A Privacy Preserving Representation for Web Service Communicators' in the Cloud

D. Chandramohan[1], T. Vengattaraman[1], D. Rajaguru[2], R. Baskaran[3], and P. Dhavachelvan[1]

[1] Department of Computer Science, Pondicerry University, India
[2] Dept.of Inf.Technology, Perunthalaivar Kamarajar Inst.of Eng. & Technology, Karaikal
[3] Department of Computer Science and Engineering, Anna University, Chennai, India
{pdchandramohan,vengat.mailbox,raja.guru42, dhavachelvan}@gmail.com, baaski@cs.annauniv.edu

Abstract. The present paper focuses on maintaining one's data secrecy in cloud storage area and it may depend on their privacy policy and standards. The effectiveness and efficiency of preserved data from different cloud providers should maintain the integrity of original data stored in it. In the era of could computing, stored information's value, proficiency and optimization of data retrieving spotlights the importance of maintaining cloud users data, privacy, identity, reliability and maintainability it may vary for different Cloud providers (CP). Giant CP ensures their user proprietary information's are sustained more secretly using cloud technologies. During third party cloud services and exodus between inter cloud providers may lead to data portability privacy issue. More remarkable event in this case, even the cloud providers don't have implication about the information and records where it's stored and maintained in their own cloud. This is one of the obligatory research issue in cloud computing. We came frontward by proposing (EMPPC) an Evolutionary model based privacy Preserving technique and try to hold user's, to have trust in providers for maintaining their confidentiality in cloud. This proposal helps the CR (Cloud Requester and Users) to mark trust on their proprietary information and data's stored in cloud.

Keywords: Cloud computing, Web Service, Privacy, Security, Intelligent Computing, Data Portability, Intrusion Detection System, lattice.

1 Introduction

Cloud is one of the massive and major research areas for both industrial and academic field for research, many researchers have been working towards its research issues. As cloud came into existence lot of issues also surrounded to it. Normally cloud computing have most common and general issues like Interoperability, SLA-(Service level Agreement), [3-10] universal standards, unique approach for all cloud providers, data portability among different clouds, various privacy and security issues etc. Cloud computing is not a one-size-fits-all elucidation and companionship required to

K. Singh, A.K. Awasthi, and R. Mishra (Eds.): QSHINE 2013, LNICST 115, pp. 496–506, 2013.

uncover the need earliest before business into such solutions. CP consists of different layer for information dealing out with an on-demand provisioning of computational resources.

Data Portability Policy and Data Freedom

A cloud provider came across the issues of data portability in the way that users have a request of it. We are initiating a model which may help to frame an open standard because we believe in advancing this open effort. [1-6], However the CP should not permitted to change their policy on demand of their own. Very few cloud provider companies has already launched portability policies. Fig.1 the portability policy proposal is still in its preschooler stages and will nurture as awareness increases, with more unambiguous questions emerging when issues are recognized. CP and SN (social network) providers will need to pay finicky consideration to the projected right for users to port their personal information to another CP, as well as their right to erase their information. Fig.1. [9-21], The right for CR to port their data to a new CP will also be of an explicit anxiety to SN whose servers continue to edge over with user information. The right for CR to involve along with CP to relocate their data to a new CP and it should promote cloud shopping. This will encourage larger antagonism between cloud providers. One of the most valuable weapons for CRs have in their hand is to switch different providers. This is an idyllic policy that should be pursued by all CP. The initiative by means of data Liberation campaign is to be welcomed, even if it residue vague whether the actual motive is to reduce the cloud competitors in maintaining their data container, rather than making customers free from CP data. There are some considerable difficulties to truly liberal cloud users due to data migration policy. [19-26], The policy framing bench is responsible to act in response to its customers if any information exploitation happens.

Practical Challenges

a) Any policy right must illustrate a fetish between a CR data and their fundamental rights to use of it. [5-9]
b) The policy right should be limited to liberate the data held by the cloud provider. [3-7]
c) Whatever the data transferred between different CPs will relay on the configuration of the data format and interfaces they are using, some CPs store data in the favored format for data exchange internally. [11-18]
d) Different CP data format is harder to understand and it may not be portable while transferring data to a new CP. [20-26]
e) The exact raw data is easier to transfer but difficult to maintain its secrecy.

Promoting a Privacy Market and Industry Standards

Cloud requestors very frequently may change their provider based on the providers advance privacy preservation techniques adopted and assurance to CR, [22] there may

be some Pit fall if some exploration happens to user's data after adapted to new privacy policy of CPs. Many researchers have been repeatedly initiating to frame an [17-19] universal standard format which helps a provider to permit other business competitive provider to gasp different CPs technology, and it should be compatible to new CP technology which makes an effortless transform, can be achievable to normalize the user personal information and data. These migration possibilities should be informed to all CR and users as different cost for porting their data.

2 Background and Related Work

In his approach Anna et al [1] the author addresses the quandary of safeguarding privacy in trust consultation. He initiates the notion of privacy preserving discovery, with a set that does not include attributes or credentials, or combinations of these, which may negotiate privacy. [3] To obtain privacy preserving disclosure sets, he proposed two techniques based on the notions of substitution and generalization. Keith Frikken et al [2006] in his work he presented few protocols that protect both sensitive credentials and sensitive policies as privacy preserving mechanism. Travis D et al [2008] his research team propose a method to support the software engineering effort to derive security requirements from regulations; in which the methodology for directly extracting access rights and obligations from regulation texts. [8-9] The methodology provides statement-level coverage for an entire regulatory document to consistently identify and infer six types of data access constraints and assign required priorities between access rights and obligations to avoid unlawful information disclosures. Alex X et al and team in [2011] they propose a VGuard framework with efficient protocol that allows a cloud policy owner and a cloud request owner to collaboratively determine whether the request satisfies the policy without the policy owner knowing the request and the request owner knowing the policy. Pengcheng Xiong et al and team [6] proposes a cost-aware resource management system based on SLA- service level agreement termed as SmartSLA which consists of two main components: the system modelling module and the resource allocation decision module. To prevent the online social community the author Dongsheng Li et al [7] came forward to propose an interest group based privacy-preserving recommender system called Pistis. By identifying inherent item-user's interest groups and separating user's private interests from their public interests. Multi-agent based service accessing and security system flow discussed by authors et al [2], [4], [5], [12], [15-16] The author Xiaohui Liang et al [12] proposed the privacy preserving emergency call scheme by enabling patients in life-threatening emergencies to fast and accurately transmit emergency data to the nearby helpers via mobile healthcare social networks. The author Chien-Ding Lee et al [2011] similarly the authors discussed the necessity of secure web services and mitigation of the same in cloud [10-14], [17-22] in his approach he made few regulation to comply with the HIPAA (Health Insurance Portability and Accountability Act), a flexible cryptographic key management solution is proposed to facilitate interoperations among the applied cryptographic mechanisms. Author et al proposed an efficient service cache in an peer

to peer networking which simulates the idea of deliver the service in most stipulated period of time [23], Sachin Kadloor et al [16] proposal to develop a dynamic program to compute the optimal privacy preserving policy that minimizes the correlation between user's traffic and adversary's waiting times of cloud user. Chun-Tao Hong et al [18] propose a new MapCG model as a Map-Reduce framework to provide source code level portability between CPUs (Central processing units) and GPUs (Graphics processing units). D.Chandramohan et al [15] proposed a testbed for evaluating the efficiency of services and these features are inherited in our proposed model for driving new parameters and functions to maintain the privacy and its security in cloud environment during data portability or migration between different cloud Providers'.

3 Proposed Model

This approach focus on portability issue in cloud, a user can hold their account details and information along with respective trusted cloud providers, it get pursued until the user mark their uncomfortable with particular CP. Even cloud provider suggestion may be unsuccessful during back tracking the client information maintained by them. They do not have a clear identification where the actual data resides inside their CP cloud. By using this proposal our main objective is to resolve this issue at a minimum risk and maximum benefit to both the providers and users.

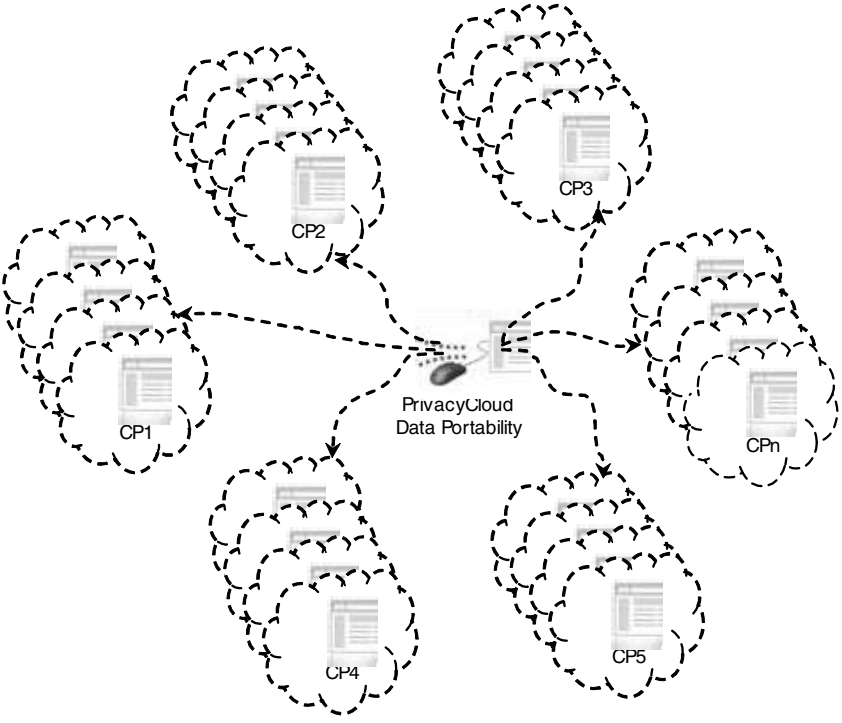

Fig. 1. Privacy Breach in Inter Cloud Portability and Data Migration

The proposed impend strenuous on resolving issues such as adaptability, scalability, reliability, privacy and security, to access the client information as ubiquitous local services virtually in any system. If a user what's to withdraw all his data from one cloud and wish to transfer his data to another cloud, here comes the data portability and its privacy issues. With an open standard and privacy policies cloud computing can able to achieve portability with a huge percentage as freely and loosely coupled with all cloud providers with standard application via internet with in user authorized control. Security is one of the most important frames for cloud provider it will utilize data storage and transmission encryption, user authentication, and authorization, all cloud user concern about the liability of isolated data accessed by criminals like hackers, intruders, and annoyed employees. Cloud providers are extremely aware to this problem and applied extensive possessions to extenuating this kind of distress. Reliability also one of the main issues to feel uncomforted with cloud providers both financially and technologically trustworthy in current market. By using superfluous storage technique some CPs modifying the original data stored with them and lead to signing off from one provider to another. Ownership to CR data has been transferred to the cloud; some users concern that they could lose several data or CP thinks all of their rights are incapable to protect the rights of their beloved customers. Many CP are concentrating on this issue with full standard policy for user and providers benefited agreements.

$$\text{Sim}\,(C_1, C_2) = e^{-ch} \cdot \frac{e^{\beta h} - e^{-\beta h}}{e^{\beta h} + e^{-\beta h}} \tag{1}$$

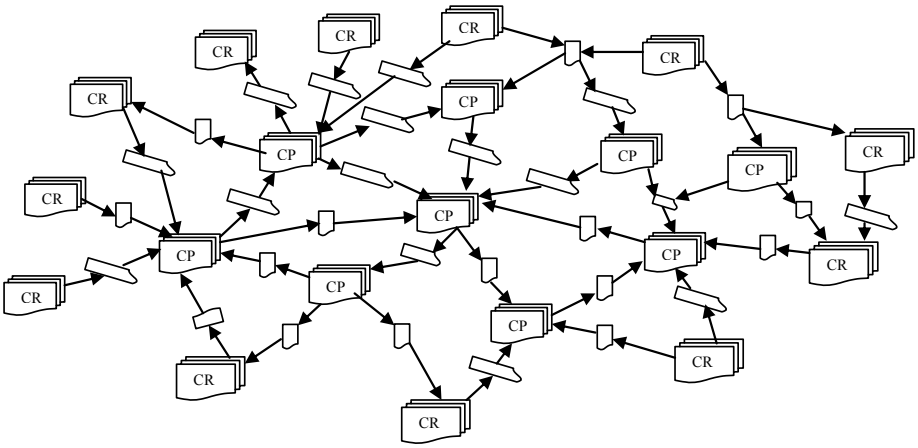

Fig. 2. Privacy EMPPC Intelligent model for Preserving Cloud Users Data

Like this agreement users would be prudent to seek recommendation from their beloved authorized delegates. Data backup CP surplus servers and regulates data backing processes, but some CP worry about being able to manage their own support. Many cloud providers are now presenting data chuck onto medium or allowing cloud users to back up data through ordinary downloads. Data portability and conversion

some CR and users are worried that they wish to switch cloud providers; they may have complicated in relocating their data. Porting and exchanging data is highly reliant on the environment of the CPs data reclamation arrangement, fussy in personal belongings where the configuration cannot be effortlessly revealed. As service antagonism nurtures until some open standards befall established, the data portability issue will be more ease, and adaptation progression will be offered by sustaining more accepted cloud providers with some conditions like a cloud users or CR should pay for some ritual data exchange. Supporting multiplatform and more are big issue for IT sector using direct services, the cloud-based service assimilates athwart different environment and operating systems, and some personalized amendment of the service acquire of any new problem into it. Multiplatform sustainment and its necessities will show the simplicity as more user edges are converted into normal web-based system supports. Intellectual Property originates few new features and to use CP as part of the discovery. Once some CP recognizes that computing makes potentially experiences much more of the same fortune as owned new faceplates the proprietary systems, for low-risk processes and for insensible information, the cloud-based services can be endorsed, established, tartan, and made more protected by merging them with habitual non-cloud IT practices.

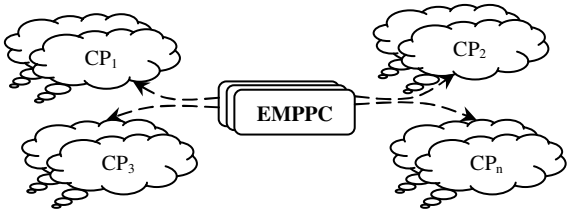

Fig. 3. An Evolutionary Model Based Communicators' Privacy Preserving in the Cloud

In this innovative and competitive cloud world a mammoth development in all related areas. There presents 200 percentage chance of switch over from one provider to some other providers. If a user what's to withdraw all his data from one cloud and wish to transfer his data to another cloud, here comes the data portability and its privacy issues. Designing an Evolutionary model using Intrusion detection system protocol is developed by sharing information based intrusion detection system and the proposed system is embedded in all cloud layer and its neighborhood nodes to provide privacy and security to those data.

$$Cd_A\,(x_i, x_j) = (x_i - x_j)^I\, A\, (x_i - x_j) \tag{2}$$

$$CS_A\,(x_i, x_j) = x_i^T\, A\, xj \tag{3}$$

3.1 Some Properties of ID-Intrusion Detection System Used in EMPPC

Alert / Alarm, True Positive, False Positive, False Negative, True Negative, Noise, Site policy, Site Policy awareness, Confidence value, Alarm filtering, Attacker

identification, Masquerader (Duplicate), Misfeasor, Clandestine user (User act as an Administrator)

$$CD(x,y)=(max\{log\, f(x), log\, f(y)\}\, log\, f(x,y))/ \quad (4)$$
$$log\,[\,M\,min\,[\,\{\,[log\,]\,[f\,(x), log\,[\,f\,(y)\,]\,]\,\}\,]\,]$$

$$\frac{\sum_{(n.m)\in A} Sim\, l(n.m)}{|\,P_1\,| + |\,P_2\,|} \quad (5)$$

$$CC_{IN}\left(p_i, t_j\right) = K, \forall\, k > 1 \quad (6)$$

CP- Cloud Provider, CR- Cloud Requestors Fig.3. EMPPC -The proposed Evolutionary model illustrates many preprocessed approaches to check all promising

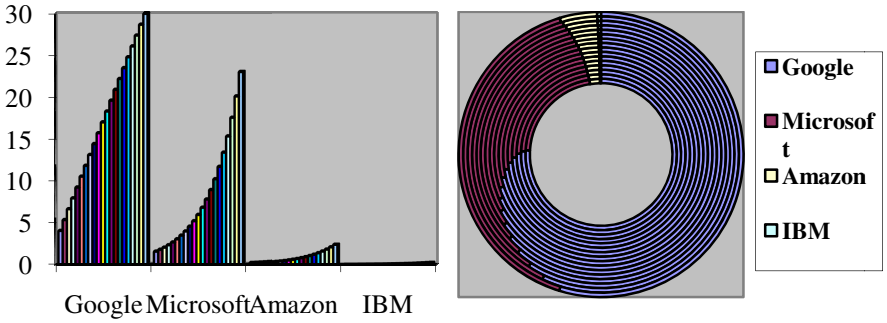

Fig. 4. Cloud Service Privacy Assessment of different providers and Interoperability evaluation in normal scenario

Fig. 6. Cloud Service Privacy with different provider's Evaluation in Medium scenario

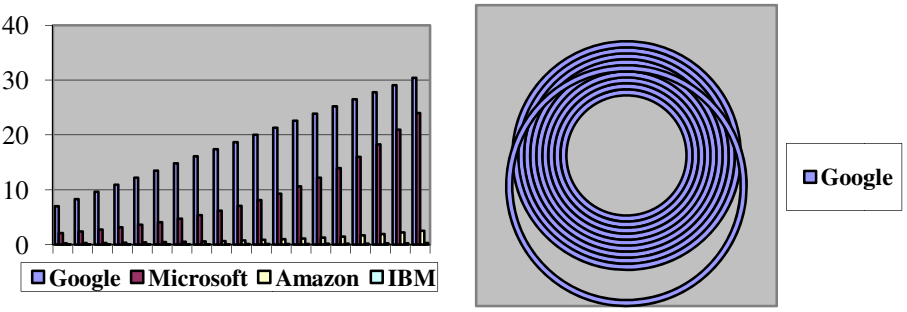

Fig. 5. Cloud Service Privacy Breach Evaluation in Typical Mode

Fig. 7. Cloud Service Privacy Evaluation in Custom Mode with Proposed System Approach from providers perception

Table 1. Cloud Service Privacy assessment of different providers evaluation in normal scenario

Google	Microsoft	Amazon	IBM
4.0	1.5194	0.1589	0.0166
5.3	1.7406	0.1820	0.0190
6.6	1.9941	0.2085	0.0218
7.9	2.2845	0.2389	0.0250
9.2	2.6171	0.2737	0.0286
10.5	2.9982	0.3135	0.0328
11.8	3.4348	0.3592	0.0376
13.1	3.9350	0.4115	0.0430
14.4	4.5080	0.4714	0.0493
15.7	5.1644	0.5401	0.0565
17.0	5.9165	0.6187	0.0647
18.3	6.7780	0.7088	0.0741
19.6	7.7651	0.8120	0.0849
20.9	8.8958	0.9303	0.0973
22.2	10.1912	1.0657	0.1114
23.5	11.6752	1.2209	0.1277
24.8	13.3754	1.3987	0.1463
26.1	15.3231	1.6024	0.1676
27.4	17.5544	1.8357	0.1920
28.7	20.1106	2.1030	0.2199
30.0	23.0391	2.4093	0.2519

Table 2. Cloud Service Privacy evaluation in Typical Mode

Google	Microsoft	Amazon	IBM
10.0	2.8455	0.2976	0.0311
11.3	3.2598	0.3409	0.0356
12.6	3.7345	0.3905	0.0408
13.9	4.2783	0.4474	0.0468
15.2	4.9014	0.5126	0.0536
16.5	5.6151	0.5872	0.0614
17.8	6.4327	0.6727	0.0703
19.1	7.3695	0.7706	0.0806
20.4	8.4426	0.8829	0.0923
21.7	9.6720	1.0114	0.1058
23.0	11.0805	1.1587	0.1212
24.3	12.6940	1.3274	0.1388
25.6	14.5425	1.5208	0.1590
26.9	16.6601	1.7422	0.1822
28.2	19.0861	1.9959	0.2087
29.5	21.8655	2.2865	0.2391

Table 3. Cloud Service Privacy breach with different providers evaluation in Medium scenario

Google	Microsoft	Amazon	IBM
7.0	2.0793	0.2174	0.0227
8.3	2.3820	0.2491	0.0260
9.6	2.7289	0.2854	0.0298
10.9	3.1263	0.3269	0.0342
12.2	3.5815	0.3745	0.0392
13.5	4.1031	0.4291	0.0449
14.8	4.7006	0.4916	0.0514
16.1	5.3851	0.5631	0.0589
17.4	6.1692	0.6451	0.0675
18.7	7.0676	0.7391	0.0773
20.0	8.0968	0.8467	0.0885
21.3	9.2758	0.9700	0.1014
22.6	10.6265	1.1112	0.1162
23.9	12.1739	1.2731	0.1331
25.2	13.9467	1.4585	0.1525
26.5	15.9776	1.6708	0.1747
27.8	18.3043	1.9141	0.2002
29.1	20.9697	2.1929	0.2293
30.4	24.0233	2.5122	0.2627

Table 4. Cloud Service Privacy evaluation in Custom Mode with different providers

Over all Web Service Suitability x; f(x); f'(x); f''(x)		
No of services	**Suitability**	**Providers**
100	10	Google
100	25.2	Microsoft
100	40.4	Amazon
100	55.6	IBM
100	70.8	Sales force
100	86	VMware
100	101.2	Verizon
100	116.4	Accenture
100	131.6	Sodexo
100	146.8	Infosys Technologies

customs to locate the portability between cloud providers. It will act as a gateway for all providers and reveille the privacy actions throughout some malicious attacks experience for the period of portability surrounded by different cloud providers. This paper discusses about portability issues and privacy technique to solve those portability problem occurring for users and cloud providers. Above properties illustrates the technique adopted to maintain the secrecy of any proprietary information. Fig.2 and fig. 3 will give an apparent idea to researches about the proposed work. Equation (1-6) describes the privacy implications in the proposed system. Data migration and its possibilities are expressed if a user currently using CP_1 he can able to migrate to CP_n possibilities as per the compatibility of different cloud providers, the proposed system handles the situation more appropriately and it notifies to all CPs to maintain a standard format to avoid the compatibility issues.

Different privacy invasion have been tremendously increasing in day today life. As privacy breach protection and mitigation stagey the proposed approach acts accordingly. The service provider utilized various privacy techniques to drop down these issues and those representations are tabulated in Table 1, 2, 3 and 4. These invasion handling are plotted and expressed in fig.4, fig.5, fig.6 and fig.7. In vast storage data centers like grid, cloud and distributed storage area are identified as an enormous data breach happening gradually. Table 1 explains the different cloud providers privacy policy, have get varied as per their norms, most of the factors are enriched to be hidden and almost all leading providers are committed to persuade their customers with their attractive policy.

4 Conclusion

This paper proposes an evolutionary privacy model for data portability privacy in cloud which persuades the subsistence of cloud users to have enough trust on cloud providers and co-cloud users. It encompasses both CP and Cloud User (CU) with self and mechanized systems. Most cloud providers don't put forward and missed to mark the practice of privacy techniques. In our paper we came up with various privacy protection techniques and explored them as survival of the fittest in cloud environment. Similarly table 2, 3 and 4 explore the privacy breach of providers taken into consideration according to its recognition. Proposed approach get fulfilled only when both cloud providers and cloud requestors / end-users ensures all their data have their own privacy in different cloud provider during data portability. The future research focuses on portability in interoperable privacy issues, researchers can hope this proposal will prove to be a useful foundation for solving their issues on privacy for cloud layer in all stipulated areas.

Acknowledgement. This work is a part of the Research Project sponsored under the Major Project Scheme, UGC, India, Reference No: F. No. 40-258/2011 (SR), dated 29 June 2011. The authors would like to express their thanks for the financial support offered by the Sponsored Agency.

References

1. Squicciarini, A.C., Bertino, E., Ferrari, E., Ray, I.: Achieving Privacy in Trust Negotiations with an Ontology-Based Approach. IEEE Transactions on Dependable and Secure Computing 3(1), 13–30 (2006)
2. Victer Paul, P., Saravanan, N., Jayakumar, S.K.V., Dhavachelvan, P., Baskaran, R.: QoS enhancements for global replication management in peer to peer networks. Future Generation Computer Systems 28(3), 573–582 (2012)
3. Vengattaraman, T., Abiramy, S., Dhavachelvan, P., Baskaran, R.: An Application Perspective Evaluation of Multi-Agent System in Versatile Environments. International Journal on Expert Systems with Applications 38(3), 1405–1416
4. Abirami, S., Baskaran, R., Dhavachelvan, P.: A survey of Keyword spotting techniques for Printed Document Images. Artificial Intelligence Review 35(2), 119–136 (2011)
5. Victer Paul, P., Vengattaraman, T., Dhavachelvan, P.: Improving efficiency of Peer Network Applications by formulating Distributed Spanning Tree. In: Proceedings - ICETET 2010, pp. 813–818 (2010)
6. Xiong, P., Chi, Y., Zhu, S., Moon, H.J., Pu, C., Hacıgumus, H.: Intelligent Management of Virtualized Resources for Database Systems in Cloud Environment. In: IEEE ICDE Conference 2011, pp. 87–98 (2011)
7. Li, D., Lv, Q., Xia, H., Shang, L., Lu, T., Gu, N.: Pistis: A Privacy-Preserving Content Recommender System for Online Social Communities. In: 2011 IEEE/WIC/ACM International Conferences on Web Intelligence and Intelligent Agent Technology, pp. 79–86 (2011)
8. Venkatesan, S., Dhavachelvan, P., Chellapan, C.: Performance analysis of mobile agent failure recovery in e-service applications. International Journal of Computer Standards and Interfaces 2(1-2), 38–43 ISSN:0920-5489
9. Chandramohan, D., Veeraiah, D., Shanmugam, M., Balaji, N., Sambasivam, G., Khapre, S.: SVIP-enhanced security mechanism for SIP based voIP systems and its issues. In: Meghanathan, N., Nagamalai, D., Chaki, N. (eds.) Advances in Computing & Inform. Technology. AISC, vol. 176, pp. 81–86. Springer, Heidelberg (2012)
10. Vengattaraman, T., Dhavachelvan, P.: An Agent-Based Personalized E-Learning Environment: Effort Prediction Perspective. In: IEEE-IAMA 2009 (2009)
11. Dhavachelvan, P., Uma, G.V., Venkatachalapathy, V.S.K.: A New Approach in Development of Distributed Framework for Automated Software Testing Using Agents. International Journal on Knowledge Based Systems 19(4), 235–247 (2006)
12. Liang, X., Lu, R., Chen, L., Lin, X. (Sherman) Shen, X.: PEC: A Privacy-Preserving Emergency Call Scheme for Mobile Healthcare Social Networks. IEEE Journal of Communications and Networks 13(2), 102–112 (2011)
13. Dhavachelvan, P., Uma, G.V.: Reliability Enhancement in Software Testing – An Agent-Based Approach for Complex Systems. In: Das, G., Gulati, V.P. (eds.) CIT 2004. LNCS, vol. 3356, pp. 282–291. Springer, Heidelberg (2004)
14. Dhavachelvan, P., Uma, G.V.: Multi-agent Based Integrated Framework for Intra-class Testing of Object-Oriented Software. In: Yazıcı, A., Şener, C. (eds.) ISCIS 2003. LNCS, vol. 2869, pp. 992–999. Springer, Heidelberg (2003)
15. Chandramohan, D., Jayakumar, S.K.V., Khapre, S., Nanda Kishore, M.S.: DWSE-Simulator For Distributed Web Service Environment. IEEE ICRTIT 2011, 1203–1208 (2011)

16. Kadloor, S., Gong, X., Kiyavash, N., Venkitasubramaniam, P.: Designing Router Scheduling Policies: A Privacy Perspective. IEEE Transactions on Signal Processing 60(4), 2001–2012 (2012)
17. Carlson, M.: Systems and Virtualization Management: Standards and the Cloud (A report on SVM 2011). Journal of Network and Systems Management (2012)
18. Hong, C.-T., Chen, D.-H., Chen, Y.-B., Chen, W.-G., Zheng, W.-M.: Providing Source Code Level Portability Between CPU and GPU with MapCG. Journal of Computer Science and Technology 27(1), 42–56 (2012)
19. Chandramohan, D., Vengattaraman, T., Basha, M.S.S., Dhavachelvan, P.: MSRCC – mitigation of security risks in cloud computing. In: Meghanathan, N., Nagamalai, D., Chaki, N. (eds.) Advances in Computing & Inform. Technology. AISC, vol. 176, pp. 525–532. Springer, Heidelberg (2012)
20. Nanda Kishore, M.S., Jayakumar, S.K.V., Satya Reddy, G., Dhavachelvan, P., Chandramohan, D., Soumya Reddy, N.P.: Web Service Suitability Assessment for Cloud Computing. In: Wyld, D.C., Wozniak, M., Chaki, N., Meghanathan, N., Nagamalai, D. (eds.) NeCoM/WeST/WiMoN 2011. CCIS, vol. 197, pp. 622–632. Springer, Heidelberg (2011)
21. Saleem Basha, M.S., Dhavachelvan, P.: Web Service Based Secure E-Learning Management System- EWeMS. International Journal of Convergence Information Technology 5(7), 57–69 ISSN: 1975 9320
22. Dhavachelvan, P., Uma, G.V.: Complexity Measures For Software Systems: Towards Multi-Agent Based Software Testing Proceedings. In: ICISIP 2005, pp. 359–364 (2005)
23. Victer Paul, P., Saravanan, N., Baskaran, R., Dhavachelvan, P.: Efficient service cache management in mobile P2P networks. Future Generation Computer Systems (2012) ISSN 0167-739X, doi:10.1016/j.future.2012.12.001