ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 1, January 2015

Further Investigations on Methods Developed for Preserving Privacy of Computational Grids

R.S.Venkatesh[1], P.K.Reejeesh[2], Prof.S.Balamurugan[3], S.Charanyaa[4]

Department of IT, Kalaignar Karunanidhi Institute of Technology, Coimbatore, TamilNadu, India[1,2,3]

Senior Software Engineer Mainframe Technologies Former, Larsen & Tubro (L&T) Infotech, Chennai, TamilNadu, India[4]

ABSTRACT: This paper reviews methods developed for anonymizing data from 2001 to 2003 . Publishing microdata such as census or patient data for extensive research and other purposes is an important problem area being focused by government agencies and other social associations. The traditional approach identified through literature survey reveals that the approach of eliminating uniquely identifying fields such as social security number from microdata, still results in disclosure of sensitive data, k-anonymization optimization algorithm ,seems to be promising and powerful in certain cases ,still carrying the restrictions that optimized k-anonymity are NP-hard, thereby leading to severe computational challenges. k-anonimity faces the problem of homogeneity attack and background knowledge attack . The notion of l-diversity proposed in the literature to address this issue also poses a number of constraints , as it proved to be inefficient to prevent attribute disclosure (skewness attack and similarity attack), l-diversity is difficult to achieve and may not provide sufficient privacy protection against sensitive attribute across equivalence class can substantially improve the privacy as against information disclosure limitation techniques such as sampling cell suppression rounding and data swapping and pertubertation. This paper aims to discuss efficient anonymization approach that requires partitioning of microdata equivalence classes and by minimizing closeness by kernel smoothing and determining ether move distances by controlling the distribution pattern of sensitive attribute in a microdata and also maintaining diversity.

KEYWORDS: Data Anonymization, Microdata, k-anonymity, Identity Disclosure, Attribute Disclosure, Diversity

I. INTRODUCTION

Need for publishing sensitive data to public has grown extravagantly during recent years. Though publishing demands its need there is a restriction that published social network data should not disclose private information of individuals. Hence protecting privacy of individuals and ensuring utility of social networ data as well becomes a challenging and interesting research topic. Considering a graphical model [35] where the vertex indicates a sensitive label algorithms could be developed to publish the non-tabular data without compromising privacy of individuals. Though the data is represented in graphical model after KDLD sequence generation [35] the data is susceptible to several attacks such as homogeneity attack, background knowledge attack, similarity attacks and many more. In this paper we have made an investigation on the attacks and possible solutions proposed in literature and efficiency of the same.

II. MOVING FROM SECURITY TO DISTRIBUTED TRUST IN UBIQUITOUS COMPUTING ENVIRONMENTS

We will be able to access the resources and services of a ubiquitous computing from anywhere at any time. This results in many security issues. The present security method focuses on authentication and access control. For consideration we put forward a method for improving the security by adding a trust. Only if the user has right to access a resource, he is allowed to use the resource.

Combination of a ubiquitous computer with hand-held and embedded devices will give more services to the user. The main objective of a ubiquitous computer is to provide more intelligent service which are accessible even to

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 1, January 2015

mobile users through a smart office scenario. For this purpose, "centaurus" was developed. But unexpectedly many security risks were observed in centaurus.

So a best and suitable approach is "distributed trust". Policies were initiated for access control, authentication and delegation. If a user is found with a capacity to use a service, then it is considered that the user has the "right" to access the service. A delegator can humble pass on the rights to a delegate. This is called as delegation.

Distributed Trust Management is helpful in solving trust problems without using authentication, but by using public key with access control. A security policy gives a group of paradigms for authorization, access control and trust. Each and every domain providing services should pass these security policies. A domain makes use of security agents and delegations make use of authorized agents. A delegation is viewed as giving permission to itself. That is, only the user having right to delegate a service can practically delegate that service and also the capacity to delegate can itself be delegated.

Trusted agents are provided with some privileges. A trusted agent helps a user to delegate service to other user whom they trust so a delegation chain is obtained. The chain is broken if and only if the requirements of a user are unsatisfied.

Generally, a user can send a request to security agent seeking to use the service under it. The security agent will produce some authorization certificates that are given to users as "tickets" to access the service. The security agent recognizes a delegation depending upon the policy of delegator and delegate. "XML Signatures" are used to solve the privacy issue in distributed networks.

In order to see the ubiquitous computing in reality, we need to add distributed trust to the security infrastructure. The trust will provide more flexibility and easy to services.

III. TOWARDS TRUST – AWARE RESOURCE MANAGEMENT IN GRID COMPUTING SYSTEMS

A Grid computing system implements resource management using techniques like sandboxing, encryption and access control methods. But the overhead seen in these methods causes the system to degrade. Hence we use a resource management algorithm to implement "trust" in the system.

The demanding situations that occurs in Grid system due to resource management are

i. Geographical distribution of resources.
ii. Resource heterogeneity.
iii. Usage of grid domains having their own policies and practices.
iv. Grid domains using different access and cost models.

When the resources are distributed commonly, we need to take into account of "Quality of services" and "Security" issues. Hence "resource management systems" are encouraged to decide the allocation of resources. The main objective of trust – aware resource management system is to minimize the security overhead by using Resource Management Systems. A "trust relationship" is provided among the resource consumer and resource provider.

A Grid system is partitioned into many grid domains (GD) in which a single administrator controls the set of resources and clients. Each GD is related to a resource domain and a client domain. Every resource domain includes ownership, set of type of activity and trust level. Client domain also includes certain attributes that are related to client. On behalf of client and resource, there exists two "Required Trust Levels".

In order to integrate the quality of service within the resource management system, we are intended to use trust – aware resource management algorithms. When the request from the client is received, the trust – aware resource management scheduler distributes the resources on the basis of

i. Centralized scheduler organization.
ii. Non – preemptive task execution.
iii. Indivisible tasks.

With the help of resource management algorithms, all the clients requests are combined to form a single "meta request". Few simulations were carried out to test the performance of resource management algorithms. As a result, the performance was increased when the algorithms are "trust – aware".

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 1, January 2015

IV. SECURITY FOR GRID SERVICES

Grid computing is responsible for exchanging and diverse use of resources in distributed "Virtual Organizations". The web service mechanisms are implemented for the necessity of privileged network services.

Virtual Organization (VO) includes set of users and related resources or services. Security barriers like certification and authorization are observed while managing and controlling resources in a Virtual Organization. To resolve these barriers, the Virtual Organization is treates as a "Bridge".

In general, the users and resources in a Virtual Organization are controlled by the policies and standards formulated by classical organizations. To access a particular resource, we need a "binary trust relationship" between

i. A local user and their organization.
ii. The VO and the user.

A grid security model should possess the following three functionalities.

i. Multiple security mechanisms.
ii. Dynamic creation of services/resources.
iii. Dynamic establishment of trust domains.

A user – driven security model is required for formulating policies and standards for controlling resources in VO. A Globus Toolkit version 2 (GT2) security model provides services for Grid Allocation and Management of resources, Monitoring & Discovering and Data Movement. The GT2 provides proxy certificates and community authorization services. If these security services are satisfied, the user can be trusted.

The Globus Toolkit version 3 (GT3) is integrated using Open Grid Services Architecture (OGSA) which defines few web services and their behavior. GT3 makes use of HTTP, Simple Object Access Protocol (SOAP), Web Services Description Language (WSDL) and security related protocols.

A Grid computing must emphasis certain security mechanisms like authentication, authorization, credential conversion, auditing and delegation to perform a secure operation. The Gt3 incorporated using OGSA derives well – defined protocols for many security services like credential processing service, authorization service, credential conversion service, identity mapping service and audit. Using a hosting environment, the interaction of services/resources will be secured.

The GT3 has two main benefits when compared to GT2.

i. GT3 makes use of web services – uses security protocols and standards.
ii. Tight least-privilege model – GT3 makes use of minimum or no privileged services.

The GT3 is designed to be compatible with GT2. GT3 also provides a complex service called Grid Resource Allocation and Management (GRAM). This allows a remote client to interact with the resources needed in a secure manner.

V. CONCLUSION AND FUTURE WORK

Various methods developed for anonymizing data from 2001 to 2003 is discussed. Publishing microdata such as census or patient data for extensive research and other purposes is an important problem area being focused by government agencies and other social associations. The traditional approach identified through literature survey reveals that the approach of eliminating uniquely identifying fields such as social security number from microdata, still results in disclosure of sensitive data, k-anonymization optimization algorithm ,seems to be promising and powerful in certain cases ,still carrying the restrictions that optimized k-anonymity are NP-hard, thereby leading to severe computational challenges. k-anonimity faces the problem of homogeneity attack and background knowledge attack . The notion of l-diversity proposed in the literature to address this issue also poses a number of constraints , as it proved to be inefficient to prevent attribute disclosure (skewness attack and similarity attack), l-diversity is difficult to achieve and may not provide sufficient privacy protection against sensitive attribute across equivalence class can substantially improve the privacy as against information disclosure limitation techniques such as sampling cell suppression rounding and data swapping and pertubertation. Evolution of Data Anonymization Techniques and Data Disclosure Prevention Techniques are discussed in detail. The application of Data Anonymization Techniques for several spectrum of data

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 1, January 2015

such as trajectory data are depicted. This survey would promote a lot of research directions in the area of database anonymization.

REFERENCES

1. Pieter Van Gorp and Marco Comuzzi "Lifelong Personal Health Data and Application Software via Virtual Machines in the Cloud" IEEE Journal of Biomedical and Healthcare Informatics, Vol. 18, No. 1, Jan 2014
2. Sape J. Mullender, Andrew S.Tanenbaum, "Protection and Resource Control in Distributed Operating Systems", 1984.
3. Paul J.Levine, "Computer security system for a time shared computer accessed over telephone lines US 4531023 A, 1985
4. John G.Campbell,Carl F.Schoeneberger,"Remote hub television and security systems", US 4574305 A, 1986.
5. A Pfitzmann, "Networks without user observability", Computers & Security 6/2 (1987) 158-166, 1987
6. TF Lunt, " Automated audit trail analysis and intrusion detection: A survey" In Proceedings of 11th National Conference on Security, 1988
7. Lichtenstein Eric Stefan 1984 a, Computer control medical care system US4464172.
8. ARalph R.Frerichs, Dr. PH.Robert A. Miller 1985, Introduction of a Microcomputer for Health Research in a Developing Country.
9. Steven P.Brown 1986, Combinational Medical Data, Identification and health Insurance card.
10. Peter P. Gombrich, Richard J. Beard, Richard A. Griffee, Thomas R. Wilson, Ronald E. Zook, Max S. Hendrickson 1989,A Patient care system,US4835372 A.
11. Paavo T. Kousa, " VOICE NETWORK SECURITY SYSTEM" US 4797672 A, 1989
12. D Graft, " Methodology for network security design", IEEE Transactions on Computers, 1990
13. Heberlein, "Network Security MONITOR, 1991
14. John R. Corbin, " Apparatus and method for licensing software on a network of computers US 5138712 A", 1992
15. S Gordon, "Computer Network Abuse", 1993.
16. Neil Bodick, Andre L. Marquis1990, Interactive system and method for creating and editing a knowledge base for use as a computerized aid to the cognitive process of diagnosis,US4945476 A.
17. Angela M. Garcia, Dr.,Boca Raton 1991 a, System and Method for scheduling and Reporting Patient related services including prioritizing services,US5974389 A.
18. Clark Melanie Ann, John Finley, Huska; Michael Edward, Kabel; Geoffrey Harold, Graham, Marc Merrill 1991 b,System and Method for scheduling and Reporting Patient Related services.
19. Robert W. Kukla1992,Patient care communication system, US5101476 A
20. Mark C. Sorensen 1993, Computer aided medical diagnostic method and apparatus, US5255187 A.
21. Edward J. Whalen, San Ramon, Olive Ave Piedmont 1994,Computerized file maintenance System for managing medical records including narrative patent documents reports.
22. Desmond D. Cummings 1994b,All care health management system, US5301105 A.
23. Woodrow B. Kesler Rex K Kesslerin 1994 c,Medical data draft for tracking and evaluating medical treatment.
24. Joseph P. Tallman, Elizabeth M. Snowden, Barry W. Wolcott 1995, Medical network management system and process, US5471382 A.
25. Peter S. Stutman, J. Mark Miller 1996,Medical alert distribution system with selective filtering of medical information
26. Edwin C. Iliff1997,computerized medical diagnostic system including re-enter function and sensitivity factors, US5594638 A.
27. Timothy Joseph Graettinger, Paul Alton DuBose 1998, Computer-based neural network system and method for medical diagnosis and interpretation. US5839438 A.
28. Melanie Ann Clark, John Finley Gold, Michael Edward Huska, Geoffrey Harold Kabel, Marc Merrill Graham1999,Medical record management system and process with improved workflow features, US5974389 A.
29. Richard S. Surwit, Lyle M. Allen, III, Sandra E. Cummings 2000 a, Systems, methods and computer program products for monitoring, diagnosing and treating medical conditions of remotely located patients, US6024699 A.
30. Jeffrey J. Clawson 2000 b, Method and system for giving remote emergency medical counsel to choking patients, US6010451 A.
31. Marc Edward Chicorel 2001, Computer keyboard-generated medical progress notes via a coded diagnosis-based language, US6192345 B1.
32. Charlyn Jordan2002, Health analysis and forecast of abnormal conditions.
33. Jeffrey J. Clawson2003, Method and system for an improved entry process of an emergency medical dispatch system
34. PekkaRuotsalainen 2004, A cross-platform model for secure Electronic Health Record communication.
35. Roger J. Quy2005, Method and apparatus for health and disease management combining patient data monitoring with wireless internet connectivity, US6936007 B2.
36. Avner Amir, Avner Man2006 a, System and method for administration of on-line healthcare, WO2006006176 A2.
37. Paul C.Tang, Joan S. Ash, David W. Bates, J. Marc overhage and Daniel Z.Sands 2006 b, Personal Health Records: Definitions, Benefits, and Strategies for Overcoming Barriers to Adoption.
38. Christopher Alban, KhiangSeow2007, Clinical documentation system for use by multiple caregivers.
39. Brian A. Rosenfeld, Michael Breslow2008, System and method for accounting and billing patients in a hospital environment.
40. Jacquelyn Suzanne Hunt, Joseph Siemienczuk 2009, Process and system for enhancing medical patient care.
41. Richard J. Schuman2010, Health care computer system, US7831447 B2.
42. Kanagaraj, G.Sumathi, A.C.2011,Proposal of an open-source Cloud computing system for exchanging medical images of a Hospital Information System
43. AvulaTejaswi, NelaManoj Kumar, GudapatiRadhika, SreenivasVelagapudi 2012 a, Efficient Use of Cloud Computing in Medical Science.
44. J. Vidhyalakshmi, J. Prassanna 2012 b, Providing a trustable healthcare cloud using an enhanced accountability framework.
45. Carmelo Pino and Roberto Di Salvo 2013, A Survey of Cloud Computing Architecture and Applications in Health.
46. K.S. Aswathy, G. Venifa Mini 2014 a, Secure Alternate Viable Technique of Securely Sharing the Personal Health Records in Cloud.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 1, January 2015

47. Abhishek Kumar Gupta, Kulvinder Singh Mann 2014 sharing of Medical Information on Cloud Platform.
48. D. C. Kaelber, A. K. Jha, D. Johnston, B. Middleton, and D. W. Bates, "Viewpoint paper: research agenda for personal health records (PHRs),"J. Amer. Med. Inform. Assoc., vol. 15, no. 6, pp. 729–736, 2008.
49. J. Ahima, "Defining the personal health record," vol. 76, no. 6, pp. 24–25, Jun. 2005.
50. W. Currie and M. Guah. "Conflicting institutional logics: a national programme for it in the organizational field of healthcare:, Journal of Information Technology, 22:235–247,2007.
51. M. Gysels, A. Richardson, and J. I. Higginson "Does the patient-held record improve continuity and related outcomes in cancer care: a systematic review", Health Expectations,10(1):75–91, Mar. 2007.
52. International Organization for Standardization. ISO TR20514:2005 Health Informatics - Electronic Health Record Definition, Scope and Context Standard. International Organization for Standardization (ISO). Geneva, Switzerland,2005.
53. B.Powmeya , Nikita Mary Ablett ,V.Mohanapriya,S.Balamurugan,"An Object Oriented approach to Model the secure Health care Database systems,"In proceedings of International conference on computer , communication & signal processing(IC^3SP)in association with IETE students forum and the society of digital information and wireless communication,SDIWC,2011,pp.2-3
54. Balamurugan Shanmugam, Visalakshi Palaniswami, "Modified Partitioning Algorithm for Privacy Preservation in Microdata Publishing with Full Functional Dependencies", Australian Journal of Basic and Applied Sciences, 7(8): pp.316-323, July 2013
55. Balamurugan Shanmugam, Visalakshi Palaniswami, R.Santhya, R.S.Venkatesh "Strategies for Privacy Preserving Publishing of Functionally Dependent Sensitive Data: A State-of-the-Art-Survey", Australian Journal of Basic and Applied Sciences, 8(15) September 2014.
56. S.Balamurugan, P.Visalakshi, V.M.Prabhakaran, S.Chranyaa, S.Sankaranarayanan, "Strategies for Solving the NP-Hard Workflow Scheduling Problems in Cloud Computing Environments", Australian Journal of Basic and Applied Sciences, 8(15) October 2014.
57. Charanyaa, S., et. al., , A Survey on Attack Prevention and Handling Strategies in Graph Based Data Anonymization. International Journal of Advanced Research in Computer and Communication Engineering, 2(10): 5722-5728, 2013.
58. Charanyaa, S., et. al., Certain Investigations on Approaches forProtecting Graph Privacy in Data Anonymization. International Journal of Advanced Research in Computer and Communication Engineering, 1(8): 5722-5728, 2013.
59. Charanyaa, S., et. al., Proposing a Novel Synergized K-Degree L-Diversity T-Closeness Model for Graph Based Data Anonymization. International Journal of Innovative Research in Computer and Communication Engineering, 2(3): 3554-3561, 2014.
60. Charanyaa, S., et. al., , Strategies for Knowledge Based Attack Detection in Graphical Data Anonymization. International Journal of Advanced Research in Computer and Communication Engineering, 3(2): 5722-5728, 2014.
61. Charanyaa, S., et. al., Term Frequency Based Sequence Generation Algorithm for Graph Based Data Anonymization International Journal of Innovative Research in Computer and Communication Engineering, 2(2): 3033-3040, 2014.
62. V.M.Prabhakaran, Prof.S.Balamurugan, S.Charanyaa," Certain Investigations on Strategies for Protecting Medical Data in Cloud", International Journal of Innovative Research in Computer and Communication Engineering Vol 2, Issue 10, October 2014
63. V.M.Prabhakaran, Prof.S.Balamurugan, S.Charanyaa," Investigations on Remote Virtual Machine to Secure Lifetime PHR in Cloud ", International Journal of Innovative Research in Computer and Communication Engineering Vol 2, Issue 10, October 2014
64. V.M.Prabhakaran, Prof.S.Balamurugan, S.Charanyaa," Privacy Preserving Personal Health Care Data in Cloud" , International Advanced Research Journal in Science, Engineering and Technology Vol 1, Issue 2, October 2014
65. P.Andrew, J.Anish Kumar, R.Santhya, Prof.S.Balamurugan, S.Charanyaa, "Investigations on Evolution of Strategies to Preserve Privacy of Moving Data Objects" International Journal of Innovative Research in Computer and Communication Engineering, 2(2): 3033-3040, 2014.
66. P.Andrew, J.Anish Kumar, R.Santhya, Prof.S.Balamurugan, S.Charanyaa, " Certain Investigations on Securing Moving Data Objects" International Journal of Innovative Research in Computer and Communication Engineering, 2(2): 3033-3040, 2014.
67. P.Andrew, J.Anish Kumar, R.Santhya, Prof.S.Balamurugan, S.Charanyaa, " Survey on Approaches Developed for Preserving Privacy of Data Objects" International Advanced Research Journal in Science, Engineering and Technology Vol 1, Issue 2, October 2014
68. S.Jeevitha, R.Santhya, Prof.S.Balamurugan, S.Charanyaa, " Privacy Preserving Personal Health Care Data in Cloud" International Advanced Research Journal in Science, Engineering and Technology Vol 1, Issue 2, October 2014.
69. K.Deepika, P.Andrew, R.Santhya, S.Balamurugan, S.Charanyaa, "Investigations on Methods Evolved for Protecting Sensitive Data", International Advanced Research Journal in Science, Engineering and Technology Vol 1, Issue 4, Decermber 2014.
70. K.Deepika, P.Andrew, R.Santhya, S.Balamurugan, S.Charanyaa, "A Survey on Approaches Developed for Data Anonymization", International Advanced Research Journal in Science, Engineering and Technology Vol 1, Issue 4, Decermber 2014.
71. S.Balamurugan, S.Charanyaa, "Principles of Social Network Data Security" LAP Verlag, Germany, ISBN: 978-3-659-61207-7, 2014
72. S.Balamurugan, S.Charanyaa, "Principles of Scheduling in Cloud Computing" Scholars' Press, Germany,, ISBN: 978-3-639-66950-3, 2014
73. S.Balamurugan, S.Charanyaa, "Principles of Database Security" Scholars' Press, Germany, ISBN: 978-3-639-76030-9, 2014

APPENDIX

S.no	YEAR	AUTHORS	TITLE
1	1984	Sape .MULLENDER and Andrew S TANENBAUM	PROTECTION AND RESOURCE CONTROL IN DISTRIBUTED OPERATING SYSTEMS
2	1985	Paul j.Levine	COMPUTER SECURITY SYSTEM FOR TIME SHARED COMPUTER ACCESSED OVER TELEPHONE LINES
3	1986	Norman Hardy	COMPUTER SYSTEM SECURITY

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 1, January 2015

4	1987	Andreas Pfitzmann, Michael Waidner	NETWORKS WITHOUT USER OBSERVABILITY
5	1988	Chris J. Mitchell	KEY STORAGE IN SECURED NETWORK
6	1989	Fred C. Piper	VOICE NETWORK SECURITY SYSTEM
7	1990	Donald Graji Mohnish Pabrai Uday Pahrai	METHODOLOGY FOR NETWORK SECURITY DESIGN
8	1991	L. Todd Heberlein	NETWORK SECURITY MONITOR
9	1992	John R. Corbin	APPARATUS AND METHOD FOR LICENSING SOFTWARE ON A NETWORK OF COMPUTERS
10	1993	Michael P.	COMPUTER NETWORK ABUSE
11	1994	Bruce E. McNair	SYSTEM AND METHOD FOR GRANTING ACCESS TO A RESOURCE
12	1995	Scott D. Hammersley, Arthur D. Smet, Peter M. Wottreng	METHOD AND APPARATUS FOR INTRAPROCESS LOCKING OF A SHARED RESOURCE IN A COMPUTER SYSTEM
13	1995	Daniel B. Clifton	RESOURCE ACCESS SECURITY SYSTEM FOR CONTROLLING ACCESS TO RESOURCES OF DATA PROCESSING SYSTEM
14	1996	Wei-Ming Hu	METHOD AND APPARATUS FOR AUTHENTICATING A CLIENT TO A SERVER COMPUTER SYSTEMS WHICH SUPPORT DIFFERENT SECURITY MECHANISMS
15	1997	Mark S. Miller, E. Dean Tribble, Norman Hardy, Christopher T. Hibbert	DIVERSE GOODS ARBITRATION SYSTEM AND METHOD FOR ALLOCATING RESOURCES IN A DISTRIBUTED COMPUTER SYSTEM
16	1998	Ian Foster, Carl Kesselman,Gene Tsudik, Steven Tuecke	A SECURITY ARCHITECTURE FOR COMPUTATIONAL GRIDS
17	1999	Daniel S. Glasser, Ann Elizabeth McCurdy, Robert M. Price	METHOD AND SYSTEM FOR CONTROLLING USER ACCESS TO A RESOURCE IN A NETWORK COMPUTING ENVIRONMENT
18	2000	Rajkumar Buyya, David Abramson, and Jonathan Giddy	AN ARCHITECTURE FOR A RESOURCE MANAGEMENT AND SCHEDULING SYSTEM IN A GLOBAL COMPUTATIONAL GRID
19	2001	Lalana Kagal, Tim Finin and Anupam Joshi	MOVING FROM SECURITY TO DISTRIBUTED TRUST IN UBIQUITOUS COMPUTING ENVIRONMENT
20	2002	Farag Azzedin and Muthucumaru Maheswaran	TOWARDS A TRUST-AWARE RESOURCE MANAGENT IN GRID COMPUTING SYSTEM
21	2003	Von Welch1 Frank Siebenlist2 Ian Foste	SECURITY FOR GRID SERVICES

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 1, January 2015

22	2004	Ivan Krsul, Arijit Ganguly, Jian Zhang	VMPLANTS:PROVIDING AND MANAGING VM EXECUTION ENVIRONMENTS FOR GRID COMPUTING
23	2005	Daniel Olmedilla1, Omer F. Rana2, Brian	SECURITY AND TRUST ISSES IN SEMANTIC GRIDS
24	2006	David S. Linthicum	MOVING TO CLOUD COMPUTING STEP BY STEP
25	2007	Uzi Dvir	SECURITY SERVER IN THE CLOUD
26	2008	Mladen A. Vouk	CLOUD COMPUTING-ISSUES,RESEARCH AND IMPLEMENTATIONS
27	2009	Meiko Jensen,	ON TECHNICAL ISSUES OF CLOUD COMPUTING
28	2010	S. Subashini n, V.Kavitha	SECURITY ISSUES FOR CLOUD COMPUTING
29	2011	Luis M. Vaquero	SECURITY ISSUES IN CLOUD COMPUTING
30	2012 I	Deyan Chen1, Hong Zhao	DATA SECURITY AND PRIVACY PRESERVATION IN CLOUD COMPUTING
31	2012 A	Mohammed A. AlZain ,	CLOUD COMPUTING SECURITY SINGLE-MULTI CLOUDS
32	2013 C	Ming Li,	SCALABLE AND SECURE SHARING OF PERSONAL HEALTH RECORDS
33	2013 B	Miltiadis Kandias,	INSIDER THREAT IN CLOUD COMPUTING
34	2013 A	Niroshinie Fernando	MOBILE CLOUD COMPUTING-SURVEY
35	2014 D	Diogo A. B. Fernandes	SURVEY ISSUES IN CLOUD COMPUTING
36	2014 B	Md Whaiduzzaman	SURVEY ON VEHICULAR CLOUD COMPUTING
37	2014 A	A.Madhuri1, T.V.Nagaraju	RELIABLE SECURITY IN CLOUD COMPUTING ENVIRONMENT
38	2015 A	IbrahimAbaker	RISE OF BIG DATA ON CLOUD COMPUTING-REVIEW AND OPEN ISSUES
39	2015	TargioHashem	RISE OF CLOUD COMPUTING ARCHITECTURE IN BIG DATA
40	2015D	Gavin O Donnell,	CLOUD COMPUTING
41	2016	Sundas Iftikhar, Anum Tariq,	OPTIMAL TASK ALLOCATION ALGORITHM FOR COST MINIMIZATION AND LOAD BALANCING OF GSD TERMS
42	2016	Hamed Rezaei, Behdad Karimi, and Seyed Jamalodin	EFFECT OF CLOUD COMPUTING SYSTEM IN TERMS OF SERVICE QUALITY OF KNOWLEDGE MANAGEMENT SYSTEM
43	2017	Thanh Dat Dang	A FRAMEWORK FOR CLOUD BASED SMART HOME
44	2018	Christian Biener, Martin	INSURABILITY OF CYBER RISK

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 1, January 2015

BIOGRAPHY

R.S.Venkatesh and P.K.Reejeesh are currently pursuing their B.Tech. degree in Information Technology at KalaignarKarunanidhi Institute of Technology, Coimbatore, Tamil Nadu, India. Their areas of research interests include Network Security, Cloud Computing and Database Security.

Prof.S.Balamurugan obtained his B.Tech degree in Information Technology from P.S.G. College of Technology, Coimbatore, Tamil Nadu, India and M.Tech degree in Information Technology from Anna University, Tamil Nadu, India respectively. He is currently working towards his PhD degree in Information Technology at P.S.G. College of Technology, Tamil Nadu, India. At present he holds to his credit **65 papers International Journals and IEEE/ Elsevier International Conferences.** He is currently working as Assistant Professor in the Department of Information Technology, Kalaignar Karunanidhi Institute of Technology, Coimbatore, Tamil Nadu, India affiliated to Anna University TamilNadu, India. He is **State Rank holder** in schooling. He was **University First Rank holder** M.Tech. Semester Examinations at Anna University, Tamilnadu, India. He served as a Joint Secretary of IT Association, Department of Information Technology, PSG College of Technology, Coimbatore, Tamilnadu, India. He is the **recipient of gold medal and certificate of merit** for best journal publication by his host institution **consecutively for 3 years**. Some of his professional activities include invited Session Chair Person for two Conferences. He has guided 16 B.Tech projects and 2 M.Tech. projects. He has won a best paper award in International Conference. His areas of research interest accumulate in the areas of Data Privacy, Database Security, Object Modeling Techniques, and Cloud Computing. He is a life member of ISTE,CSI. **He has authored a chapter in an International Book "Information Processing" published by I.K. International Publishing House Pvt. Ltd, New Delhi, India, 978-81-906942-4-7. He is the author of 3 books titled "Principles of Social Network Data Security", ISBN: 978-3-659-61207-7, "Principles of Scheduling in Cloud Computing" ISBN: 978-3-639-66950-3, and "Principles of Database Security", ISBN: 978-3-639-76030-9.**

S.Charanyaa obtained her **B.Tech** degree in Information Technology and her **M.Tech** degree in Information Technology from Anna University Chennai, Tamil Nadu, India. She was **gold medalist** in her B.Tech. degree program. She has to her credit **27 publications in various International Journals and Conferences**. Some of her outstanding achievements at school level include **School First Rank holder** in **10^{th} and 12^{th} grade**. She was working as Software Engineer at Larsen & Turbo Infotech, Chennai for 3 years where she got promoted as Senior Software Engineer and worked for another 2 years. She worked at different verticals and worked at many places including Denmark, Amsterdam handling versatile clients. She is also the recipient of **best team player award for the year 2012 by L&T**. Her areas of research interest accumulate in the areas of Database Security, Privacy Preserving Database, Object Modeling Techniques, and Cloud Computing. **She is the author of 3 books titled "Principles of Social Network Data Security", ISBN: 978-3-659-61207-7, "Principles of Scheduling in Cloud Computing" ISBN: 978-3-639-66950-3, and "Principles of Database Security", ISBN: 978-3-639-76030-9.**