Further More Investigations on Evolution of Approaches and Methodologies for Securing Computational Grids

R.S.Venkatesh¹, P.K.Reejeesh², Prof.S.Balamurugan³, S.Charanyaa⁴

Department of IT, Kalaignar Karunanidhi Institute of Technology, Coimbatore, TamilNadu, India¹²³
Senior Software Engineer Mainframe Technologies Former, Larsen & Tubro (L&T) Infotech, Chennai, TamilNadu, India⁴

ABSTRACT: This paper reviews methods developed for anonymizing data from 2004 to 2006. 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-anonymity 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-anonymity 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 network 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. VM PLANTS: PROVIDING AND MANAGING VIRTUAL MACHINE EXECUTION ENVIRONMENTS FOR GRID COMPUTING – 2004

VM - Virtual Machine plants provide a reliable and flexible environment for problem solving in a grid computing systems. Service oriented architecture is employed to represent VM plant middle for providing VM customization and efficient cloning.
The main objective of this architecture is to provide flexibility, fast VM instantiation, scalability, resilience to failures and interoperability. Flexibility is obtained by applying the cloning process onto various VM technologies. Interoperability is achieved by using efficient cloning mechanisms.

Every users and resource providers select a unique service for distributed computing in VM plant architecture. A “classic” Virtual Machine has the ability to run on different OS. It provides isolation and security mechanisms; supports customization and encapsulation; provide support for legacy applications.

The VM plant architecture works on the basis of services provided within web and grid frame works. The client communicates with the service through VMshop. The service then makes use of standard mechanisms to create a new virtual machine. The client cannot directly access the VM plants. The new instantiated VM’s are used for accessing VM plants. The VMshop can provide secure access to resources; configuring network; gives resources access information; supports query handling.

VM plant uses “Production Process Planner” (PPP) for the process of creating new Virtual Machine. The PPP after receiving a request, selects an exact VM from the VM warehouse. VM information system gives information about currently used machines. VM monitor is used to update the VM information system.

Once the exact Virtual Machine is selected, it has to satisfy the following tests.

i. Subset test
ii. Prefix test
iii. Partial test

After this the Virtual Machine is cloned using VM Production Line. Then the VM should parse on several configuration processes. After cloning and configuration processes are completed, the virtual workspace is combined with n IP address. The cloning and configuration techniques are used for describing the feasibility of the VM. VM Plants architecture is efficient for instantiation of VM clones and flexible for producing new services.

III. SECURITY AND TRUST ISSUES IN SEMANTIC GRIDS – 2005

A large scale distributed computing system such as “Grid computing” should have the ability to allow sharing of resources over a “Virtual Organization” (VO). Recently, the Grid Security Infrastructure (GSI) possesses a trust relationship between Grid Computers. But still there are no suitable methods for authentication and authorization. Even they do not have the ability to select a “trustworthy” user.

“Access Control” is enhanced using Property based authorization mechanisms, automatic certification, bidirectional & iterative security negotiations and policy based authorization. The “Trust Management” includes two basic approaches.

i. Policy - based trust management.
ii. Reputation – based trust management.

The Policy - based trust management reveals certain rules, standards and policies to identify whether a user is “trustworthy” or “untrustworthy”. The Policy - based trust management is responsible for taking access control decisions. The system which posses Policy - based trust makes use of semantics for making decisions.

The Reputation – based trust management concentrates on public - key certificates, P2P system, mobile ad – hoc network and semantic web.

A user to access a resource must satisfy some of the following security mechanisms.

i. Proxy certificates signed by a Certification Authority.
ii. Identity based authorization.
iii. Simple authentication/authorization.
A term called “Community” is introduced in which all the users can communicate with each other efficiently. The introduction of these communities will decrease the cost of interaction. Communities can be formed either implicitly or explicitly. There are four phases in which a trust is achieved in virtual organization.

i. Service provider identification – determines VO objectives.
ii. Formation and service provider invitation – compute community trust and provision resources.
iii. Operation and service provider interaction – trust based service invocation.
iv. Dissolution – terminates the resources.

In Grid Computing, the security and trust issues in a Virtual Organization is computed using policy – based and reputation – based trust management approaches. The basic idea of this paper is to point out the restrictions of resources and access control protection mechanisms seen in Grid Computing.

IV. MOVING TO CLOUD COMPUTING STEP – BY – STEP – 2006

Cloud computing is the extension of SOA which provides resources such as Storage – as – service, Data – as – a – service and platform – as – a – service. The logic is to identify which cloud service can be adopted for the exiting SOA.

A cloud is organized with the help of following services.

i. Testing – as – a – service
ii. Management – as – a – service
iii. Application – as – a – service
iv. Process – as – a – service
v. Information – as – a – service
vi. Database – as – a – service
vii. Storage – as – a – service
viii. Infrastructure – as – a – service
ix. Platform – as – a – service
x. Integration – as – a – service
xi. Security – as – a – service

Security and performance are observed as barriers in cloud. However, cloud does not support all the computing resources. The cloud computing is suitable for cases where
i. Applications, processes and data are independent.
ii. New applications are used.
iii. Web – based platform is used.
iv. Core internal enterprise architecture should be good.

Cloud computing is not suitable when
i. Processes, applications and data are coupled.
ii. High security is needed.
iii. Application is legacy.
iv. The points of integration are not well defined.

The cloud architecture describes about the
i. Business drivers.
ii. Information under management.
iii. Existing services under management.
iv. Core business processes.

There are several steps involved in the process of creating cloud. They are
i. Access the business.
ii. Access the culture.
iii. Access the value.
iv. Understand your services, processes, data and cloud resources.
v. Identify candidate data, services and processes.
vi. Create a governance strategy and security strategy.
vii. Bind candidate services to data and processes.
viii. Relocate services, processes and information.
ix. Implement security, governance and operations.

V. CONCLUSION AND FUTURE WORK

Various methods developed for anonymizing data from 2004 to 2006 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-anonymity faces the problem of homogeneity attack and background knowledge attack. The notion of 1-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), 1-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 perturbation. 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
8. ARalph R. Friechis, Dr. PH. Robert A. Miller 1985, Introduction of a Microcomputer for Health Research in a Developing Country.
16. Neil Bodick, Andre L. Marquiss 1990, Interactive system and method for creating and editing a knowledge base for use as a computerized aid to the cognitive process of diagnosis US 4945476 A.
17. Angela M. Garcia, Dr. Boca Ratom 1991 a, System and Method for scheduling and Reporting Patient related services including prioritizing services, US 5974389 A.
22. Desmond D. Cummings 1994 b, All care health management system, US 5301105 A.
International Journal of Innovative Research in Science, Engineering and Technology
(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 1, January 2015


25. Peter S. Stutman, J. Mark Miller 1996, Medical alert distribution system with selective filtering of medical information

26. Edwin C. Illif1997, computerized medical diagnostic system including re-enter function and sensitivity factors, US5594638 A.


30. Jeffrey J. Clawson 2000 b, Method and system for giving remote emergency medical counsel to choking patients, US6010451 A.


33. Jeffrey J. Clawson 2003, Method and system for an improved entry process of an emergency medical dispatch system

34. PeekaRuttsalainen, 2004, A cross-platform model for secure Electronic Health Record communication.


38. Christopher Alban, Khan Seow 2007, Clinical documentation system for use by multiple caregivers.


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. Avula Tejaswi, NelaManoj Kumar, GudapatiRadhika, SeenivasVelagapudi 2012 a, Efficient Use of Cloud Computing in Medical Education.

44. J. Vidyahalakshmi, J. Prassanna 2012 b, Providing a trustable healthcare cloud using an enhanced accountability framework.


47. Abhishek Kumar, Gupta, Kulvinder Singh 2014 sharing of Medical Information on Cloud Platform.


53. B. Powmeya, Nikita Mary Ablett, V.Mohanapriya, S.Balamurugan, “An Oriented approach to Model the secure Health care Database systems,” In proceedings of International conference on computer , communication & signal processing(IC’SPin association with IETE students forum and the society of digital information and wireless communication,SDIWC 2011,pp.2-3


64. V.M.Prabhakaran, Prof.S.Balamurugan, S.Charanyak, “Privacy Preserving Personal Health Care Data in Cloud”, International Advanced Research Journal in Science, Engineering and Technology Vol 1, Issue 2, October 2014

DOI: 10.15680/IJIRSET.2015.0401077 www.ijirset.com

19009
APPENDIX

<table>
<thead>
<tr>
<th>S.no</th>
<th>YEAR</th>
<th>AUTHORS</th>
<th>TITLE</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1984</td>
<td>Sape MULLENDER and Andrew S TANENBAUM</td>
<td>PROTECTION AND RESOURCE CONTROL IN DISTRIBUTED OPERATING SYSTEMS</td>
</tr>
<tr>
<td>2</td>
<td>1985</td>
<td>Paul J. Levine</td>
<td>COMPUTER SECURITY SYSTEM FOR TIME SHARED COMPUTER ACCESSED OVER TELEPHONE LINES</td>
</tr>
<tr>
<td>3</td>
<td>1986</td>
<td>Norman Hardy</td>
<td>COMPUTER SYSTEM SECURITY</td>
</tr>
<tr>
<td>4</td>
<td>1987</td>
<td>Andreas Pfitzmann, Michael Waidner</td>
<td>NETWORKS WITHOUT USER OBSERVABILITY</td>
</tr>
<tr>
<td>5</td>
<td>1988</td>
<td>Chris J. Mitchell</td>
<td>KEY STORAGE IN SECURED NETWORK</td>
</tr>
<tr>
<td>6</td>
<td>1989</td>
<td>Fred C. Piper</td>
<td>VOICE NETWORK SECURITY SYSTEM</td>
</tr>
<tr>
<td>7</td>
<td>1990</td>
<td>Donald Graji, Mohnish Pabrai, Uday Pabrai</td>
<td>METHODOLOGY FOR NETWORK SECURITY DESIGN</td>
</tr>
<tr>
<td>8</td>
<td>1991</td>
<td>L. Todd Heberlein</td>
<td>NETWORK SECURITY MONITOR</td>
</tr>
<tr>
<td>9</td>
<td>1992</td>
<td>John R. Corbin</td>
<td>APPARATUS AND METHOD FOR LICENSING SOFTWARE ON A NETWORK OF COMPUTERS</td>
</tr>
<tr>
<td>10</td>
<td>1993</td>
<td>Michael P.</td>
<td>COMPUTER NETWORK ABUSE</td>
</tr>
<tr>
<td>11</td>
<td>1994</td>
<td>Bruce E. McNair</td>
<td>SYSTEM AND METHOD FOR GRANTING ACCESS TO A RESOURCE</td>
</tr>
<tr>
<td>12</td>
<td>1995</td>
<td>Scott D. Hammersley, Arthur D. Smet, Peter M. Wottreng</td>
<td>METHOD AND APPARATUS FOR INTRAPROCESS LOCKING OF A SHARED RESOURCE IN A COMPUTER SYSTEM</td>
</tr>
<tr>
<td>13</td>
<td>1995</td>
<td>Daniel B. Clifton</td>
<td>RESOURCE ACCESS SECURITY SYSTEM FOR CONTROLLING ACCESS TO RESOURCES OF DATA PROCESSING SYSTEM</td>
</tr>
</tbody>
</table>
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 Finn and Anupam Joshi  MOVING FROM SECURITY TO DISTRIBUTED TRUST IN UBQUITOUS 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 Krusl, 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 ISSUES 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. AlZain1  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
BIOGRAPHY

R.S.Venkatesh and P.K.Reejesh are currently pursuing their B.Tech. degree in Information Technology at KalaigairKarunanidhi 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, Kalaigair 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 in 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: 978-3-639-66958-3, 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 10th and 12th grade. She was working as Software...