PRIVACY IN CLOUD COMPUTING: A SURVEY

Dr. Arockiam L[1], Parthasarathy G[2] and Monikandan S[3]

[1]Associate Professor,St.Joseph's College,Trichy, Tamilnadu, India
larockiam@yahoo.co.in
[2]Assistant Professor, TRP Engineering College,Trichy,Tamilnadu, India
parthasarathee.g@gmail.com
[3]Research Scholar,ManonmaniamSundaranar University, Tirunelveli,India
moni.tamil@gmail.com

ABSTRACT

Various cloud computing models are used to increase the profit of an organization. Cloud provides a convenient environment and more advantages to business organizations to run their business. But, it has some issues related to the privacy of data. User's data are stored and maintained out of user's premises. The failure of data protection causes many issues like data theft which affects the individual organization. The cloud users may be satisfied, if their data are protected properly from unauthorized access. This paper presents a survey on different privacy issues involved in the cloud service. It also provides some suggestions to the cloud users to select their suitable cloud services by knowing their privacy policies.

KEYWORDS

Cloud computing,Security,Privacy

1. INTRODUCTION

Cloud computing is a model for enabling convenient, on demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction[1]**.** It reduces the capital expenditure and operational expenditure involved in the IT Infrastructure of an organization.

Cloud computing has some attributes that are shared, standard service, solution-packaged, self-service, elastic scaling and usage-based pricing. Cloud has three different service models. They are *(i) Software as a Service* (SaaS) which uses provider's application over a network. Instead of purchasing the software, cloud user rents the software for use on a pay per use model.*(ii)Platform as a Service*(PaaS):- It deploys user applications in cloud. The Cloud provider gives an environment to application developers, who develop applications and offer those services through the provider's platform.*(iii)Infrastructure as a Service*(IaaS):- It deals with rent processing, storage and network capacity. The basic idea is to offer the computing services like processing power, disk space etc., based on the usage.

The Cloud computing can be deployed in four different models namely,(i)Private Cloud-Enterprise owned or leased,(ii)Public Cloud- Sold to the public, mega scale infrastructure,(iii)Hybrid cloud- The combination of two or more cloud types,(iv)Community Cloud-shared infrastructure for specific community[3].

Cloud computing offers increased amount of storage and processing power to run users applications. It enables new ways to access information, processes and analyze data. It also connects people and resources from any location all over the world [4].Even though, the users

Natarajan Meghanathan, et al. (Eds): SIPM, FCST, ITCA, WSE, ACSIT, CS & IT 06, pp. 321–330, 2012.
 DOI : 10.5121/csit.2012.2331

have gained more advantages in cloud, there are certain limitations faced by the users when it is implemented. Data protection, operational integrity, vulnerability management, business continuity (BC), disaster recovery (DR) and identity management (IM) are top concerns of security issues for Cloud Computing. Among the above, Privacy is the most important key concern. Security and privacy of Cloud Computing system becomes a key factor for users to adapt it.

Moreover, many security and privacy incidents are also observed in today's Cloud Computing systems. The Below list provides a few of them [7]:

- Google Docs found a flaw that inadvertently shares user's docs in March 2009.
- A Salesforce.com employee fell victim to a phishing attack and leaked a customer list, which generated further targeted phishing attacks in October 2007.
- Epic.com lodged a formal complaint to the FTC against Google for its privacy practices in March 2009. EPIC was successful in an action against Microsoft Passport.
- Steven Warshak stops the government's repeated secret searches and seizures of his stored email using the federal Stored Communications Act (SCA) in July, 2007. However, the government argues that the Fourth Amendment doesn't protect emails at all when they are stored with an Internet Service Provider (ISP) or a webmail provider like Hotmail or Gmail.

This paper mainly focuses on the issues related to Privacy in cloud computing**.** Privacy is defined as a fundamental human right related to the collection, use, disclosure, storage and destruction of personal data (Personally Identifiable Information-PII). The American Institute of Certified Public Accountants (AICPA) and Canadian Institute of Charted Accountants (CICA) define that it is the right and obligation of individuals and organizations with respect to the collection, use, retention, and disclosure of personal information. Privacy is the protection of appropriate use of personal information of cloud user [9].

Privacy breaches may create many problems to cloud users. Cloud Users always expect high level protection for their sensitive data. Violation of protection leads to user's dissatisfaction. For example, consider that an organization maintains their sensitive data in the cloud unfortunately the data may be stolen. This will suffer the organizational growth and it may also leverage the competitor to come up.

The rest of the paper is organized as follows: Section II introduces the origin of privacy issues. The privacy issues and challenges are described in Section III. Section IV proposes the suggestions to preserve privacy to the cloud users and the cloud providers. The observations made in this survey are mentioned in Section V and finally Section VI concludes the survey.

2. ORGIN OF PRIVACY ISSUES

Data Privacy is about security of the Personally Identifiable Information (PII). Personal information should be managed as a part of the data used by the organization. According to the KPMG Data Life Cycle [13], there are different phases, where the user will face some privacy issues. KPMG stands for the group of people Klynveld,Peat,Marwick and Goerdeler, who formed the organization.

2.1. Phases in KPMG Data Life Cycle

The KPMG is a global organization which provides Audit, tax and Advisory Services. They are mostly involved with management of personal information of the customer. According to KPMG, data may have seven different phases in its life cycle.Figure 1.gives the various phases available in the KPMG data life cycle.

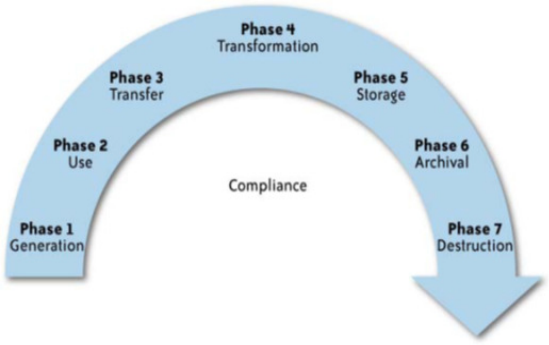

Figure1. KPMG Data Life Cycle [15]

2.1.1. Generation of the Information

In this phase, the organization should know about the owner of the PII i.e. who has created the PII and how the ownership is maintained in the organization are to be known.

2.1.2. Use

It is the usage of the personally identified information. The PII is used only by an organization or used by any third party vendor.

2.1.3. Transfer

When information is transferred to the cloud by an organization using public networks, there is a chance of data theft during the data transfer.

2.1.4. Transformation

While transferring information, each user should get the assurance for the integrity of PII. It is the process of checking, if any intruder involved during information transfer.

2.1.5. Storage

The appropriate access control mechanism is available to restrict the access of data. It restricts various users to access the storage.

2.1.6. Archival

The period of storage is to be mentioned. i.e., how long the data will be retained by the cloud provider.

2.1.7. Destruction

Cloud Provider destroys PII obtained from cloud users in a secure manner to avoid potential breach of the information.

3. PRIVACY ISSUES AND CHALLENGES

The Personally identifiable information (PII) has easily found in the cloud computing service because of the privacy issues [16]. Once the provider known that the PII like Name, Address and Credit card number, it will create many difficulties to the user. Privacy issues exist for a long time in computing literature, and many law acts have been published to protect users' individual privacy as well as business secret. Nevertheless, these acts are expired and inapplicable to new scenarios, where a new relationship between users and providers (i.e. three parties) raises [7].The Figure 2.gives the various privacy issues involved in the cloud computing.

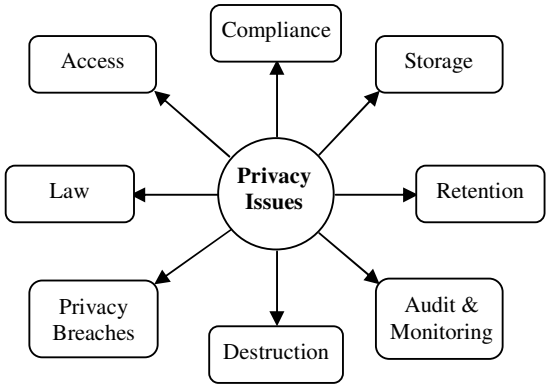

Figure 2. The Major Privacy Issues of Cloud computing.

The above said privacy issues are to be addressed in detail.

3.1. Access.

Cloud provider has the ability to access the individual's data in the cloud. Confirmation after deletion must be given to the user when there is a deletion request. Normally, the confirmation given by the providers will not satisfy the cloud users.

3.2. Compliance.

The list of applicable laws, regulations, standards and contractual commitments govern cloud data. There are many acts available to protect the data like Electronic communication Privacy Act (ECPA), USA Patriot Act (UPA) etc. Sometimes, to maintain the law and order in the country, cloud user's data may be needed by the government. In this situation, the above acts failed to maintain the privacy [7].

3.3. Storage.

It indicates the physical location of user's data in the cloud. There are many physical locations available throughout the world. Many organizations are not comfortable to store their data away from their organizations [19]. Storing data in different data centers in different locations, may lead to unauthorized access and uses. Proper assurance is not given by the cloud providers for the transparency of data.

3.4. Retention.

It indicates theduration of the data storage .The stored data must be deleted automatically after the completion of the specified duration. Otherwise, privacy issues will be raised.

3.5. Destruction.

This type of issue is involved with the deletion of data from the cloud. Providers do not have the rights to delete data, without getting permission from the cloud user.

3.6. Audit and Monitoring.

It is the way of watching the cloud providers by the cloud users. Since, cloud providers are not monitored properly, it leads to the improper use of user's data.

3.7. Privacy breaches.

If there is any mischievous act with the cloud user data, cloud user must be able to identify it[9].The absence of identifying the breach will cause a drawback in the business. Here, the real

time attack happened on the user data in the Google Service Provider. In Google, the IT Giant faced the hacker's attack in the January 2010 from China. So, they decided to close their large internet market in China, because the attacks were well organized and dangerous [20].

3.8. Law.

Technology is improving day by day. Whenever the technology changes, the issues related to the technology will alsochanged. But the law governing the issue is not updated regularly.All the policies stated by the cloud provider should be transparent. If it is not transparent, then the cloud user does not understand the policies clearly.

There are many challenges faced by the cloud provider as well as the cloud user before choosing their service provider. A detailed description of the challenges involved in this behavior is given below.

The Figure 3.depicts the top level designs of cloud provider policy usecases. Two different usecases are used in this system. They are:

- Payments
- Cloud Provider Privacy Policy(CP3)

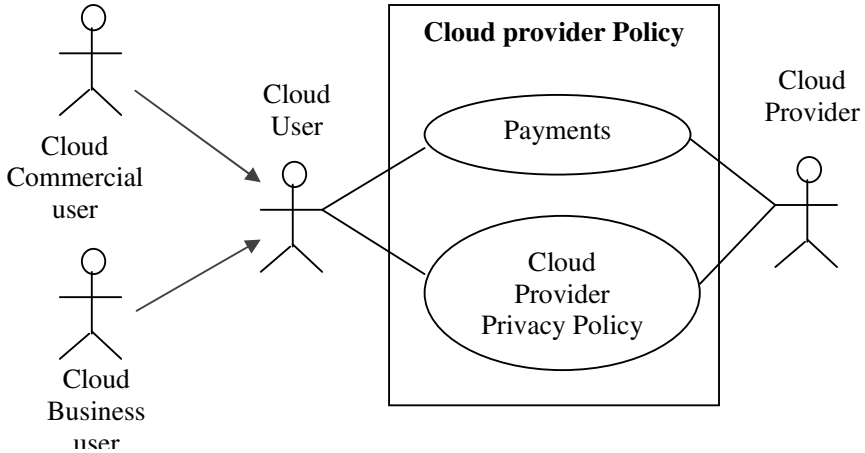

Figure 3.Usecases ofcloud

The actors are cloud users and cloud providers. The CP3 usecase provides detailed privacy policies of the cloud providers. Once users want to select a cloud provider, they should pay more attention on CP3use case.

The Figure 4. depicts CP3usecase in detail; it has six different privacy constraints in the cloud service.CP3usecaseis extended by several usecases that are Physical Location, Data Recovery, Access Right, Transborder flow, Audit trails and Laws. All these use cases are extending use cases because they are related to the data storage issues in the cloud. These usecases are providing optimum information about CP3.

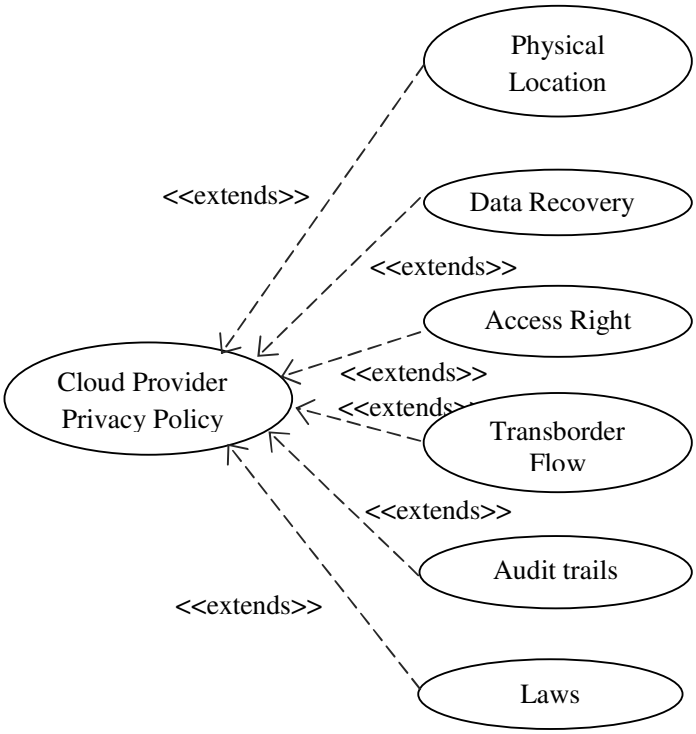

Figure 4.Usecase of cloud provider privacy policy(Low Level)

The following section gives the suggestions to meet the above mentioned challenges.

4. SUGGESTIONS TO PRIVACY ISSUES

4.1. For Cloud User

These suggestions are given to the cloud user when placing their data in the Cloud Provider.

The cloud usershould carefully read the privacy policy before placing their information in the cloud. If a cloud user doesn't understand any of the policies, it should be clarified with the provider or may consider other service providers.

Cloud user must have a close attention regarding rights to use, disclose, or make public cloud user information.

Suppose thecloud user wants to remove any data from the cloud, the cloud provider must take necessary steps to remove the data. The Cloud user has rights to check whether that data is still retained by the cloud provider.

Cloud users should notplace any important data which may be helpful for their competitors, government and others.

Cloud users mustalways have a consultation with their technical support group about the advisability of keeping their data in the cloud.

4.2. For Cloud Providers

The following suggestions are for the providers to maintain the cloud user's data in the Cloud.

- Cloud provider must ensure that they are not violating any law or policy.
- Cloud Provider should mention the physical location of the cloud user's data in the cloud.
- Cloud Provider should maintain the isolationbetween different user's data.
- Protection mechanism of cloud must be known to the user.
- Recovery plans are to be mentioned by the provider in case of natural disaster.
- Cloud Provider must list the various laws and regulations that govern the cloud user's data.
- Cloud users must be given advance notice to the changes of the privacy policies
- Periodically, the provider should conduct the audit trails and maintain log of user's data.

5. OBSERVATION

Many organizationsare willing to enter into the cloud computing to reduce the capital expenditure. To attract more number of users, various privacy issues should be addressed. The important privacy issues identified in this survey are listed in Table I.

Table 1. Privacy issues and related description

Item No.	Privacy Issue	Description
1.	Protection of Data	How the CP is describing to protect the data.
2.	Physical Location	The Place Where the cloud user data is stored mentioned by CP.
3.	Data Loss	If the cloud user data is lost, then what is the response of CP?
4.	Access Control	To avoid the unauthorized access
5.	Transborder Flow	The law differs from country to country

5.1. Protection of Data

Cloud providers are asked to describe about how they protect data. Cloud provider must portray regarding which encryption technique is being used for protecting data.

5.2. Physical Location

Cloud users have the rights to know about the place where their data is going to be stored. So, the cloud provider ought to give the exact regional data center of the cloud for the data storage.

5.3. Data Loss

Suppose, if a user's data are lost or mingled with other user's data. The Provider should take responsibility to correct the data loss with proper response to cloud user.

5.4. Access Control

Cloud provider will have to follow various accessing levels in the cloud by applying access control lists. There may be a different level of access to the cloud user's data. To avoid the unauthorized access, the provider will create access list. The Table 2 describes the privacy policies of different cloud providers.

Table 2.Privacy policy of cloud providers

Sl.No	Parameter	Rackspace	Windows Azure	Amazon Web Services
1.	Disclosure of PII	Inside the organization and the third party , those doing work on behalf of Rackspace	Inside the organization and occasionally contract with other companies to provide services on our behalf	Inside the organization and third party people working on our behalf.
2.	Physical Location	Eight data centers in three region viz., North America(5), Europe(2) and Asia(1)	Six data centers in three regions viz., U.S(2), Europe(2), Asia(2)	Six data centers in three regions viz., U.S(3), Europe(1), Asia(2)
3.	Data Loss	Recovery Possible through Unmetered Managed Backup Service	Recovery Possible	Recovery possible through Reduced Redundancy Storage
4.	Access Control	ACL Based Security Model	Rule Based Authorization	SSL encrypted endpoints using the HTTPS protocol
5.	Trans border Flow	Not Available	Not Available	Not Available

5.5.Transborder Flow

In addition to the above, the cyber law is not universal; it will vary among countries. Since clouds are located in different regions of the world, the provider should furnish the law when the data are crossing different borders.

6. CONCLUSION

CloudComputing is a set of network enabled services, providing scalable, QoS guaranteed, normally personalized, inexpensive computing infrastructures on demand, which could be accessed in a simple and pervasive way. Most of the IT organizations are preparing themselves to migrating to cloud computing. The following findings are suggested to the cloud users, when they are selecting the cloud providers. First, the cloud user should concentrate on how the data is protected from one another, where their data is located, how the access is limited. Second, Cloud userhas right to know the rules and laws followed by different countries when it comes Transborder flow. Cloud users should try to get the proper solution for the above said privacy issues from the cloud providers. This will help the cloud user to select a suitable cloud provider who cares their data and provides a high end data protection.

REFERENCES

[1] Mell, P., &Grance, T. (2009, 7 10). The NIST Definition of Cloud Computing, from NIST Information Technology Laboratory, http:// www.nist.gov/itl/cloud/upload/cloud-def-v15.pdf, retrieved on may 2011.

[2] J. Geelan, “Twenty one experts define cloud computing. Virtualization,” Electronic Magazine, http://virtualization.sys-con. com/node/612375 , viewed on July 2011.

[3] Ross A. Lumley, “Cyber Security and Privacy in Cloud Computing: Multidisciplinary Research Problems in Business”, the George Washington University, Report GW-CSPRI-2010-4, December 18, 2010, pp 1-10.

[4] Michael Miller, “Cloud Computing: Web-Based Applications That Change the Way You Work and Collaborate Online”, QueKnowledge and Grids,2010,ISBN-13: 978-0-7897-3803-5, pp105-

112.

[5] WassimItani, AymanKayssi and Ali Chehab, "Privacy as a Service: Privacy-Aware Data Storage and Processing in Cloud Computing Architectures", in Proc. of Eighth IEEE International Conference on Dependable, Autonomic and Secure Computing, 2009, pp 711-716.

[6] Siani Pearson, AzzedineBenameur,"Privacy, Security and Trust issues arising from cloud computing", in Proc. of 2nd IEEE International Conference on Cloud Computing Technology and Science, 2010, pp 693-702.

[7] Minqi Zhou et al., "Security and Privacy in Cloud Computing: A Survey", in Proc. of Sixth International Conference on Semantics, Publications, First Printing, Augutst 2008, pp149-150.

[8] ReijoM. Savola, ArtoJuhola, IlkkaUusitalo, "Towards Wider Cloud Service Applicability by Security, Privacy and Trust Measurements", in Proc. of 4th International Conference on Application of Information and Communication Technologies(AICT), 2010,pp1-6.

[9] Tim Mather, SubraKumaraswamy, SahedLatif ," Cloud Security And Privacy, an Enterprise Perspective on Risks and Compliance", O'Reilly Publications, First Edition, September 2009, ISBN: 978-0-596-80276-9, pp149-150.

[10] R.Savola, "Towards a risk driven methodology for privacy Metrics development", Symposium on Privacy and Security Applications (PSA'10), August 2010, pp 20-22.

[11] Wayne A. Jansen, NIST, "Cloud Hook: Security and Privacy Issues in Cloud Computing", in Proc. of 44th Conference on SystemSciences-2011,pp 1-10.

[12] Srijith K Nair, "Toward Secure Cloud Bursting Brokerage and Aggregation",Eighth IEEE European Conference on Web Services,2010,pp 189-196.

[13] http://mscerts.programming4.us/programming/cloudsecurityandprivacywhatisthedatalifecycle .aspx, retrieved on June 2010

[14] Ran Li et al., "Thinking the cloud computing in China",in Proc. of 2nd IEEE International Conference on InformationManagement and Engineering (ICIME),2010,pp669-672.

[15] Frank Gens, "Bringing Cloud into the Enterprise", Cloud Leader ship Forum. http://www.eiseverwhere.com/file_uploads/86cde4f4 bf015bb8cd2153ea7e0287ff_Day_1_815am_Frank_Gens_Bringing_Cloud_into_the_ Enterprise.pdf, retrieved on July 2011.

[16] Siani Pearson, "Taking Account of Privacy When Designing Cloud Computing Services", HP Laboratories, Tech. Rep. HPL- 2009-54, 2009, http://www.hpl.hp.com/techreports/2009/HPL-2009-54.pdf.retrieved on July 2011

[17] Rajarshri chakra borty et al., "The Information Assurance Practicesof Cloud Computing Vendors",IEEE Trans. Cyber Security,2010,pp 29-37.

[18] Miranda Mowbray,SianiPearson,YunShen, "Enhancing Privacy in Cloud Computing via Policy-based obfuscation", Journal of Supercomputing,Springer Science Business Media,LLC 2010.

[19] HassaanTakabi et al, "Security and Privacy Challenges in Cloud ComputingEnvironments", The IEEE Computer and Reliability Socieitis,November/December 2010,pp 24-31.

[20] RuiMaximoEsteves,ChunmingRong,"Social Impact of Privacy in Cloud Computig", in Proc. of 2nd IEEE International Conference on Cloud Computing Technology and Science,2010,pp 593-596,

[21] I-HsunChauang et al, "An Effective Privacy Protection Scheme for Cloud Computing", in Proc. of IEEE Conference ICACT,2011,pp 260-265.

[22] http://www.worldprivacyforum.org/cloudprivacy.html retrieved on August 2011.

[23] PelinAngin, Bharat Bhargava, RohitRanchal, NoopurSingh,MarkLinderman, "An Entity-centric Approach for Privacy and Identity Management in Cloud Computing", in Proc. of Practices of Cloud Computing Vendors", IEEE Trans,Cyber Security,2010,pp29-37.

[24] https://www.infosecisland.com/blogview/3539-Privacy-and-Cloud-Computing-Challenges.html retrieved on July 2011

[25] David Tancock, SianiPearson,AndrewCharlesworth,"Analysis of Privacy Impact Assessments within Major Jurisdictioons", in Proc. of Eigth IEEE Annual International Conference on privacy,security and trust,2010,pp119-125.

[26] Frank Doelitzscher,Charistoph Reich, Anthony Sulistio, "Designing Cloud Services Adhering to Government Privacy Laws",in Proc. of 10thIEEE International Conference on Computer and Information Technology (CIT 2010), pp 930-935.

[27] Shuai Zhang et al., "Cloud Computing Research and Development Trend", in Proc. of Second International Conference on Future Networks,2010,pp93-73.

[28] George Reese, "Cloud Application Architectures",O'ReillyMedia,April 2009, First Edition,ISBN: 978-0-596-15636-7, pp 80-84.

Authors

Arockiam L is working as Associate Professor in the Department of Computer Science, St.Joseph's College (Autonomous), Tiruchirappalli, Tamil Nadu, India. He has 23 years of experience in teaching and 16 years of experience in research. He has published 87 research articles in the International / National Conferences and Journals. His research interest includes Software metrics, Data Mining, Mobile Computing, Web Services and Cloud Computing.	
Parthasarathy G is working as Assistant Professor in the Department of Computer Science and Engineering, TRP Engineering College, Tiruchirappalli, Tamil Nadu, India. His research interests include Cloud Computing, Expert Systems and Web Services.	
Monikandan S is working as a Assistant Professor in Department of MCA in Christhuraj Institute of Computer Application, Tiruchirappalli, Tamilnadu. He is doing his Ph.D in ManonmaniamSundaranar University, Tirunelveli,india. His research interest includes Privacy in Cloud Environment and Web Technology.