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 Evolution of Approaches Developed For Database Security

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 1989 to 1993 . 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.

The remainder of the paper is organized as follows. Section 2 deals about voice network security systems. Section 3 deals about methodology for network security design. Computer Network abuse is depicted in Section 4. Section 5 concludes the paper and outline the direction for Future Work.

II. VOICE NETWORK SECURITY SYSTEMS

Paavo T. Kousa (1989) say voice network security systems reveals a secure environment for exchanging attacker to gain access when the voice message is transferred among users. The voice message is transferred among users. The important thing to be noted is that the voice message is exchanged between the users of remote locations.

In earlier network message system, the users mailbox was used to save the voice messages. In this system, first the voice message is loaded into the request, the message is distributed among the receivers. But the main drawback is the interruption of those messages created by an intruder with the voice message. Even encryption algorithms can be employed to exchange voice message. But still this is not appropriate for all the networks and also these system seems to be more expensive.

The recent network security systems consists of a base station and node station. Every message is encrypted and included in the message transmit protocol and then it is transmitted to the receiver.
The secret key and a public key both used for encryption. These two keys are used at the initial stage of producing a key. Each and every content of all the messages is encrypted and decrypted using the key produced before.

Initially, the base station selects a random number and adds it with the node encryption key and sends it to the respective key and sends it to the respective node station. The node station retains that random number by decrypting the message. This random number is used as a root for producing more random numbers. The node station encrypts the message with second random number and sends it to base station. Now base stations decodes and retains the random number. By this way the real information to be transmitted is exchanged between the base and node stations. This will result in a secure communication. The attacker will feel hard to access the voice message system.

Any number of node station can be employed in a network security system. Base station and node station exchanges messages bi-directionally. Before they transmit messages the base station will send a wake-up signal to the node station. In turn the node station will send a ready signal to base station. After this the connection is established and they start transferring messages.

Before transmitting the message , a checksum is also added to the message to identify the existence of attackers. But checksum is not employed to the system because it will erode the security altering technique of the system. Sometimes checksum are used in the systems to detect errors. A "checksum verifier" is used for testing the checksum used.
During the transfer of message, the base system's identification is sent to node station and the node systems identification is received by the base station.

This system provide secure way of exchanging messages between base and node stations. Eliminates the attackers to gain access to the system.

III. METHODOLOGY FOR NETWORK SECURITY DESIGN

D Graft (1990) says Security becomes the major issue in all network communication systems. To overcome this security issue, a new methodology for network security systems was designed with the help of OSI model and security architecture. This type of design methodology is required because the earlier designs like "ad hoc" did not show good results. So, the main aim is to identify the workability of this design methodology.

Design methodology for network security consists of three phases:
1.Specification phase-gathers all the system requirements and defines certain set of conditions to design.
2.Design phase-explains the system architecture, service mechanisms and protocols used.
3.Implementation Phase-Validation and verification analysis of performance and workability.
"Problem-centered Approach" is employed in specification phase. That is , prior to designing and implementing process, the problem to be solved is first analyzed properly. There are two components in a specification phase:
1.Identifying Requirements-the requirements are based upon the problem that we have taken. In a completely insecure system, the requirements will be more to protect the system whereas in a secure system, the requirements will be less. Anyway the tame idea is to increase the security that the system provides.
Initial step in identifying the requirements is to select a proper domain where all security services will function effectively. The security services and protocols to be used is collected in the name of application requirements. A detailed study is made on the security services used. Security management comprises of requirements needed for the management of security. Additionally, the key distribution methods are used for solving management issues.

2.Defining conditions- There are three basic conditions that we have to consider for designing. They are applicable standards, Network type and topology and organization.

10.15680/ijircce.2015.0301044

A proper solution for the problem is designed in the design phase. The solution should fulfill the requirements specified in the specification phase. This phase defines the overall architecture of the security system. The security architecture includes all the functions needed to maintain the ”security” in a system. These functions are inserted into the 7 layers of OSI Model. However, placing all these functions in OSI Model will have many risks. The security mechanisms and the protocols are selected appropriately on the basis of conditions and services needed for the system. The protocol should not erode the security of the system.

Heberlein (1991) In the implementation phase, the design is developed into working product by distributing the design to the various software and hardware that are needed for verification and validation, testing obtaining performance and workability-satisfies all the requirements.

We have studied a new methodology for network security systems. But still we have few drawbacks. More concentration is required to select the appropriate security protocols. Security mechanisms and security protocols can’t be detached from each other. It does not support new developments. We can use this new design methodology for simple applications only.

John R. Corbin (1992) in this paper the author inform us that inorder to install the Network Security Monitor(NSM),either one of the following commands are used to install NSM from the tar file tar xvf nsm,tar while for the NSM distributed on tape, use tar xv command. Both the command will produce a new directory called NSM in the local directory. In this paper the author describes an detailed information about each and every command which is used for creating a file structure,and the operations that will be performed to attain a desired task.

IV. COMPUTER NETWORK ABUSE

Un authorization of data and manipulation of data by an intruder are the main computer abuses seen in “cyberspace”. Computer abuse is an illegal act in communication technology.

“The Alleged Problem” observes the computer abuses in a network. It is categorized into three subsections. The computer crime and security falls under first subsection. It examines whether the user accessing the system is authorized or not. Also tells about the usage and cost expenditure of methods employed. The second subsection observes the crimes committed by attackers. The third subsection represents the computer abuses in media.

Remote computing is the biggest advantage for computer users. It allows a user to access the computer from a remote location. But the drawback that we come across in remote computing is authentication. The general form that we user for authentication is passwords. Even though if a unique and strong password is used, an attacker gains access to the computer system very easily by guessing the passwords. So using a password is not a good idea for securing computer systems.
Password protection method remains insecure among local users also. “Shoulder-surfing” is a method used by the hackers to find the passwords. Apart from password authentication . we have many other methods to reduce the abuse in a system. Some of them are encryption techniques and call-back systems. Only a user in remote location can access the encrypted data sent using telephone lines. In call-back system, only a remote user with unique phone no can access the target system.

Among local users, biometric and mechanical systems of authentication were used to reduce local abuses. Biometric system includes voice and fingerprint. Mechanical system includes insertion of magnetic card. But these are not used every time because they are very expensive. In addition , privacy of a user seem to be a drawback in these systems. Still if we improve the computer security, the capacity of computer abuses will be reduced.

Now coming into abuse in media, the well known hacker “Kevin Mintick” hacked “Digital Equipment Corporation” by simply tracing telephone lines. Some case studies portrays that there are more “human” hackers than “computer” hackers. The “Hacking Ethic” was used to maintain the system and it allows a faithful hacker to access the computer system but does not cause any destructive to the computer system.

To avoid computer abuses, there are many criminal laws that can be followed. Commonly used one is “State and federal criminal laws”. It consists of three subsections. The first subsection deals with state crime laws. Second sub section deals with federal crime laws. It mainly focus on computer abuses like wire fraud and interstate transportation of stolen property. Eg: computer Fraud and abuse act and Electronic communications Privacy Act. The third sub section deals with the legal proceedings of criminal laws.

Many criminal laws fails because of the following circumstances. They are,
1.Arbitrary Spatial Distinction in cyberspace.
2.Risk in detecting criminal activity.
3.Difficulty in obtaining criminal identity.
4.Difficulty of proving criminal capability.
5.Absense of incentives to report Computer Abuse.
6.Absence of deterrence in criminal laws.

The above circumstances are seen in Ex-post criminalization method. Implementing this method is of no use. To compensate, EX-ANTE prevention method can be employed. Here also we have three subsections. The first two subsections uses indirect federal regulation. The third subsection observes whether the above methods are suitable or not.

The best way to avoid computer abuses is to use EX-ANTE prevention method. It gradually increases the computer security by employing proper sophisticated authorization methods.

V. Conclusion and Future Work

Various methods developed for anonymizing data from 1989 to 1993 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 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.
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^{3}SP)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
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
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