ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 1, January 2015

Further More Investigations on Methods 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 1994 to 1997 . 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. SYSTEM AND METHOD FOR GRANTING ACCESS TO A RESOURCE

This generally deals with permitting access to a system resource and identification whether the user accessing the system is an authorized user or an attacker. An unauthorized user trying to access a resource will result in heavy financial loss.

Access to a resource is controlled based upon two features :

1.User permissions or subject oriented controls.

2.Access control lists or object oriented controls.

Access to a resource is granted easily only when number of subjects /objects are less.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 1, January 2015

Usually, any access control system will involve transactions of both valid and invalid user. The data determined from these transactions are brought from these transactions are brought together into a multidimensional attribute space. This forms a cluster. Every cluster will reveal the behavior of an attribute. Now, to find whether the user accessing resource is an authorized user, we have to compare both attributes of a user accessing resource and attributes obtained from a cluster. From the result, we can identify the type of user accessing the resources.

The type of user identification is depicted in mathematical concepts for well understanding. Multiple records were used to store data derived from transactions. Clusters are derived b analyzing the records using minimum distance modeling technique. Clusters are identified by their coordinate. Relative distances are evaluated to make an access decision.

The mechanisms of access control system is as follows. The two types of records are stored in a processor or a standalone database. One record stores the input of authorized user and the other stores the input of an attacker. Whenever an access is permitted, a "bill" will be produced stating the type of user(valid or invalid). To distinguish between the records, we add a key data field to each record. A cluster locator is used to compare the attributes of accessing user and the attributes of others stored in the database.

This, type of access control system becomes more effective when we use probably analysis rather than using minimum distance consideration. Generally, the probability of acceptance will be high and probability of rejection will be low. The probability both the authorized user and hacker is observed and compared. As per the result, if the probability is high, the user will be permitted to access the resource otherwise , he will be denied.

The recent access control techniques are more effective than prior access control techniques. In case, if there are more resources available, the system can include additional databases. These systems can also be modified to enhance the performance and efficiency.

III. METHOD AND APPARATUS FOR INTRAPROCESS LOCKING OF A SHARED RESORUCE IN A COMPUTER SYSTEM – 1995(I)

In a computer system, the intra process locking technique executes plurality of functions asynchronously with the help of operating system. An access to a shared resource can also be permitted using operating system. If a program included in a process wants to access the shared resource, then a request is sent to the Operating System stating it to lock out all the programs/processes within the system. Often, two types of locks are used – shared locks and exclusive locks.

The term "lock" does not exist in prior computer systems because those systems execute only one task/program at a time. Only after completing the current task, the system allows the next task to execute. Hence locks were not needed. Example of such type of system is DOS. Obliviously, when technology improved the computer users started to perform multiple tasks simultaneously. Every system started performing in multitasking mode.

"Locking" came into existence when multiple tasks were executed at the same time in a computer system. When a "lock" is established only one task can access the resource. All other task running in the system will be restricted to use the resources. But locks used in computer systems will affect the data and system integrity.

The main idea of recent approach is to improve the performance of a system by using intra process locking method to a shared resource. An operating system control and coordinates the computer system. Each and every process is executed asynchronously using Operating System.

A system unit includes a processor which is also connected to workstation controller, memory and shared resource. The memory contains a lock table. A workstation includes keyboard display and input devices. When implemented, the software is executed by the processor and stored in the memory.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 1, January 2015

Generally, a segment of data comprises shared resource and is stored using a space is commonly shared between all the programs and threads. In a computer system, one program can execute multiple threads also multiple programs can 't execute multiple threads.

Whenever a process starts accessing the shared resource, the Operating System will supply key to that particular process taken from the shared resource. At the same time, the Operating System will lock all other processes from accessing the shared resource. The process can keep the key till it completes its operations.

A process can contain many programs. In a "process – level locking" system, if one program needs to access shared resources means, the Operating System will supply key to all the programs included in that process. Then Operating System will supply key to all the programs included in that process. Then Operating System will permit only that particular program to use the shared resource by restricting others. The process-level locking will decrease the performance of the system.

In case of "program-level locking", the Operating System will give the key to only that particular program which needs to access the shared resource. The impact of process-level locking is ignored here.

The lock table in the memory is used to make hash entries. All the hash entries will include a resource address field and a pointer field. Resource address field stores the address of shared resource. The pointer field will be pointing to the first lock entry in the resource address. The lock entry will have next entry field, process field, program field, and lock type field. The next entry field indicates the second lock entry. The lock type field will tell whether the lock is an exclusive or shared lock.

IV. RESOURCE ACCESS SCURITY FOR CONTROLLING ACCESS TO RESOURCES OF DATA PROCESSING SYSTEM – 1995

The data processing system makes use of a resource access security system in order to control the access to resources. Data processing systems includes descriptors to assign addresses in the address spaces to access resources. Both the process and data are established using descriptors.

In a data processing systems, sharing of resources means accessing a database that contains hardware, software and data. The greatest impact on such systems is that the essential data is deleted. Hence some processing systems require multiple security systems for sensitive data protection.

A combined software and hardware protection mechanisms is required to control the information flow in a data processing security systems. First, the security policy of a computer is implemented and the resources in the data processing system are governed by applying access control mechanisms. Next, the user's capability is controlled to execute some operations and perform system administrative responsibilities. Prior to permit the access to use resources, the conventional data processor security system involves password authentication t be performed by the user when requests for the resource.

In order to establish communication between the host computer and terminal, we need to store the identification data in the memory first. Then the identification data is transferred between the host computer and terminal when an access is requested. The communication is established after a coincidence is found between the transferred identification data. But this type of security systems has many drawbacks.

Some conventional data processor made up of ring architecture will increase the security in the system. Highest privilege rings are used for most sensitive and trusted data; Lower privilege rings are used for less sensitive and less trusted data. This type of security system will have many features to access the resources with more privileges. If a trusted process accesses highest privilege rings, then all the sensitive data in that ring will also be accessed. Similarly, if a sensitive data accesses highest privilege rings, then all the trusted process in that ring will also be accessed. A trusted

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 1, January 2015

process control and an access control is separated from each other with the help of orthogonal protection mechanisms. Thus the number of privilege levels are increased.

The orthogonal protection system can be implemented by adding all the resources like data, software, input-output port, cache memory with the help of descriptors are assigned to have an extra privilege levels. Each descriptor will select a resource and adds additional information's of privilege level, classification level and resource address in the data processing system. A domain is used to arrange all the resources required to perform an operation. Information related to this domain is added into the descriptor . The resources are converted into pages to represent classification levels. Now, the information related to classification level and pages are added into descriptors.

The information of address in the address space is also included in the descriptors. The descriptor after including all the information , is represented as a virtual address of the resource. Thus when descriptor tries to access a resource, a descriptor translator will convert the descriptor to determine the real address of the resource.

The descriptor translation requires the data stored in information table. The input from the descriptor to the resource will control the access of a resource. The user privilege level is determined from the domain table. Page table includes page of resources. Resource access security system will allow an access to a resource, if and only if that resource is obtained by a user, domain and page information. Data processing system uses a register to store the user, domain and page information.

In the data processing system, every user is allocated a clearance level that represent classification and domain that represents across privileges. By joining the clearance level that represents classification and domain that represents access privileges. By joining the clearance level with privileges, the user right to access is coined. The privileges states are classified into three states – application state, exception state and supervisor stat. The application privilege helps application processes to run. Exception state is used by exception handlers. Supervisor state has the kernel of the data processing system. All the three states provide control for registers in the data processing system.

The unprivileged instructions are implemented using secure processors. Secure processors also handle jump instructions. It also has permission to access the memory management registers. The secure processor also has a secure register file.

Thus the resource access security system provides a control mechanism to access resources in a data processing system.

V. METHOD AND APPARATUS FOR AUTHENTICATING A CLIENT TO SERVER COMPUTER SYSTEMS WHICH SUPPORT DIFFERENT SECURITY MECHANISMS – 1996

Many security mechanisms are imposed when a client accesses a computer system. "Authentication Gateway" is a security mechanism most commonly used for authentication. It asks for a username and password when a client logins the system. The authentication gateway serves as a proxy server in order to provide an access key to the client. Many users share a common computer resource in a computer network. Hence some computer networks like distributed computing system includes "authentication of users" to share the resources. Generally, in this type of systems some users/computer will ate as "servers" and others will act as "clients".

Usually, a client system will send a request to the server system for a service. Service basically includes accessing a file system or a database. The server system prior to provide service will ask for the user to authenticate. Also authentication of server is required in some client system. As computer networks become large, authenticating of client becomes difficult.

Both client and server do not use same security mechanisms. Usually, the client system will impose a security mechanisms of server will involve a server from the proxy server to imitate the client. Then the client can access the required information from the server through proxy server.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 1, January 2015

Authentication of any user will involve a group of security features that indicates the client to invoke the server. An "access key" is produced to retrieve these security features, and the access key is sent to the client, to invoke the proxy server, we have to send the access key to the proxy server; imitating the client step involves the access key to retrieve the client security features in order to invoke a server.

The authentication gateway system consists of authentication means and proxy server means. The "authentication means" comprises of a log in invoke of a client, given a username and security device, identifying a group of security features, providing an access key for the client. The "proxy server means" comprises of a server invoking a client, security features obtained by using access key, make use of the security features to imitate the client in order to invoke the server.

Client system authentication does not bother about the security protocols used in server system. But the server system will authenticate each and every client before providing service. The complexity will be more when a PC is used as a client system. To overcome this type of complexities, a prior mechanism called "delegation" is employed. Delegation means the client will give its authority to a proxy server to serve as a client. This mechanism also has certain drawbacks. Several other prior methods include embed passwords, modifying a server to act as server and client, etc, also have many issues in terms of security.

The recent mechanism "authentication gateway" serves as an intermediate for client and server systems. This mechanism also suffers from an issue. That is the proxy server does not have the access permission to use the objects of client. But still it has several advantages.

1. A client can access the server after passing the authentication process; no need to modifying the server.
2. Reduces the overhead of a proxy server.
3. Capable of processing with multiple servers.
4. Transparent to all application process of client.
5. Proxy server need not store the secret key of client.
6. The existing mechanism is featured to adopt the future modifications.

VI. DIVERSE GOODS ARBITRATION SYSTEM AND METHOD FOR ALLOCATING RESOURCES IN A DISTRIBUTED COMPUTER SYSTEM – 1997

Diverse foods arbitration is a technique used for allocating users with the computer resources required. This type of technique is referred to multiprocessor computer system , distributed computer system and interconnected computer system.

A resource can be automatically managed if it is cheaper and most probably used for lower-value uses. In contrast, expensive resources are used for higher-value uses. All the low-value uses can be grouped together and applied for high-value uses.

There are four types of allocation methods used for allocating resources in a system. They are

1.FCFS
2. Priority based
3. Prorata allocation method
4. "Single good" auction method.

In FCFS systems, the bandwidth is allocated for each requests and when there is no bandwidth to allocate, the requests are denied.

In a priority based allocation methods, lower priority requests are replaced with higher priority requests when there is no bandwidth to allocate the request. In the single good auction method, the amount of goods needed and the bid price is specified by the requester. There are several techniques used for implementing single good auction method – English auction and Dutch auction. Single good auction method is responsible for satisfying the requests of various requesters by supplying multiple goods simultaneously.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 1, January 2015

The diverse goods arbitration system and method for allocating resources are applied between bidding requesters. This system makes use of a varying "second-price sealed-bid" auction method. Here, the goods are allocated for right price to the right buyers.

A user requesting for a computer resource will transfer a set of bid states to the arbiter. Each bid will reveal the information of resource requested and the bid price for the resource.

The arbiter uses some data stored in it for allocating computer resources and uses additional data for receiving bid slates. The arbiter will select a combination of "winning bid" based on highest bid price. We have to select a second "winning bid" combinations for the next requester.

The architecture of a distributed computer system consists of multiple signal source, subscribers, various users/requesters, switch based communication network. The subscribers requests for bandwidth to allocate resources to the diverse goods agoric arbiter. Then a winning bid combination is identified and the arbiter will send a permit message to allow the users to allocate the system resources. This arbitration process is again implemented if a new bid is found or a network configuration is manipulated.

Sometimes the architecture is associated with a CPU and network interface to store the bid slates sent by the subscribers. An allocation record is used for maintaining the maximum allocation level of each resource. A local memory is also included in the architecture for storing bid prices of the resources. A bid combination pointer is used for indicating all accessible combinations of bids. Thus a distributed computer system makes use of a diverse goods arbitration system and methods for allocating resources between various users.

VII. CONCLUSION AND FUTURE WORK

Various methods developed for anonymizing data from 1994 to 1997 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.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 1, January 2015

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^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

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 1, January 2015

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

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 1, January 2015

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

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 1, January 2015

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