A COMPREHENSIVE SURVEY ON SECURITY ISSUES IN CLOUD COMPUTING AND DATA PRIVACY LAW IN INDIA

Anupama Mishra[1], DhawalVyas [2]

Government Engineering College, Bharatpur

Abstract

Cloud computing is a new computing paradigm that brought a lot of advantages especially in ubiquitous services where everybody can access computer services through internet With cloud computing, there is no need of physical hardware or servers that will support the company's computer system, internet services and networks. Cloud computing technology is a new concept of providing dramatically scalable and virtualized resources, bandwidth, software and hardware on demand to consumers. Consumers can typically requests cloud services via a web browser or web service. Using cloud computing, consumers can safe cost of hardware deployment, software licenses and system maintenance. On the other hand, it also has a few security issues. This paper introduces cloud security problems. The data in cloud need to secure from all types of security attacks. Another core services provided by cloud computing is data storages.

Keywords— *Cloud Computing, Security and Countermeasures, Consumers, XML Signature Element Wrapping, Browser Security, Cyber Laws, policy, Data Privacy.*

---******---

1. INTRODUCTION

Cloud computing is receiving a great deal of attention, both in publications and among users, from individuals at home. Yet it is not always clearly defined. Cloud computing is a subscription-based service where you can obtain networked storage space and computer resources. One way to think of cloud computing is to consider your experience with email. Your email client, if it is Yahoo!, Gmail, Hotmail, and so on, takes care of housing all of the hardware and software necessary to support your personal email account. When you want to access your email you open your web browser, go to the email client, and log in. The most important part of the equation is having internet access. Your email is not housed on your physical computer.Cloud computing builds on established trends for driving the cost out of the delivery of services while increasing the speed and agility with which services are deployed. It shortens the time from sketching out application architecture to actual deployment. Cloud computing incorporates virtualization, on-demand deployment, Internet deliveryof services, and open source software. The benefits of cloud computing are many. One is reduced cost, since you pay as you go. Other benefits are the portability of the application is that users can work from home, work, or at client locations. This increased mobility means employees can access information anywhere they are. There is also the ability of cloud computing to free-up IT workers who may have been occupied performing updates, installing patches, or providing application support. Along with the good services of Cloud Computing has o offer, there are security problems which make users anxious about the safety, reliability and efficiency of migrating to cloud computing. Big companies have second thought whether to move into the cloud because they might compromise the operation and the important information of the company. After analysing and calculating the possible risk.Migrating into the "Cloud" will make computer processing much more convenient to the users. One of the considerations when moving to cloud is the security problems.

2. BACKGROUND

2.1 CLOUD COMPUTING MODELS

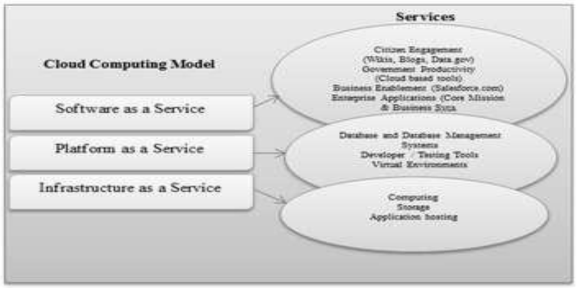

FIGURE-1

*a. SaaS:*Tousethe provider's applications runningon a cloud infrastructure and accessiblefrom various client devices through a thin client interface such as a Web browser.

*b. PaaS:*To deploy onto the cloud infrastructure consumer-created applications using programming languagesandtools supported by the provider(java, python, .Net)

c. IaaS: To provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications.

2.2 LAYERS OF CLOUD COMPUTING MODEL

There are five layers in cloud computing model, the Client Layer, Application Layer, Platform layer, Infrastructure layer and server layer. In order to address the security problems, every level should have security implementation.

Client Layer: In the cloud computing model, the cloud client consist of the computer hardware and the computer software that is totally based on the applications of the cloud services and basically designed in such way that it provides application delivery to the multiple servers at the same time, as some computers making use of the various devices which includes computers, phones, operating systems, browsers and other devices.

Application layer: The Cloud application services deliver software as a service over the internet for eliminating the need to install and run the application on the customer own computers using the simplified maintenance and support for the people which will use the cloud interchangeably for the network based access and management of the network software by controlling the activities which is managed in the central locationsby enabling customers to access the applications remotely with respect to Web and application software are also delivered to many model instances that includes the various standards that is price, partnership and management characteristics which provides the updates for the centralize features.

Platform layer: In the cloud computing, the cloud platform services provides the common computing platform and the stack solution which is often referred as the cloud infrastructure and maintaining the cloud applications that deploys the applications without any cost and complexity of the buying and managing the hardware and software layers.

Infrastructure layer: The Cloud Infrastructure services delivers the platform virtualization which shows onlythe desired features and hides the other ones using the environment in which servers, software or network equipment are fully outsourced as the utility computing which will based on the proper utilization of the resources by using the principle of reusability that includes the virtual private server offerings for the tier 3 data centerand many tie 4 attributes which is finally assembled up to form the hundreds of the virtual machines.

Server layer: The server layer also consist of the computation hardware and software support for the cloud service which is based on the multi-core processors and cloud specific operating systemsand coined offerings.

3. NETWORK ISSUES IN CLOUD COMPUTING:

Therearedifferentnetworkissuesoccurincloudcomputingsome ofwhicharediscussedbelow:

3-1DenialofService:

When hackers over flows a network server or web server with frequent request of services to damage the network, the denial of service cannot keep up with them, server could not legitimate client regular requests. For example a hacker hijacks the web server that could stop the functionality of the web server from providing the services In cloud computing, hacker attack on the server by sending thousands of requests to the server that server is unable to respond to the regular clients in this way server will not work properly. Counter measure for this attack is to reduce the privileges of the user that connected to a server. This will help to reduce the DOS attack. (ScarfoneK,2007)

3-2 Man in the Middle Attack:

This is another issue of network security tha will happen if secure socket layer (SSL) is not properly configured. For example if two parties are communicating with each other and SSL is not properly installed then all the data communication between two parties could be hack by the middle party. Counter measure for this attack is SSL should properly install and it should check before communication with other authorized parties.

3-3 Network Sniffing:

Another type of attack is network sniffer, it is a more critical issue of network security in which unencrypted data are hacked through network for example an attacker can hack passwords that are not properly encrypted during communication. If the communication parties not used encryption techniques for data security then attacker can capture the data during transmission as a third party. Counter measure for this attack is parties should used encryption methods for securing there data.

3-4 Port Scanning:

There may be some issues regarding port scanning that could be used by an attacker as Port80 (HTTP) is always open that is used for providing web services to the user. Other ports such as 21 (FTP) etc are not opened all the time it will open when needed therefore ports should be secured by encrypted until and unless the server software is configured properly. Counter measure for this attack is that fire wall is used to secure the data from port attacks.(Services,2009).

3-5 SQL Injection Attack:

SQL injection attacks are the attacks where a hackers uses the special characters to return the data for example in SQL scripting the query end up with where clause that may be modified by adding more information in it. For example an argument value of variable y or 1 == 1 may cause there turn of full table because 1 == 1 is always seems to be true.

3-6 Cross Site Scripting:

It is a type of attack in which user enters right URL of a web site and hacker on the others it redirect the user to its own web site and hack its credentials. For example user entered the URL in address bar and attacker redirects the user to hacker site and then he will obtain the sensitive data of the user. Cross site scripting attacks can provide the way to buffer overflows, DOS attacks and inserting spiteful software into the web browsers for violation of user's credentials. (Yang,2003)

4. SECURITY ISSUES IN CLOUD COMPUTING:

Security issues of cloud computing are discussed below:

4-1 XML Signature Element Wrapping:

XML signature Element Wrapping is the fine renowned attack for web service. It is use to defend a component name, attribute and value from illegal party but unable to protect the position in the documents. (Jamil&Zaki, 2011b) Attacker targets the component by operating the SOAP messages and putting anything that attacker like. Counter measure for this attack is using the digital certificate e.g. X.509 authorized by third party such as certificate authorities and also uses the mixture of WS-security with XML signature to a particular component. The following graph presents a view of the rate of cyber attacks in last 10 years.

4-2 Browser Security:

The second issue is Browser Security. As a client sent the request to the server by web browser the web browser have to make use of SSL to encrypt the credentials to authenticate the user. If hacker installs sniffing packages on intermediary host, the attacker may get the credentials of the user and use in these credentials in the cloud system as a valid user. (Jensen, 2009) Counter measure for this attack is Vendor should use WS-security concept on web browsers .

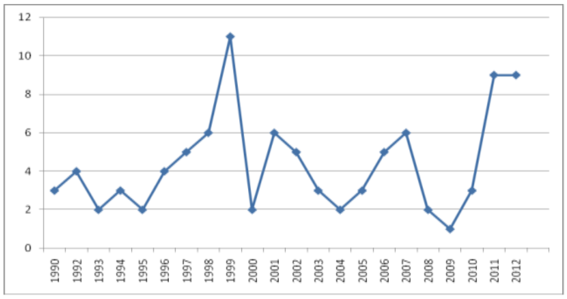

FIGURE-2

4-3 Cloud Malware Injection Attack:

The third issue is Cloud Malware Injection Attack, which tries to damage a spiteful service, application or virtual machine. An interloper is obligatory to generate his personal spiteful application, service or virtual machine request and put it into the cloud structure (Booth, 2004). Once the spiteful software is entered into the cloud structure, the attacker care for the spiteful software as legitimate request. If successful user ask for the spiteful service then malicious is implemented. Attacker upload virus program in to the cloud structure. Counter measure for this attack isauthenticity check for received messages. Store the original image file of the request by using hash function and compare it with the hash value of all upcoming service requests.

4-5 Data Protection:

Data protection in cloud computing is very important factor it could be complicated for the cloud customer toefficiently check the behavior of the cloud supplier and as a result he is confident that data is handled in a legal way, but it does not like that this problem is intensify in case of various transformation of data. Counter measure this attack is that a consumer of cloud computing should check data handle either it is handled lawfully or not.

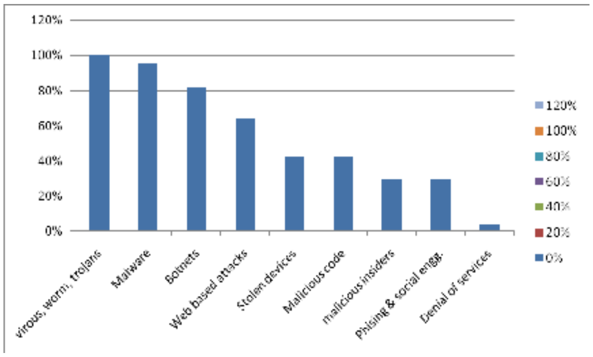

FIGURE-4

5. SECURITY ISSUE CAUSES AND SOLUTIONS:

We will focus on specific problems for various kind of attacks in the cloud: a) Wrapping attack, b) Malware-Injection attack, c) Flooding attack, d) Data stealing that can result from a Browser attack and e) Accountability checking.

*Wrapping Attack Problem:*When a user makes a requestfrom his VM through the browser, the request is first directed to the web server. In this server, a SOAP message is generated. This message contains the structural information that will be exchanged between the browser and server during the message passing. Before message passing occurs, the XML document needs to be signed and canonicalization has to be done. Finally, the SOAP header should contain all the necessary information for thedestination after computation is done.For a wrapping attack, the adversary does its deception during the translation of the SOAP message in the TLS (Transport Layer Service) layer. The body of the message is duplicated and sent to the server as a legitimate user. Theserver checks the authentication by the Signature Valuewhich is also duplicated) and integrity checking for themessage is done. As a result, the adversary is able to intrudein the cloud and can run malicious code to interrupt the usualfunctioning of the cloud servers.

Wrapping Attack Solution:

Since an adversary can intrude in the TLS layer; we propose to increase the security during the message passing from the web server to a web browser by using the SOAP message. Specifically, as thesignature value is appended, we can add a redundant bit (STAMP bit) with the SOAP header. This bit will be toggled when the message is interfered with by a third party during the transfer. When it is received in the destination, theSTAMP bit is checked first and if it is found toggled, then anew signature value is generated in the browser end and thenew value sent back to the server as recorded to modify theauthenticity checking.

*Malware-Injection Attack Problem:*In a malware-injection attack, an adversary attempts to inject malicious service or code, which appears as one of the valid instance services running in the cloud. If the attacker is successful, then the cloud service will suffer from eavesdropping. This can be accomplished via subtle data modifications to changethe functionality, or causing deadlocks, which forces a legitimate user to wait until the completion of a job which was not generated by the user.This type of attack is also known as ameta-data spoofing attack.When an instance of a legitimate user is ready to run in the cloud server, then the respective service accepts the instance for computation in the cloud.

Malware-Injection Attack Solution: Usually when a customer opens an account in the cloud, the provider creates an image of the customer's VM in the image repository system of the cloud. The applications that the customer willrun are considered with high efficiency and integrity. Wepropose to consider the integrity in the hardware level, because it is very difficult for an attacker to intrude in theIaaS level. We utilize the File Allocation Table (FAT) system architecture, since its straightforward technique is supported by virtually all existing operating systems From the FAT table we can know about the code or application that a customer is going to run.

Flooding Attacks: The fourth issue is Flooding Attack. Attacker attacks the cloud system openly. The most significant feature of cloud system is to make available of vigorously scalable recourses. Cloud system repeatedly increase its size when there is further requests from clients, cloud system initialize new service request in order to maintain client requirements. Flooding attack is basically distributing a great amount of non-sense requests to a certain service. Once the attacker throw a great amount of requests, by providing more recourses cloud system will attempt to work against the requests, ultimately system consume all recourses and not capable to supply service to normal requests from user. Then attacker attacks the service server.

Flooding Attacks solutions: Counter measure for this attack is it's not easy to stop Dos Attacks. To stop from attacking the server, Intrusion detection system will filter the malicious requests, installing firewall.

Data Stealing Problem: This is the most traditional and common approach to breach a user account. The user account and password are stolen by any means. As a result, the subsequent stealing of confidential data or even thedestroying of data can hamper the storage integrity and security of the cloud.

Data Stealing Solution: At the end of every session, the customer will send an e-Mail about the usage and duration with a special number to be used for log in next time. In this way, the customer will be aware of the usage and charges as well as be availed with a unique number to be used every time to access the system.

Accountability Check Problem: The payment method in acloud System is “No use No bill”. When a customer launches an instance, the duration of the instance, theamount of data transfer in the network and the number of CPU cycles per user are all recorded. Based on this recorded information, the customer is charged. So, when an attacker has engaged the cloud with a malicious service or runs malicious code, which consumes a lot of computationalpower and storage from the cloud server, then the legitimate account holder is charged for this kind of computation. As a result, a dispute arises and business reputations are hampered.

As there are some security issues in cloud so we need some strong laws against these issues keeping that in mind expearts decided to form some laws against these issues .Then on the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011, which came into effecton11 April, 2011.

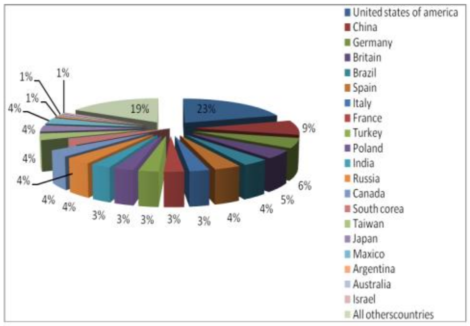

FIGURE-5

6. LAWS OF PRIVACY IN INDIA:

The Data Privacy Law in India is contained primarily in:

1. Section43A of the Information Technology Act
2InformationTechnology(Reason a security practices and procedures and sensitive personal data or information) Rules,2011.
3. Section 72 A of the Information Technology Act This paper focuses on the Information Technology(Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011, which came into effect on 11 April, 2011.These are referred to as *Data$Privacy$ Rules* in this paper.

The *Data Privacy Rules* relate to information of two primary types:

1."Personalinformation"which means any information that relates to a natural person, which, either directly or indirectly, in combination with other information available or likely to be available with a body corporate, is capable of identifying such person.
2. "Sensitive personal data or information" of a person Sensitive personal data or information does not include any information that is freely available or accessible in public domain or furnished under the Right to Information Act, 2005 or any other law. *Data Privacy Rules* includes :

1. Insurance companies
2. Banks
3. Hospitals
4. All business organizations
5. Doctors,
6. Stockbrokers
7. chartered accountants
8. Retails stores, restaurants, ecommerce Companies.
7. Call centers, BPOs, LPOs etc.

All these entities are required by law to provide a **data privacy policy** on their website. This policy should providedetails relating to:

1. Clear and easily accessible statements of its practices and policies,
2. Type of information collected,
3. Purpose of collection and usage of such information,
4. Disclosure of information
5. Reasonable security practices and procedures

All these entities must obtain consent from the provider of the information regarding purpose of usage **before** collection of such information.

Privacy policy for handling of or dealing in personal information including sensitive personal data or information of customers and employees as mandated by Rule 4 of Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011.NonDcompliance with any of the provisions of the data $privacy $rules is penalized with a compensation /penalty of upto Rs. 25,000 under section 45 of the Information Technology Act. Additionally, in some cases there may be liability under section 43A of the Information Technology Act. Under the original Information Technology Act, 2000, compensation claims were restricted to Rs. 1crore. Now claims up to Rs 5crore are under the jurisdiction of Adjudicating Officers. Claims above Rs5crore are under the jurisdiction of the relevant courts. Additionally, in some cases there may be liability under section 72A of the Information Technology Act. This section provides for imprisonment upto 3 years and / or fine uptoRs 5 lakh.

7. INFORMATION TECHNOLOGY AUDIT &COMPLIANCE SENSITIVE PERSONAL DATA ORINFORMATION RULES

MINISTRY OF COMMUNICATIONS ANDINFORMATION TECHNOLOGY

(Department of Information Technology)

NOTIFICATION

New Delhi, the 11th April, 2011

G.S.R. 313(E).—In exercise of the powers conferred by clause (ob) of sub-section (2) of section 87 read with section 43A of the Information Technology Act,2000 (21 of 2000), the Central Government hereby makes the following rules, namely.—

1. Short title and commencement

(1) These rules may be called the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011.

(2) They shall come into force on the date of their publication in the Official Gazette.

2. Definitions —

(1) In these rules, unless the context otherwise requires,

(a)"Act" means the Information Technology Act, 2000 (21 of 2000);

(b)"Biometrics" means the technologies that measure and analyse human body characteristics, such as 'fingerprints', 'eye retinas and irises', 'voice patterns', "facial patterns”, ‘hand measurements' and 'DNA' for authentication purposes;

(c)"Body corporate" means the body corporate as defined in clause (i) of explanation to section 43A of the Act;

(d) "Cyber incidents" means any real or suspected adverse event in relation to cyber security that violates an explicitly or implicitly applicable security policy resulting

In unauthorised access, denial of service or disruption, unauthorised use of a computer resource for processing or storage of information or changes to data, information without authorisation;

(e)"Data" means data as defined in clause (o) of sub-section (1) of section 2 of the Act;

(f)"Information" means information as defined in clause (v) of sub-section (1) of section 2 of the Act;

(g)"Intermediary" means an intermediary as defined in clause (w) of sub-section

(1) of section 2 of the Act;

(h) "Password" means a secret word or phrase or code or passphrase or secret key or encryption or decryption keys that one uses to gain admittance or access to information;

(i)"Personal information" means any information that relates to a natural person,which, either directly or indirectly, in combination with other information available or likely to be available with a body corporate, is capable of identifying such person.

(2) All other words and expressions used and not defined in these rules but defined in theAct shall have the meanings respectively assigned to them in the Act.

3.Sensitive personal data or information.

Sensitive personal data or information of a person means such personal information which consists of information relating to;—

(i) password;

(ii) financial information such as Bank account or credit card or debit card or other payment instrument details ;

(iii) physical, physiological and mental health condition;

(iv) sexual orientation;

(v) medical records and history;

(vii) any detail relating to the above clauses as provided to body corporate for providing service; and

(viii) any of the information received under above clauses by body corporate for processing, stored or processed under lawful contract or otherwise:

provided that, any information that is freely available or accessible in public domain for furnished under the Right to Information Act, 2005 or any other law for the time being in force shall not be regarded as sensitive personal data or information for the purposes of these rules.

4. Body corporate to provide policy for privacy and disclosure of information.— (1)

The body corporate or any person who on behalf of body corporate collects, receives, possess, stores, deals or handle information of provider of information, shall provide a privacy policy for handling of or dealing in personal information including sensitive personal data or information and ensure that the same are available for view by such providers of information who has provided such information under lawful contract.

(i) Clear and easily accessible statements of its practices and policies;

(ii) type of personal or sensitive personal data or information collected under rule 3;

(iii) purpose of collection and usage of such information;

(iv) disclosure of information including sensitive personal data or information as provided in rule 6;

(v) reasonable security practices and procedures as provided under rule 8.

5. Collectionofinformation.

(1) Body corporate or any person on its behalf shallobtain consent in writing through letter or Fax or email from the provider of the sensitive personal data or information regarding purpose of usage before collection of such information.

(2) Body corporate or any person on its behalf shall not collect sensitive personal data or information unless

(a) the information is collected for a lawful purpose connected with a function or activity of the body corporate or any person on its behalf; and

(b) The collection of the sensitive personal data or information is considered necessary for that purpose.

(3) While collecting information directly from the person concerned, the body corporate or any person on its behalf snail take such steps as are, in the circumstances, reasonable to ensure that the person concerned is having the knowledge of

(a) the fact that the information is being collected;

(b) the purpose for which the information is being collected; (c) the intended recipients of the information; and

(d) the name and address of

(i) the agency that is collecting the information; and

(ii) the agency that will retain the information.

(4) Body corporate or any person on its behalf holding sensitive personal data or information shall not retain that information for longer than is required for the purposes for which the information may lawfully be used or is otherwise required under any other law for the time being in force.

(5) The information collected shall be used for the purpose for which it has been collected.

(6) Body corporate or any person on its behalf permit the providers of information, as and when requested by them, to review the information they had provided and ensure that any personal information or sensitive personal data or information found to be inaccurate or deficient shall be corrected or amended as feasible:Provided that a body corporate shall not be responsible for the authenticity of the personal information or sensitive personal data or information supplied bythe provider of information to such boy corporate or any other person acting on behalf of such body corporate.

6. Disclosure of information.

(1) Disclosure of sensitive personal data or information by body corporate to any third party shall require prior permission from the provider of such information, who has provided such information under lawful contract or otherwise, unless such disclosure has been agreed to in the contract between the body corporate and provider of information, or where the disclosure is necessary for compliance of a legal obligation.

(2) Notwithstanding anything contain in sub-rule (1), any sensitive personal data on Information shall be disclosed to any third party by an order under the law for the time being in force.

(3)The body corporate or any person on its behalf shall not publish the sensitive personal data or information.

(4) The third party receiving the sensitive personal data or information from body corporate or any person on its behalf under sub-rule (1) shall not disclose it further.

7. *Transfer of information.*

A body corporate or any person on its behalf may transfersensitive personal data or information including any information, to any other body corporate or a person in India, or located in any other country, that ensures the same levelof data protection that is adhered to by the body corporate as provided for under these Rules.

8. Reasonable Security Practices and Procedures.

(1) A body corporate or a person on its behalf shall be considered to have complied with reasonable security practices and procedures, if they have implemented such security practices and standards and have a comprehensive documented information security programme and information security policies that contain managerial, technical, operational and physical security control measures that are commensurate with the information assets being protected with the nature of business.

(2) The international Standard IS/ISO/IEC 27001 on "Information

(3) Any industry association or an entity formed by such an association, whose members are self-regulating by following other than IS/ISO/IEC codes of best practices for data protection as per sub-rule(1), shall get its codes of best practices duly approved and notified by the Central Government for effective implementation.

(4) The body corporate or a person on its behalf who have implemented either IS/ISO/IEC 27001 standard or the codes of best practices for data protection as approved and notified under sub-rule

(5) shall be deemed toG have complied with reasonable security practices and procedures provided that such standard or the codes of best practices have been certified , duly approved by the CentralGovernment.

CONCLUSIONS AND FUTURE WORK

Cloud computing is a new term that is introduced in business environment where users can interact directly with the virtualized resources and safe the cost for the consumers. Some security issues and their counter measures are discussed in this paper. It has several models to protect its data for the business users. An organization used private clouds within its organization to prevent from loss of data. Cloud computing have several deployment models that help in retrieving the information. SAAS, PAAS, IAAS are the three models for cloud computing. Security in cloud computing consist of security abilities of web browsers and web service structure. Some laws of data pravicy are also discussed in this papare. Under these laws there are also the provision for compensation andimprisonment.These rules and laws has been proved successful in resolving the security issues of cloud computing.

REFERENCES

[1] “Attack on Cloud Computing” By NaradWaheed.
[2]“Complying with the Data Privacy Law in India” By RohasNagpl Asian School of Cyber Laws.Publishedin2012byAsianSchoolofCyberLaws.!
[3] **“**Security Attacks and Solutions in Clouds” KaziZunnurhain and Susan V. VrbskyDepartment of Computer Science ,The University of Alabama ,Tuscaloosa, AL 35487-0290, e-mail- kzunnurhain@crimson.ua.edu, vrbsky@cs.ua.edu

[4]“Securevirtualizationforcloudcomputing”FlavioLombardi[a] ,RobertoDiPietro[b,c,]..[a]ConsiglioNazionaledelleRicerche,DCSPI-SistemiInformativi,PiazzaleAldoMoro7,00187Roma,Italy [b]UniversitadiRomaTre,DipartimentodiMatematica,L.goS.LeonardoMurialdo,100149Roma,Italy [c]UNESCOChairinDataPrivacy,UniversitatRoviraiVirgili,Tarragona,Spain
[5] Danish Jamil et al. / International Journal of Engineering Science and Technology (IJEST)”SECURITY ISSUES IN CLOUD COMPUTING AND COUNTERMEASURES” DANISH JAMIL Department of Computer Engineering, Sir Syed University of Engineering & Technology, Main University Road, Karachi, Sindh-75300, Pakistan,HASSAN ZAKI Department of Computer Engineering, Sir Syed University of Engineering & Technology, Main UniversityRoad, Karachi, Sindh-75300, Pakistan
[6]“The Basics of Cloud Computing”AlexaHuth and James Cebulahttp://csrc.nist.gov/publications/drafts/800-145/Draft-SP-800-145_cloud-definition.pdf