Survey on Security on Cloud Computing by Trusted Computer Strategy

K.Deepika[1], N.Naveen Prasad[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 2009 to 2010. 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 networr 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. THE EUCALYPTUS OPEN SOURCE CLOUD COMPUTING SYSTEM[2009]

Daniel nurmi, Rich wolski, Chris grzegorczyk, Graziano obertelli, sunil soman, lamia youseff, Dmitrii zagorodnov Generally ,cloud computing systems fundamentally provide access to large pool of data and computational resources through a variety of interfaces.Those interfaces are similar to existing grid and HPC resources management and programming systems. Today,the most cloud computing systems are perfectly rely upon infrastructure. That infrastructure is invisible to the research community.In this paper,the authors presented the EUCALYPTUS which is an open source software framework for cloud computing. This open source software framework implements infrastructure as a service(IaaS). The architecture of the EUCALYPTUS system is simple,flexible and modular with a hierarchical design reflecting common resource environments found in many academic settings. The authors described the four high level components,each with its own web service interface,that comprise a EUCALYPTUS installation . It

includes node controller, cluster controller, storage controller and cloud controller. Node controller executes on every node that is designated for hosting VM instances. Each and every node controller makes queries to discover the node's physical resources like the number of cores,the size of the memory,the available disk space and also to learn about the state of virtual machine instances on the node. And next the author says that clster node generally executes on a cluster front end machine, or any machine that has network connectivity to both the nodes running NC's and to the machine running the cloud controller. Many of the cloud controller operations are similar to the NC's operations but are generally plural instead of singular(eg: run instances,terminate instances). Basically the cloud controller calculates how many simultaneous instances of the specific "type" can execute on its collection of NC's and reports that number back to the CLC. VM instance interconnectivity is one of the most interesting challenges in the design of cloud computing infrastructure. While designing EUCALYPTUS, the authors recognized that the VM instance network solution must address connectivity isolation ad performance. This EUCALYPTUS design attempts to maintain inter-VM network performance as close to native as possible.

Within EUCALYPTUS, the CC currently handles the three modes . the first configuration instructs the system to attach the VM's interface directly to a software ethernet bridge connected to a real physical machines network. The second configuration allows an admin to define static media access control(MAC) and IP address tuples. In this mode each new instance created by the system is assigned a free MAC/IP tuple, which is released when the instance is terminated. In these modes, the performance of inter-VM communication is near native, when VM's are running on the same cluster but there is not inter –VM network isolation. Finally ,this work aims to illustrate the fact that the EUCALYPTUS system has filled on important niche in the cloud computing design space by providing a system that is easy to deploy a top existing resources, that lands itself to experimentation by being modular and open source, and that provides powerful feature out of the box through an interface compatible. The authors provided that they successfully deployed the complete system on resources ranging from a single laptop to small linux clusters. In addition, they had made a installation available to all who wish to tryout the system without installing any software. Hereby, they concluded that their experiences so far has been extremely positive, leading us to the conclusion that EUCALYPTUS is helping to provide the research community with a much needed, open source software framework around which a user base of cloud computing researchers can be developed.

III. THE SECURITY OF CLOUD COMPUTING SYSTEM ENABLED BY TRUSTED COMPUTING TECHNOLOGY (2010)

Generally,the basic networks need security to transmit information authentecately. Cloud computing provides people the way to share distributed resources and services that belong to different organizations or sites.Since distributed systems and network computing were used wildly, security has become an urgent problem and will be more important in the future. In order to improve the work efficiency, the different services are distributed in different servers that are distributed in different places.Users from multiple environment hope use the distributed computing more efficient, just like using the electric power. Then, cloud computing has become a new information for this demand.Cloud computing provides a facility that enable large-scale controlled sharing and interoperation among resources that are dispersedly owned and managed. The authors noted that the security is therefore a major element in any cloud computing infrastructure, because it is necessary to ensure that only authorized access is permitted and secure behavior is accepted.Because the cloud computing is composed of different local systems and includes the members from multiple environments, therefore the security in cloud is complicate. In one side, the security mechanism should provide guarantees secure enough to the user, on the other side, the security mechanism should not be too complex to put the users into an inconvenient situation.The authors proposed a new way that is conducive to improve the secure and dependable computing in cloud. In their design, the authors integrated the Trusted Computing Platform (TCP), which is based on Trusted Platform Module (TPM), into the cloud computing system. The TCP will be used in authentication, confidentiality and integrity in cloud computing environment.The TCP can improve the cloud computing security and will not bring much complexity to users. Because the TCP is based on relatively independent hardware modules, it does not cost too much resource of CPU, and can improve the performance of processing cryptographic computation. The authors also designed a software middleware, the Trusted Platform Support Service (TSS), on which the cloud computing application can use easily the security function of TPM.The authors then discussed about the security model of the cloud computing. In order to achieve security in cloud computing system, some technologies have been used to build the security mechanism for cloud computing. The cloud computing security can be provided as security services. Security messages and secured messages can be transported, understood, and manipulated by standard Web services tools and software. The authors noted that this mechanism is a good choice

because the web service technology has been well established in the network-computing environment.The CLOUD includes distributed users and resource

from distributed local systems or organizes, which have different security policies. According to this reason, how to build a suitable relationship among them is a challenge. In fact, the requirements for the security in cloud computing environment have some aspects, including confidentiality. multiple security policy, dynamic of the services., the trust among the entities, dynamically building trust domains.The authors proposed the mechanism of trusted computing platform and other related functions that aid to achieve the trusted cloud computing, which has a trusted computing environment.The word trust is defined as "A trusted component, operation, or process is one whose behavior is predictable under almost any operating condition and which is highly resistant to subversion by application software, viruses, and a given level of physical interference." Then the authors concentrated on the trusted computing platform.TCP operates through a combination of software and hardware: manufacturers add some new hardware to each computer to support TC functions, and then a special TC(trusted computing) operating system mediates betweenthe hardware and any TC-enabled applications. TCP provides two basic services, authenticated boot and encryption, which are designed to work together. An authenticated boot service monitors what operating system software is booted on the computer and gives applications a sure way to tell which operating system is running. It does this by adding hardware that keeps a kind of audit log of the boot process.The authors keynoted that the build trusted cloud computing system using TCP.The trusted computing mechanism can provide a way that can help to establish a security environment. The model of trusted computing is originally designed to provide the privacy and trust in the personal platform and the trusted computing platform is the base of the trusted computing. Since the internet computing or network computing has been the main computing from the end of the last century, the model of trusted computing is being developed to the network computing, especially the distributed systems environment. The cloud computing is a promising distributed system model and will act as an important role in the e-business or research environments.The authors specified the Authentication cloud computing environment in TCP.In cloud computing environment, different entities can appeal to join the CLOUD. Then the first step is to prove their identities to the cloud computing system administration. Because cloud computing should involve a large amount of entities, such as users and resources from different sources, the authentication is important and complicated. Considering these, we use the TCP to aid to process the authentication in cloud computing. Then the authors were dealt about the Role based access control model in cloud computing environment. In order to reach the goal of trusted computing, the users should come from the trusted computing platform, and take the security mechanism on this platform to achieve the privacy and security for themselves. The user has his personal ID and secret key, such as the USB Key, to get the right to use the TCP. They can use the decryption function to protect their data and other information.

The authors described that by using the remote attest function, the user in the TCP could to notify their identities and relevant information to the remote machine that they want to make access to. The authors concluded that they have analyzed the trusted computing in the cloud computing environment and the function of trusted computing platform in cloud computing. The advantages of their proposed approach are to extend the trusted computing technology into the cloud computing environment to achieve the trusted computing requirements for the cloud computing and then fulfill the trusted cloud computing. TCP is used as the hardware base for the cloud computing system. In their design, TCP provides cloud computing system some important security functions, such authentication, communication security and data protection. Related methods for these implementations are also proposed by the authors in this paper.

IV. CONCLUSION AND FUTURE WORK

Various methods developed for anonymizing data from 2009 to 2010 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. Ian Foster, YongZhao, Ioan Raicu, Shiyong Lu, "Cloud Computing and Grid Computing 360-Degree compared", [2008a]
40. Rajkumar Buyya, Chee Shin Yeo, Srikumar Venugopal, "Market-oriented cloud computing: vision, type and reality for delivering IT services as computing utilities" [2008(b)]
41. Ronald Perez, Leendert Van Doom, Reiner Sailer, " Virtualization and hardware based security" [2008(c)].

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 1, January 2015

42. Daniel nurmi, Rich wolski, Chris grzegorczyk, Graziano obertelli, sunil soman, lamia youseff, Dmitrii zagorodnov," The Eucalyptus Open source cloud computing system"[2009]
43. Zhidong Shen, Qiang Tong ," The Security of Cloud Computing System enabled by Trusted Computing Technology" [2010]
44. Farhan Bashir Shaikh, Sajjad Haider," Security Threats in Cloud Computing" (2011)
45. Sanjana Sharma, Sonika Soni, Swati Sengar ," Security in Cloud Computing"(2012)
46. 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
47. 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
48. 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.
49. 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.
50. 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.
51. 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.
52. 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.
53. 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.
54. 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.
55. 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
56. 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
57. 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
58. 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.
59. 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.
60. 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
61. 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.
62. 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.
63. 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.
64. S.Balamurugan, S.Charanyaa, "Principles of Social Network Data Security" LAP Verlag, Germany, ISBN: 978-3-659-61207-7, 2014
65. S.Balamurugan, S.Charanyaa, "Principles of Scheduling in Cloud Computing" Scholars' Press, Germany,, ISBN: 978-3-639-66950-3, 2014
66. S.Balamurugan, S.Charanyaa, "Principles of Database Security" Scholars' Press, Germany, ISBN: 978-3-639-76030-9, 2014

BIOGRAPHY

K.Deepika and N.Naveen Prasad are currently pursuing their B.Tech. degree in Information Technology at KalaignarKarunanidhi Institute of Technology, Coimbatore, Tamil Nadu, India. Their areas of research interests include Network Security, Cloud Computing and Database Security.

Prof.S.Balamurugan obtained his B.Tech degree in Information Technology from P.S.G. College of Technology, Coimbatore, Tamil Nadu, India and M.Tech degree in Information Technology from Anna University, Tamil Nadu, India respectively. He is currently working towards his PhD degree in Information Technology at P.S.G. College of Technology, Tamil Nadu, India. At present he holds to his credit **65 papers International Journals and IEEE/ Elsevier International Conferences.** He is currently working as Assistant Professor in the Department of Information Technology, Kalaignar Karunanidhi Institute of Technology, Coimbatore, Tamil Nadu, India affiliated to Anna University TamilNadu, India. He is **State Rank holder** in schooling. He was **University First Rank holder** M.Tech. Semester Examinations at Anna University, Tamilnadu, India. He served as a Joint Secretary of IT Association, Department of Information Technology, PSG College of Technology, Coimbatore, Tamilnadu, India. He is the **recipient of gold medal and certificate of merit** for best journal publication by his host institution **consecutively for 3 years**. Some of his professional activities include invited Session Chair Person for two Conferences. He has guided 16 B.Tech projects and 2 M.Tech. projects. He has won a best paper award in

International Conference. His areas of research interest accumulate in the areas of Data Privacy, Database Security, Object Modeling Techniques, and Cloud Computing. He is a life member of ISTE,CSI. **He has authored a chapter in an International Book "Information Processing" published by I.K. International Publishing House Pvt. Ltd, New Delhi, India, 978-81-906942-4-7. He is the author of 3 books titled "Principles of Social Network Data Security", ISBN: 978-3-659-61207-7, "Principles of Scheduling in Cloud Computing" ISBN: 978-3-639-66950-3, and "Principles of Database Security", ISBN: 978-3-639-76030-9.**

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