for data storage security in Cloud Computing. International Conference on Communication, Information & Computing Technology (ICCICT), pp: 1 – 6. DOI: 10.1109/ICCICT.2012.6398205.

[15] G. Kulkarni, J. Gambhir, T. Patil, and A. Dongare, 2012. A security aspects in cloud computing. International Conference on Software Engineering and Service Science (ICSESS), pp: 547 – 550. DOI: 10.1109/ICSESS.2012.6269525.

[16] Shetty.S, Luna. N, and Kaiqi Xiong, 2012. Assessing network path vulnerabilities for secure cloud computing . Conference on Communications (ICC), pp: 5548 – 5552. DOI: 10.1109/ICC.2012.6364720.

[17] John E. Dunn, 2009. Spammers break Hotmail's CAPTCHA yet again, Tech-world. http://news.techworld.com/security/110908/spammers-break-hotmails-captcha-yet-again/ (Accessed on March 16, 2013).

[18] R. L Grossman, 2009. The Case for Cloud Computing. IT Professional, 11 (2): 23-27.

[19] Lori M. Kaufman, 2009. Data security in the world of cloud computing, IEEE Security and Privacy Journal, 7 (4): 61-64. DOI: 10.1109/MSP.2009.87 .

[20] Jonathan Katz, 2002. Efficient Cryptographic Protocols Preventing Man in the Middle Attacks. Doctoral Dissertation submitted at Columbia University, http://www.cs.ucla.edu/~rafail/STUDENTS/katz-thesis.pdf (Accessed on March 20, 2013).

[21] Adam A Noureddine, Meledath Damodaran, 2008. Security in Web 2.0 Application Development," iiWAS '08, Proc.of the 10th International Conference on Information Integration and Web-based Applications & Services, pp. 681-685.

[22] Chi-Chun Lo, Chun-Chieh Huang, Joy Ku, 2010. A Cooperative Intrusion Detection System Framework for Cloud Computing Networks. Proceedings of the 2010 39th International Conference on Parallel Processing Workshops, IEEE Computer Society. pp: 280-284. DOI: 10.1109/ICPPW.2010.46.

[23] Aman Bakshi, Yogesh B. Dujodwala, 2010. Securing cloud from DDoS Attacks using Intrusion Detection System in Virtual Machine. Proceeding of the 2010 Second International Conference on Communication Software and networks. IEEE Computer Society, USA, pp: 260-264. DOI: 10.1109/ICCSN.2010.56.

[24] Neal Leavitt, 2009. Is Cloud Computing Really Ready for Prime Time?. Computer 42(1): 15-20. DOI: 10.1109/MC.2009.20.

[25] Zhou Ti, Wang Xiao-fei, Feng Li and Wang Jing, Research on host-level security situational awareness. International Conference on Computer Science and Information Technology (ICCSIT), pp: 575 – 579. DOI: 10.1109/ICCSIT.2010.5563826.

[26] M.S. Olivier, R.P. van de Riet and E. Gudes, 1998. Specifying application-level security in workflow systems. Proceedings. Ninth International Workshop on Database and Expert Systems Applications, pp: 346 – 351. DOI: 10.1109/DEXA.1998.707423.

[27] M. Burnside, A.D. Keromytis, 2003. Accelerating application-level security protocols. The 11th IEEE International Conference on Networks-ICON2003, pp: 313 – 318. DOI: 10.1109/ICON.2003.1266209.

[28] Fen Liu and Lei Hu, 2008. ROAD: An RFID Offline Authentication, Privacy Preserving Protocol with Dos Resilience. International Conference on Network and Parallel Computing-NPC, pp: 139 – 146. DOI: 10.1109/NPC.2008.9.

[29] Yu Kang, Zibin Zheng and M.R. Lyu, 2012. A Latency-Aware Co-deployment Mechanism for Cloud-Based Services. IEEE 5th International Conference on Cloud Computing (CLOUD), pp: 630 – 637. DOI: 10.1109/CLOUD.2012.90.

[30] J.Keung, F. Kwok, 2012. Cloud Deployment Model Selection Assessment for SMEs: Renting or Buying a Cloud. IEEE Fifth International Conference on Utility and Cloud Computing (UCC), pp: 21 – 28. DOI: 10.1109/UCC.2012.29.

[31] Gansen Zhao, Chunming Rong, M.G. Jaatun, and F.E.Sandnes, 2010. Deployment models: Towards eliminating security concerns from cloud computing. International Conference on High Performance Computing and Simulation (HPCS),pp: 189 – 195. DOI: 10.1109/HPCS.2010.5547137.

[32] L. Savu, 2011. Cloud Computing: Deployment Models, Delivery Models, Risks and Research Challenges. International Conference on Computer and Management (CAMAN), pp: 1 – 4. DOI: 10.1109/CAMAN.2011.5778816.

[33] N.Ghosh and S.K.Ghosh, 2012. An approach to identify and monitor SLA parameters for storage-as-a-service cloud delivery model . IEEE Globecom Workshops (GC Wkshps), pp: 724 – 729. DOI: 10.1109/GLOCOMW.2012.6477664.

[34] T.Anstett, F. Leymann, R.Mietzner and S. Strauch, 2009. Towards BPEL in the Cloud: Exploiting Different Delivery Models for the Execution of Business Processes. World Conference on Services - I, pp: 670 – 677. DOI: 10.1109/SERVICES-I.2009.32.

[35] Irena Bojanova and A. Samba, 2011. Analysis of Cloud Computing Delivery Architecture Models. IEEE Workshops of International Conference on Advanced Information Networking and Applications (WAINA), pp: 453 – 458. DOI: 10.1109/WAINA.2011.74.

[36] J.Gibson, R. Rondeau, D. Eveleigh and Qing Tan, 2012. Benefits and challenges of three cloud computing service models. Fourth International Conference

on Computational Aspects of Social Networks (CASoN), pp: 198 – 205. DOI: 10.1109/CASoN.2012.6412402.

[37]. Pradnyesh Rane, 2010. Securing SaaS Applications: A Cloud Security Perspective for Application Providers,"Information Systems Security, http://www.infosectoday.com/Articles/Securing_SaaS_Applications.htm. (Accessed on April 12, 2013).

[38] Eric Ogren, 2009. Whitelists SaaS modify traditional security, tackle flaws, http://searchcloudsecurity.techtarget.com/news/2240181882/Gartner-forecasts-rising-interest-in-cloud-based-security-services. (Accessed on April 25, 2013).

[39] Robert Minnear, 2011. Latency: The Achilles Heel of Cloud Computing. Cloud Expo: Article, Cloud Computing Journal. http://cloudcomputing.sys-con.com/node/1745523. (Accessed on April 12, 2013).

[40] Meiko Jensen, Jorg Schwenk, Nils Gruschka, Luigi Lo Iacon, 2009. On technical Security Issues in Cloud Computing. Proc. of IEEE International Conference on Cloud Computing (CLOUD-II, 2009), India, pp. 109-116. DOI: 10.1109/CLOUD.2009.60.

[41] R. L Grossman, 2009. The Case for Cloud Computing. IT Professional, 11(2): pp. 23-27.

[42] Bernd Grobauer, Tobias Walloschek and Elmar Stöcker, 2010. Understanding Cloud-Computing Vulnerabilities. IEEE Security and Privacy, pp. 99. DOI: 10.1109/MSP.2010.115.

[43] D. Gollmann, 2008 . Securing Web Applications. Information Security Technical Report. 13(1). DOI: 10.1016/j.istr.2008.02.002.

[44] Mashups, SaaS and Cloud Computing: Evolutions and Revolutions in the Integration Landscape. http://www.redad.org/summerschool09/slides/Bentallah_CTDS09_Mashups%20and%20SaaS.pdf. (Accessed on April 12, 2013).

[45] Krishna tej Koganti, Eswar Patnala, Sai Sagar Narasingu. J.N. Chaitanya, 2013. Virtualization Technology in Cloud Computing Environment. International Journal of Emerging Technology and Advanced Engineering, 3 (3): 771-773.

[46] Security Considerations White Paper for Cisco Smart Storage. Cisco Systems. 2010. http://www.cisco.com/en/US/docs/storage/nass/csbcdp/smart_storage/white_paper/Security_Considerations_OL-23025.pdf. (Accessed on March 24, 2013).

[47] V.Saravanan, Dr.A.Sumathi, 2012. Dynamic Handoff Decision Based on Current Traffic Level and Neighbor Information in Wireless Data Networks. International Conference on Advanced Computing. DOI: 10.1109/ICoAC.2012.6416797.

[48] V. Saravanan, A. Sumathi, 2012 . Handoff Mobiles with Low Latency in Heterogeneous Networks for Seamless Mobility: A Survey and Future Directions", European Journal of Scientific Research. 81(3): 417-424.

[49] V.Saravanan, Dr.A.Sumathi, S.Shanthana and M.Rizvana, 2013. Dual Mode Mpeg Steganography Scheme For Mobile and Fixed Devices. International Journal of Engineering Research and Development, 6 (3): 23-27. DOI: 0603.067X.0023.

Biographies

PROF. V.SARAVANAN received his **B.Sc.** degree in Computer Science from Periyar University, Salem, Tamilnadu, in 2003, the **M.Sc.** degree in Computer Science from Thiruvalluvar University, Vellore, Tamilnadu, in 2005, the **MCA** degree from Periyar University, Salem, Tamilnadu, the **M.Phil** degree in Computer Science from Periyar University, Salem, Tamilnadu, and the **M.E.** degree in Computer Science and Engineering from the Anna University, Chennai, Tamilnadu, in 2008. Currently, he is pursuing **Ph.D.** degree in Computer Science and Engineering from Anna University, Chennai, Tamilnadu. At present he is an Assistant Professor of IT Department at P.S.V. College of Engineering and Technology, Krishnagiri, Tamilnadu, affiliated to Anna University Chennai. His teaching and research areas include Mobile Computing, Image Processing, Security and Cloud Computing. He has more than 10 International publications.

PROF. S.THIRUKUMARAN is an Assistant Professor in Department of Computer Applications at Adhiyamaan college of Engineering, Hosur, He received his **MCA** degree in Madras University in 2000 and he is continuing his **Ph.D.** degree in Data Mining in Anna University, Chennai. So for he has published five papers in International Journals under mining concept and his area of interest is Data Mining Content Retrieval and Cloud Computing.

Ms. M.ANITHA, is an Assistant Professor in Department of Computer Applications at Adhiyamaan college of Engineering, Hosur. She received her **B.Sc.** degree in Computer Science in Marudhar Kesari Jain College for Women, affiliated to University of Madras, Vaniyambadi, in 2003 and **MCA** degree in Priyadarshini Engineering College, affiliated to Anna University, Chennai, in 2008. Her area of interest is Cloud Computing and Security.

Ms S.SHANTHANA received her **B.E.** degree in Computer Science and Engineering from Anna University, Chennai, Tamilnadu, in 2012, Currently, she is pursuing **M.E.** degree in P.S.V. College of Engineering and Technology, Krishnagiri, Tamilnadu, affiliated to Anna University, Chennai, Tamilnadu. She has two international publications and her area of interest is Cloud Computing, Image Processing and Security.