International Journal of Grid and Distributed Computing
Vol. 10, No. 11 (2017), pp.1-10
http://dx.doi.org/10.14257/ijgdc.2017.10.11.01

A Survey on Privacy, Privacy Manager, Privacy laws and Regulations in Hybrid Cloud Network

Debabrata Sarddar[1], Sanjit Barman[2], Priyajit Sen[3] and Rajat Pandit[4]

[1]*Assistant Professor, Department of Computer Science and Engineering, University of Kalyani, Kalyani, Nadia, West Bengal, India*
[2 3] *Student (Ph.D pursuing), Department of Computer Science and Engineering, University of Kalyani, Kalyani, Nadia, West Bengal, India*
[4]*Assistant Professor, Department of Computer Science, West Bengal State University, West Bengal, India*
dsarddar1@gmail.com, go.sanjitbarman@gmail.com and priyajit91@gmail.com

Abstract

Cloud computing is the most recent technology in which information can be created, stored, manipulated and accessed wherever needed. Now, as the number of users is increasing day by day, the privacy of the overall network may lose if the private information of a person or any organisation is stolen or hacked by any other person. For that, we have made a survey over the privacy of the information stored in the cloud network. We have also discussed about the information for which privacy management is required. Privacy laws are also discussed in this paper. To protect information from cyber-crime or any other potential threats we have proposed about the need of privacy manager in the cloud network. Thus privacy of the network can be managed as well as security and trustworthiness can also be maintained.

Keywords*: Cloud Computing, Privacy Manager, Privacy laws, Privacy Infomediary and Regulations*

1. Introduction

The concept of cloud computing all users are known. At first the "cloud" :a networked collection of servers, storage system and devices to combined software, data, application, other information and computing power scattered into multiple locations across the network[1].The concept of cloud computing can be trace back to the mainframe days in 1960s when the knowledge of "utility computing" was introduced by MIT Computer scientist and Turing award winner John McCarthy who have said that "Computation may someday be formed as public utility"[2].The delimitation of Cloud computing defines as "the cloud is a parallel and distributed computing system consisting of inter-connected and potential computers that are dynamically outfit and presented as one or more unified computing resources depends upon service level agreements(SLA) build through negotiation between the service provider and buyers"[2][6].Cloud offers them so much limitless flexibility, better reliability, enhance collaboration, portability, simpler device[3].

The cloud computing model NIST defined three service models and four deployment models. The three service models called SPI model are: Cloud Software as a Services (SaaS), Cloud Platform as a Services (PaaS), and Cloud Infrastructure as a Services (IaaS). The four deployment models are: Private cloud, Public cloud, Community cloud and Hybrid cloud [2][3][6].

Received (May 30, 2017), Review Result (August 7, 2017), Accepted (August 27, 2017)

ISSN: 2005-4262 IJGDC

In initial the concept of building cloud computing are growing more and more mature, don't need to run, install or store there application or data on their personal computer. The users and many organisation, especially Small and Medium Business(SMB) enterprises takes benefit by putting their application and data on cloud .Nowadaysthey may lead to gains efficiency and effectiveness to developing cloud, deployment and also save the cost of purchasing and maintaining the infrastructure[6].To days large number of data stored in the cloud and maintaining the protection of data and taking privacy requirement using legislation in the cloud computing is a big challenge, privacy concerns will continue grow to transfer the data in cloud because lot of personal data are share related to individual and/or companies in the cloud[1].

Cloud computing demands are increase day by day, it represents new business model which enable on provisioning of computational and storage demand. Economic benefit is the man drive for cloud computing due to the fact that cloud computing offers an efficient way to reduce capital expenditure(CapEx) and operational expenditure(OpEx)[7]. Cloud computing offer immediate access the large number of data and the world most sophisticated super computers and their kin processing power, interconnected to the various location around the world and proffering speed in the tens of trillions of computations per second[3].Most of the user are used cloud which is provided by third party in a low cost, so, they don't give the efficient security and privacy. The major issue is privacy, it stems that the fact with cloud computing, data and program are stored off-premises and managed by a service provider. When third party gets hold of your data, who knows what's going on. So the key issue are identity, security and privacy is paramount concern.

Although cloud computing has many advantages but from customer's perspective, cloud computing security and privacy remain a major barrier for the adoption of the cloud computing. According to a survey carried out by Garter in 2009, more than 70% IT managers and CTOs the primary challenge of cloud computing services is that data security and privacy concerns. In March 2009, security vulnerability in Google Docs even led to serious outflow of security of the user's private information. Google Gmail also appeared global failure up to 4 hours [6]. A Salesforse.com employee fell victim to a spoofing attack and leaked a customer list, which generated further targeted spoofing attacks in October 2007. Epic.com lodged a formal complain to the FTC against Google for its privacy in March, 2009 and Epic was successfulof an action against Microsoft Passport [4],[6].

Although we can only enjoy the full benefit of cloud computing if we can give very real privacy and security that come along with storing tricky personal information in database and cloud scattered around the internet. Privacy need both companies and governmental organization, the cloud service provider give the certification and audit for these assurances [1]. It is key challenge to software engineer to reduce the privacy risk. In this paper we investigate data privacy protection issue to taken the information secure in the cloud.

2. Importance of Privacy in Cloud Computing Services

In this section we examine the notion of cloud privacy, types of information need to be protect in cloud computing.

2.1. Cloud Privacy

Privacy is the aspect of Information Technology that ability an organization or individual has to determine what information can be shared with third party. Privacy is a fundamental right, there are various forms of privacy, including 'right to be left along' and 'control of information about ourselves'. The cloud have typically process and store information about which privacy is one of the critical concern of cloud computing due to

the authenticity of the customers data and business logic reside among distributed cloud servers, which maintained by cloud provider. Therefore, there are potential risks that the confidential data (*e.g.*, financial data, business record, health records) or personal information (*e.g.*, personal profile) is disclosed to public or business competitors. The core attribute of privacy is that privacy preservability. A few securities attribute directly or indirectly influence privacy preservability, in addition to confidentiality, integrity, accountability, availability, *etc*. Privacy has been an issue of highest priority [1][5][7].

2.2. Types of Information or Data Need To Be Protected

Information stored in cloud typically resides in a shared environment collocated with data from other customers. Organizations transferring sensitive and organized data into the cloud, therefore, must account for the mean by which access to the data is controlled and the data is kept secure. 'Personal information' is a term that might be used in a slightly different aspect by different people, but in this document, we mean by this term of privacy sensitive information that include the following:

a) Personal identifiable information (PII): Information that could be identifiable or locate individual (*e.g.*, name, address) or information that can be interact with other information to identify an individual (*e.g.*, debit card number, credit card number, postal code *e.g.*,).

b) Sensitive information: information on religion, health, sexual orientation, union membership or other information that is considered private. Sensitive information includes personal financial information and job performance information, such information requires additional safety.

c) Unique device identities: information that might be uniquely traceable to a user device, *e.g.*, IP address, Radio frequency Identity(RFID) tags, unique hardware identities.

d) Information consideredbeing sensitive personally identifiable information, *e.g.*, biometric information (UIDAI) or collection of surveillance camera image in public places.

e) Usage data: usages collection of data from computer device such as printers; behavioural information, users recently visited website or usage history.

Also we protect the isolated data and sanitization of data. Privacy protection normally refers to the protection of rights of individuals, while the concept might also applied to groups of individuals, the individual aspectsof the issue is that which raises questions of privacy and liberty[1][5][9].

2.3. Privacy Challenges In Cloud Computing

The input data for cloud service is uploaded by the user in cloud which means that they typically result in user's information being present in unencrypted form on a machine that the user does not own or control, these poses some inherent privacy challenges.

The privacy challenge for designer is to design cloud services which minimized the privacy and security risk. If cloud provider can provide privacy preserving in cloud computing, there might be become more flexible and convenience in cloud computing, for example, an identity service that enable separately to easily manage their own online information and freely participate in online collaboration activities without repeated sign up. Users will not re-enter their personal data each time when they go to the new site. Instead, by using an identity service (two or more different ones), they will minimize the risk of identity theft and fraud. Privacy laws are restricted to collect, processing and transfer of personally identifiable and sensitive information limited uses of cloud service also designed. For example, a UK business company storing data from individual customers with the prominent cloud service provider Salesforce.com based on UK data protection law.The service provider responsible for housing, running and maintaining the

equipment, the client pays money as per use basis for example, Amazon Elastic Cloud Computing (EC2), Amazon S3, GoGrid.

It is also important to allay users fear about usage of information in cloud service. Confusion arises when, why their personal information is required or how it will be used or processed on to the other parties: this lack of control advances to suspicion and ultimately distrust [1][3][10][11][12].

3. Privacy Manager with in the Cloud

Privacy manager of cloud computing is reduces the risk of users private data being stolen or misused in the cloud computing and also assists the cloud provider to confirm the privacy law. Privacy manager, which helps the user manage the privacy of user's data in cloud, the privacy manager uses a feature called obfuscation, where this is possible. The idea is that data present unencrypted in cloud, the users private data is sent to the cloud in an encrypted form and processing is done on the encrypted data. The output of the processing is de-obfuscated by the privacy manager to revel the correct result. The obfuscation method uses a key which is chosen by the user and known by the privacy manager, but which is not communicated by the service provider. Thus the service provider is not able to de-obfuscate the user's data, and these data never present on the service provider's machine. This reduces the risks of theft and unauthorised users of this data. So, the obfuscate data is not personally identifiable information, and the service provider is not subject to the legal restriction that processing to the un-obfuscated data. However, it is practical some of the cloud application to work with obfuscated data.

3.1. Privacy Manager in the Client

It helps users to protect their privacy when accessing cloud services. In Figure 1 is that it can provide obfuscation and de-obfuscation service to diminish the amount of sensitive information held within the cloud. Privacy manager allows us to express privacy preferences about the treatment of their personal data, including type and degree of the obfuscation used. Personae correspond to set of privacy preferences used to simplify the process and being it more intuitive to the user.

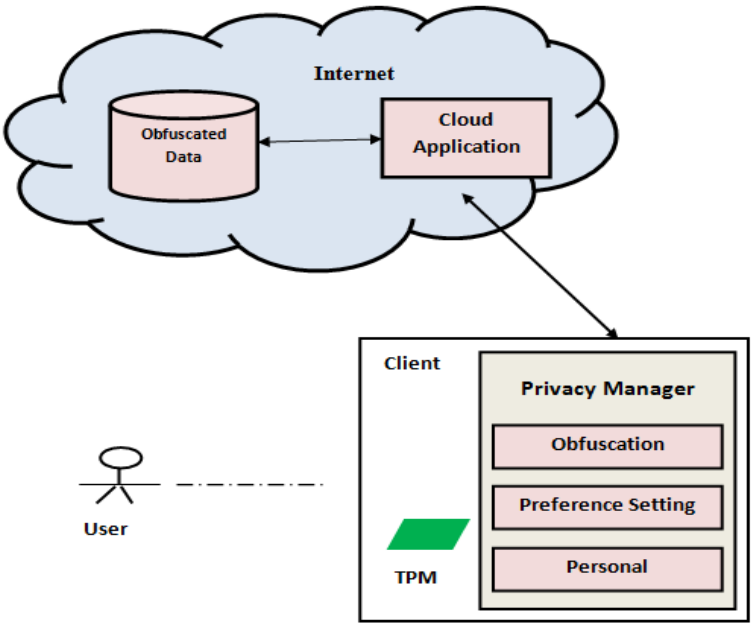

Figure1. Client based Privacy Manager

The Trusted Computing Group (TCG) address the lower level protection of data, is an organization that set up to design and develop the specification for computing platform. TCG create the trust for software processes, based on a small amount of external hardware called a Trusted Platform Module (TPM). Trusted computing will provide the cryptographic functionality; hardware based protected storage of secret information, platform attestation and mechanisms for secure boot and integrity checking. Open source operating system (*e.g.*, Linux) can support the TCG facilities further. For details to enhanced privacy, how trusted computing used see [12]. TPM in client machine can be used to protect the obfuscation key, provide encryption service and also provide for client-based privacy management are hardware based cryptographic functionality, confidentiality and integrity to decreases the risk of unsecured access to secret information(see Figure1)[7][13].

3.2. Privacy Manager in a Hybrid Cloud

The privacy manager may be deployed in a private cloud or a local network, to protect the secret information relating to different parties. This would be suitable in enterprise environments, where local protection of information is restricted in an adequate manner and its main use would be to control personal data passing to a public cloud. The privacy manager can be virtualized within the internal cloud, such as TPM could be also virtualized with in the private cloud. Advantage of this approach the cloud can be partitioned within the private cloud, including the most efficient rule of functionality of the privacy manager. It can provide enterprise control over dissemination of sensitive information and local compliance. A most significant issue is scalability, means that privacy manager might slow down traffic, provide a bottleneck.

There are different options with respect to the enterprise-focused privacy manager within the cloud. For example is that trusted virtual machines [14] could be used in the privacy cloud to support the strong enforcementof integrity and security policy manages over a virtual entity that running on a virtual platform. It would be possible to describe within the privacy manager different personae corresponding to various groups of cloud services using different virtual environments on each end user device. In this way virtualization used to push control from the cloud back to the client platform, including integrity checking.

3.3. Privacy Infomediary within the Cloud

Figure 2 shows a privacy infomediary within the cloud, how the privacy manager scattered and mediating data transfer between different trust domains, the privacy manager act on behalf of the user and allowed the degree of the data transfer based on user policy and service context and also the trustworthiness assessment of the service provisioning platform. In order to increase the transparency and accountability, notification and feedback by the privacy manager to the user also be preferable here.

Consumer organization or other entity are infomediary that trusted by the users. The infomediary might be an entity alternatively that already exists in within the cloud in order to provide an alternative function, such as an identity provider or auditor and functionality could be an extension of that. For example a open source Otemba[15] that implement user and key management and separating security keys from the cloud infrastructure. The key management role might be extended to a general infomediary role in the cloud.

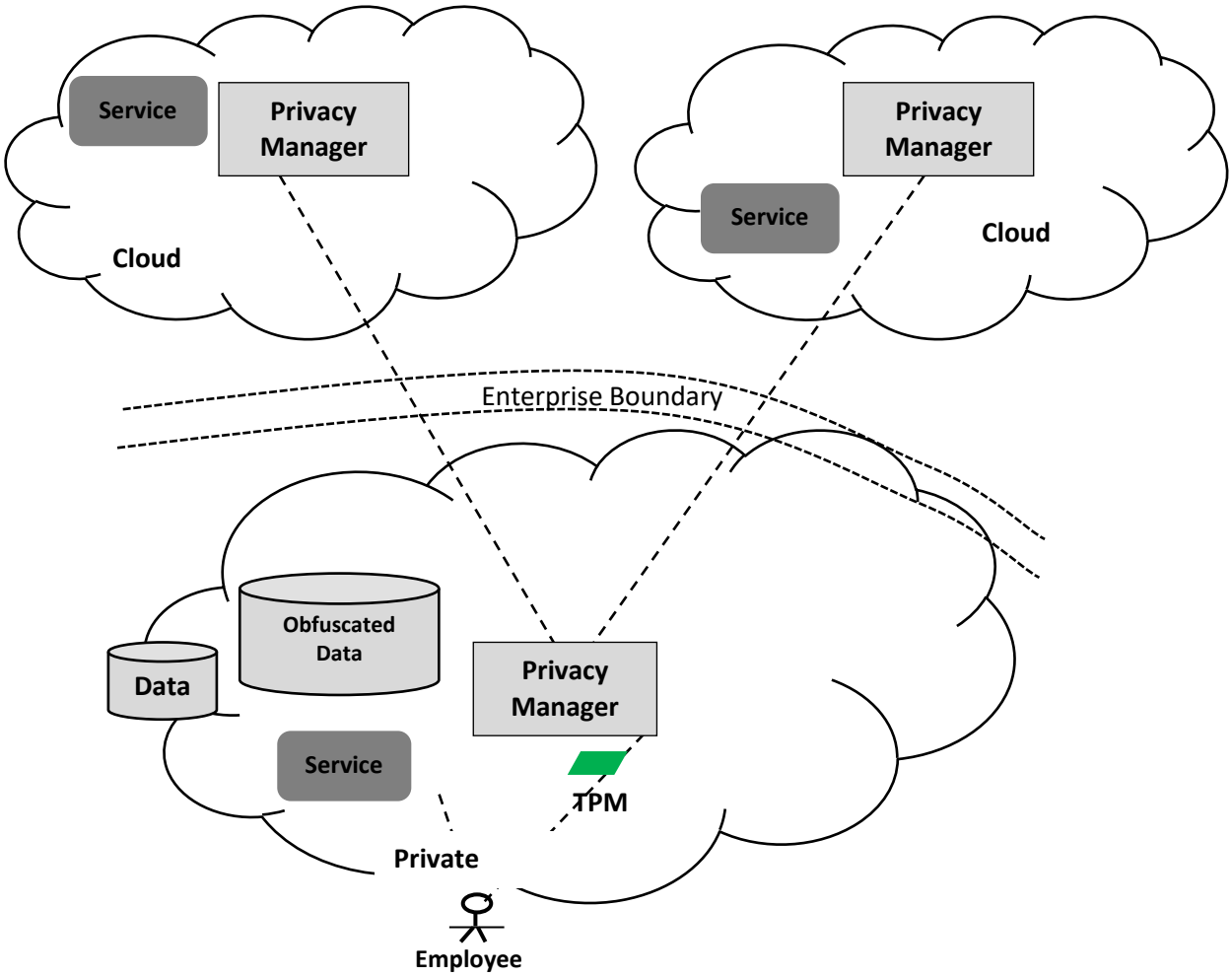

Figure 2. Privacy Manager within Cloud

The infomediary might be played a role in checking the user choices are fulfilled before providing a decryption key for decrypting any information that needs to be decrypted in order for the cloud service to be provided [16] and trust infrastructure could be useful to ensure the infrastructural building blocks for the cloud being trustworthy, secure and compliant with security best practice [7][17].

4. Privacy Issues, Data Security Law and Regulations

The following table summarizes some of the cloud computing privacy concern issues, data security issues, laws, regulations and standards.

Sl.no	Cloud computing privacy and security concerns	Issues	Related Laws, Regulation and Standards	Remarks
1	Compelled disclosure to the government	Subject to different levels of protection that the information contain by the cloud	**In India** • IT Act 2000 • RTI Act 2005[19] **In UK** • The regulation of investigatory Power Act **In USA** • Electronic Communications Privacy Act(ECPA) of 1986[4] • Stored Communication Act(SCA) • USA Patriot Act(UPA)	In UK, India, Malaysia the national cryptographic policies might allowed to cryptographic key based on the OECD guidelines.[20]
2	Fail to protect data to be disclosed to private parties	How a customer data to be protect by the cloud service provider When storing information on the cloud how can customer ensure the security compliance and is there any notification required when cloud security is breached?	**In India** • No specific laws but It Act 2005 and 2008, cyber law can be helpful. **In UK** • Data Protection Act 1998 • The Privacy and Electronic Communications Regulations 2011 **In USA** • Health Insurance Portability and Accountability Act(HIPAA) • Section 5 of the FTC Act • State Law and Regulations • Family Educational Rights and Privacy Act(GLBA) • Gramm Leach Bliley Act(GLBA)	In India the real problem is that India does not have any dedicated private organizations data protection law. In UK data protection law exists. In USA Cyber security enhancement and consumer data protection Act of 2006 pending[21]
3	Data Transfer, Accessibility and Retention	Cloud owner can the data be destructed or returned to customers Can consumers and companies have access the data on cloud	**In India** • Right to Information Act 2005 • IT Rule 2011(Reasonable Security Practices and Procedures and Sensitive Personal data or Information **In UK** • The Safe Harbor Agreement(for data transfer between US and Europe) **In USA** • Freedom Information	In India, no specific law are presented. It Rule 2011 is directly taken from European Union's In USA, where and how information is stored, secured that do not match their actual practices [18].

			Act(FOIA) • Payment Card Industry Data Security Standard(PCIDSS) • FTC Fair Information Practice	
4	Storing Location of Data	Jurisdiction Issue, physical location of the server storing the data may have legal implications	**In India** • IT Act 2008 and Personal Data Protection Act 2013 can be helpful **In UK** • EU Data Protection Directive(EC/95/46) **In USA** • NARA Regulations • Payment Card Industry Security Standard(PCIDDSS) • FTC Fair Information Practice	In India many data protection law are directly taken from European Union. In UK, many vendors' servers, traditional approach used EU Data Protection Directives depending upon the location of data, may not suitable a workable solution. In USA, Physically located documents governed by the law of state and the location of the company processing them or the laws of the state where a person resides?

Apart from the categorized listening cloud computing concerns given above, In India information Technology Act 2008 (cyber law included) and data protection Act 2013 may provide help full on data security and privacy. In case of UK, EU Directive will help to harmonize the privacy law that exist in different states in European Union and provide basic standard on privacy protection. In case of USA, various other law and regulations are NARA regulations (data location), Freedom of Information Act (electronic discovery) *etc.* are provide complete guideline on security and privacy in public cloud computing [22]. Illustrate above some act are fail to protect the information to be disclosed to government and private parties, they were used to protect privacy and fail to the new cloud computing service environment, changes to these acts should be made to adapt new Cloud Computing Environment[4][18].

5. Further Research

Research in the field of privacy legislation and cloud computing would benefit substantially if further researcher could have do more case studies with reference to challenges, laws and regulations depicting various scenarios.

6. Conclusion

In This paper, we analyse the privacy of cloud computing, in order to handle the privacy we have discussed what type of information need to be protected, some privacy challenges and we have also described a privacy manager. We have also explored some privacy issues, security laws and regulations. The impact of privacy regulations is most dramatic between traditional IT and external cloud computing. The main idea of cloud computing can bring many uncertainty with respect to compliance with privacy laws and regulations. So, current privacy regulations are not enough to solve all the privacy issue

related to the cloud computing. Not many organisations are completely aware of privacy issues in cloud computing.

References

[1] S. Pearson, "Taking account of privacy when designing cloud computing services", HP labs, ICSE'09 workshop, **(2009)**.
[2] P.K. Pattnaik, M.R. Kabat and S. Pal, "Fundamentals of cloud computing", First Edition, India 2015, ISBN: 9789325976108, pp. 1-4,17-29,82-83.
[3] J. Wang, Y. Zhao, S. Jiang and J. Le, "Providing privacy preserving in cloud computing", IEEE, **(2010)**.
[4] M. Zhou, R. Zhang, W. Xie, W. Qian and A. Zhou, "Security nd privacy in cloud computing: a survey", Sixth International conference on semantic, Knowledge and Grids, **(2010)**.
[5] H. Katzan, International Journal of Management and Information systems, vol. 14, no. 2, **(2010)**, pp. 1-12
[6] D. Chen and H. Zhao, "Data security and privacy protection issues in cloud computing", IEEE, **(2012)**.
[7] S. Pearson, Y. Shen and M. Mowbray, "A privacy manager for cloud computing" HP labs, UK.
[8] Z. Xizo and Y. Xizo, "security and privacy in cloud computing", Second Quarter, IEEE communications surveys and tutorials, vol.15, no. 2, **(2013)**.
[9] W. A. Jansen, NIST, "cloud hooks: security and privacy issues in cloud computing", Proceeding of the Hawaii International Conference on system sciences, **(2011)**.
[10] J. Salmon, "Clouded in uncertainty-the legal pitfalls of cloud computing", **(2008)**.
[11] S. Pearson, "Trusted computing: strengths, weaknesses and further opportunities for enhancing privacy", Springer, Heidelberg, vol. 3477, **(2005)**, pp. 305-315.
[12] "Trusted computing group: Trusted Platform Module (TPM) Specification 2014", https://www.trustedcomputinggroup.org/specs/TPM/.
[13] "Otemba project: The reasons for Otemba's existence", http://sourceforge.net/apps/trac/otemba/wiki/Reasons%20for%20existence.
[14] M.C. Mont, S. Pearson and P. Bramhall, "Towards Accountable Management of Identity and Privacy: Sticky Policies and Enforceable Tracing Services", IEEE Workshop on Data and Expert Systems Applications, IEEE Computer Society Press, Washington **(2003)**, pp. 377–382.
[15] A. T. AlSudiari and T.G.K. Vasista, "Cloud computing and privacy regulations:an exploratory study on issues and implementations", Advanced computing: An International Journal(ACIJ), vol. 3, no. 2, **(2012)**.
[16] "GoI, Guide on Right To information Act", 2005,http://rti.gov.in/RTICorner/Guideonrti.pdf.
[17] Singh and Dalal, "In Absence of Dedicated Privacy Law & Data Protection Law - Is India Ready for Cloud Computing?", 2010 http://www.techno-pulse.com/2010/12/privacy-data-protectionlaw-india-cloud.html.
[18] Jensen and Grance, "Guideline on security and privacy in public cloud computing", NIST, US, 2012.http://www.nist.gov/customcf/get_pdf.cfm?pub_id=909494.

Authors

Debabrata Sarddar, he is a Assistant Professor in the Department of Computer Science and Engineering, University of Kalyani, Kalyani, Nadia, West Bengal, INDIA. He has done Ph.D. at Jadavpur University. He completed his M. Tech in Computer Science & Engineering from DAVV, Indore in 2006, and his B.E in Computer Science & Engineering from NIT, Durgapur in 2001. He has published around 200 research papers in different journals and conferences. His research interest includes wireless and mobile system, Cloud Computing and WSN.

Sanjit Barman, he has done M. Tech in Computer Science and Engineering at the Department of Computer Science and Engineering, University of Kalyani, Kalyani, Nadia, West Bengal, India in 2017. He has completed his B.E.in Information Technology from University Institute of Technology, The University of Burdwan, Burdwan, and West Bengal, India in 2015.

His research interest includes Cloud Computing, Mobile and Wireless Computing, Data Structure and Algorithm

Priyajit Sen, he has done M. Tech in Computer Science and Engineering at the Department of Computer Science and Engineering, University of Kalyani, Kalyani, Nadia, West Bengal, India in 2017. He has completed his MCA from Department of Computer Science and Engineering, University of Kalyani, Kalyani, Nadia, West Bengal, India in 2015. His research interest includes Mobile Computing, Wireless Sensor Network and Cloud Computing.

Rajat Pandit, he is an assistant professor in the Department of Computer Science, West Bengal State University, Barasat, and West Bengal, India. He has completed his M.Tech (IT) from West Bengal University of Technology, West Bengal, India in 2009. He has completed his MCA from University of Jadavpur University, Jadavpur, and West Bengal, India in 2001. His research interest includes Mobile Computing, Wireless Sensor Network and Cloud Computing.

