RESEARCH ARTICLE OPEN ACCESS

A Theoretical Aspect of Cloud Computing Service Models and Its Security Issues: A Paradigm

S. B. Dash*, H.Saini **, T.C.Panda*, A. Mishra***
* Department of Information Technology, Orissa Engineering College, Bhubaneswar, India-752050
** Department of Computer Science & Engineering, Jaypee University of Information Technology, Solan, India-173234
***Department of Mathematics, CUTM, Paralakhemundi, India-761211

ABSTRACT
Cloud computing is a distributed computing environment that provides on demand services to the users for deploying their computational needs in a virtualized environment without the knowledge of technical infrastructure. Due to reliability, scalability, high performance and low band width most of the organizations are running their applications in cloud. The cloud service providers provide the services to the registered cloud users on payment basic across the glove. The cloud services are basically categorized as SaaS, PaaS, and IaaS. The services are available to the users depending on cloud deployment and the SLA (service level agreements) between the service providers and the users. Providing security to the users and trust into cloud environment is the responsibility of the cloud service providers. The main objective of this paper is to provide a clear idea about the cloud service models and outline the security issues in the service models.

Keywords - Cloud computing; Cloud computing models; Cloud Security Issues; Cloud Security Threats.

I. INTRODUCTION

Cloud computing is one of the most significantly achieved development in the IT industry. Most of the companies are running their applications in the cloud due to the rapid advancement in communication network. It is a next generation computing platform that helps the users to share the resources through communication mediums. According to National Institute of Standards and Technology (NIST) one of the most accepted definition of cloud computing is "*Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction*". European Community for Software and Software Services (ECSS) defines "*cloud computing as the delivery of computational resources from a location other than your current one"*.[1,2,3] So in simple words cloud computing can be defined as a distributed computing environment that enables the users to access and exchange their resources (applications and data) remotely and provides services to use the remote hardware and software within a network without the knowledge of technological infrastructure[4] . The figure-1 shown below gives a clear idea regarding the infrastructure requirements for cloud deployment.

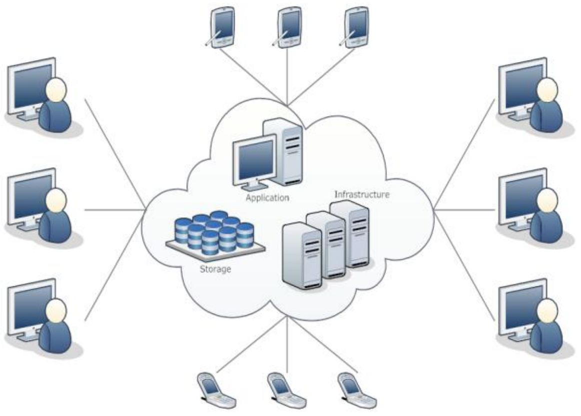

Figure-1The Cloud infrastructure

II. ADVANTAGES OF CLOUD COMPUTING

1. Flexibility/Elasticity:

Users can access computing resources as and when needed, without any human interaction. Capabilities can be rapidly and elastically provided in some cases automatically.[5]

2. Scalability Of Infrastructure.

New nodes can be added or removed from the network as can physical servers, with limited modifications to infrastructure set up and software. Cloud architecture can scale horizontally or vertically according to the user's requirements.[5]

3. **Broad Network Access.**

Capabilities are available over the network and accessed through standard mechanisms that promotes by using heterogeneous platforms (like mobile phones, laptops, and PDAs).

4. **Location Independence.**

Cloud interfaces are location independent and they can be accessed by well established interfaces such as Web services and Web browsers, so that no knowledge about exact location of the user is required. It gives high level of abstraction to the users data.

5. **Unlimited Storage.**

Storing information in the cloud gives almost unlimited storage capacity. Hence no more need to worry about running out of storage space or increasing current storage space availability.

6. **Easy Access to Information.**

Once registered in the cloud environment any one can access the information from any location provided, there is an Internet connection.

7. **Economies Of Scale And Cost Effectiveness.**

Cloud implementations regardless of the deployment models tend to be as large as possible in order to take advantage of economies of scale. Large cloud deployments can often be located close to cheap deployment to lower cost. It does not require upfront investment and much capital expenditure. Users may pay and use or pay for services and capacity as they need them.

8. **Backup and Recovery.**

Since all the user's data is stored in the cloud, backing it up and restoring the same is relatively much easier than storing the same on a physical device. Most cloud service providers are usually competent enough to handle recovery of information. Hence this makes the entire process of backup and recovery much simpler than other traditional methods of data storage.

9. **Reliability**

It improves the use of multiple sites which makes cloud computing suitable for business continuity and disaster recovery.

10. **Sustainability**

It improves resource utilization and makes the cloud environment more efficient.

III. CLOUD COMPUTING MODELS

Based on the usages of data and applications cloud computing services are broadly classified in three different types called as cloud service models. Figure- 2 shows the different types of cloud service model present in cloud environment.

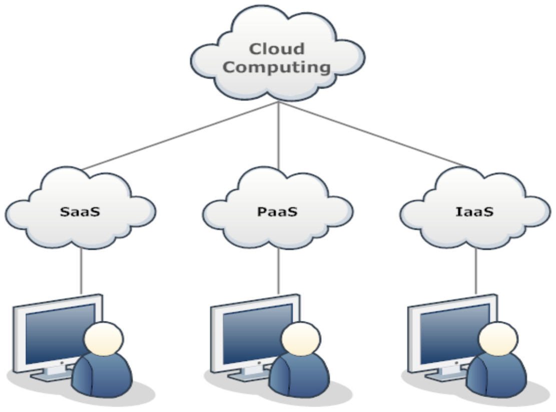

Figure-2 Types of cloud service models

And according to the usages of data and applications required by the users the cloud computing models are broadly classified in four different types called as cloud deployment models.[6,7,8,9].

IV. CLOUD COMPUTING SERVICE MODELS.

A. Infrastructure as a Service(IaaS)

Infrastructure as a Service (IaaS) is one of the three fundamental service models of cloud computing . A layers of cloud computing model and their infrastructural requirements is shown in the figure -3. In this model the users are allocated with computing resources in order to run their applications. The computing services are provided in a virtualized environment i.e in cloud by using a communication network. The best known example of IaaS is Amazon Cloud Formation, Amazon EC2. It can be implemented by utilizing the concepts like Enterprise infrastructure, Cloud hosting, and Virtual Data Centers (VDC). *Network as a service (NaaS) is a* category of cloud infrastructure services where the user can use the network connectivity as a services. NaaS involves the optimization of resource allocations and resource computing in the network. VPN, and bandwidth on demand are the common example of NaaS.[10,11,12,13,14]

Advantages of IaaS.

1. Resources are available on demand as and when the user requires it. That means the user will not have to worry about the Infrastructure required to run the application. so this scalable.
2. In IaaS the Infrastructure i.e the virtualized environment is set up and maintained by the cloud provider. So no investment in hardware for

the users. As it saves the implementation cost and time of execution.

3. The service can be accessed on demand and the client only pays for the resource or application used not for the Infrastructure
4. The service can be accessed from any location 24X7 provided there is an internet connection. So IaaS is location independent.
5. Physical security of user's data is the responsibility of the cloud provider. So the time required to give security to data is saved.
6. The chance of system failure is less. Any case of failure will be smoothly handled by the service provider. So it is fault tolerant.

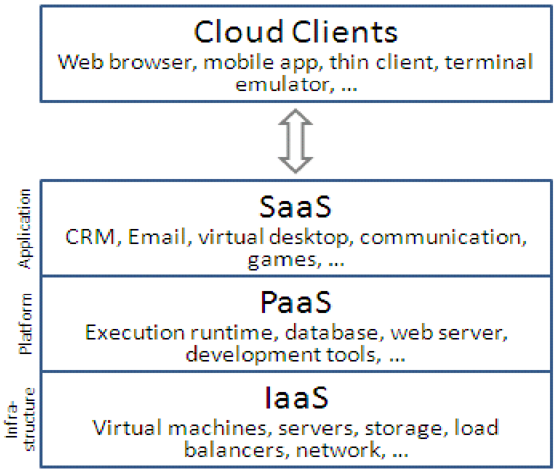
Cloud Clients
Web browser, mobile app, thin client, terminal emulator, ...
SaaS
CRM, Email, virtual desktop, communication, games, ...
PaaS
Execution runtime, database, web server, development tools, ...
IaaS
Virtual machines, servers, storage, load balancers, network, ...
Application
Platform
Infra-structure

Figure-3 The layers of cloud service models

B. Platform as a Service(PaaS).

Platform as a Service is a category of cloud computing service model that provides the developers a platform to build and use applications and services by using a communication network. PaaS services are available in the cloud and accessed by users by using web browsers. In the PaaS model, cloud providers provides a platform which includes operating system, programming language execution environment, database, and web server. The users can use these facilities to develop their applications. The well known PaaS providers are AWS Elastic Beanstalk, Cloud Foundry, Heroku, Force.com, OrangeScape. The services are constantly updated by the service providers, with existing features upgraded and additional features added. In PaaS services the user has to pay for a subscription basis and charged just for what they use. PaaS includes Operating system, Server-side scripting environment, Database management system, Server Software, Network access tools for design and development and web hosting. [13,14,15,16]

Advantages of PaaS:

1. The user doesn't have to invest for physical infrastructure as it will be provided by IaaS on demand. So this gives fully mobility to focus on the development of applications.
2. With PaaS services application development is simple. So anyone can develop an application with less technical knowledge by using web browser.
3. User can have control over the applications that are installed within their platforms and can create a platform that suits their specific requirements. They can 'pick and choose' the features they feel as necessary.
4. In PaaS the applications can be changed or modified if required.
5. The services are not isolated, application specific or location dependent. So users in various locations can work together provided they are connected through a communication medium.
6. Security of user's data and the application is the responsibility of the cloud provider. Data security, backup and recovery are the major security issues.

C. Software as a Service(SaaS)

The third model is **Software as a Service** which provides a platform in which the users access the software from the cloud. The users of SaaS will not have to worried about managing the cloud infrastructure and platform on which the application is running. The software installation and operation is the responsibility of the service providers and already available by using IaaS and PaaS.[13,14,15,16] This is typically end user applications delivered on demand over a network on a pay per use basis. The examples of SaaS include: google apps, MicrosoftOffice365, Onlive, GT Nexus, Marketo, and TradeCard. These applications are hosted in "the cloud" and can be used for a wide range of tasks for both individuals and organizations.[17,18,19]

Advantages of SaaS.

1. No additional infrastructure or platform required to run the applications, as it provided by the service provider (IaaS and PaaS).
2. Software Applications are ready to use once the user subscribes. The user only have to pay for software not for infrastructure or platform setup.
3. With SaaS services application development is simple. So anyone can develop an application with less technical knowledge any time by using web browser.
4. Software updating is automatic i.e if any updates are available online to existing user, offered free of charges.
5. SaaS provides mobility to the user where applications can be accessed via any internet enabled device, which makes it ideal for those who use a number of different devices, such as

internet enabled phones and tablets, and those who don't always use the same computer.

6. The services are not isolated, application specific or location dependent. So users in various locations can work together provided they as connected through a communication medium.
7. There are no initial setup costs is required with SaaS, as SaaS offered with other services.

V. SECURITY ISSUES

The security issues in cloud computing environment are greatest challenge of information system. Understanding the risks of the security and privacy in the cloud computing environment and developing efficient and effective solutions for it is really a difficult task. Confidentiality, integrity, reliability and availability are widely used terminology for security issues in cloud computing environment means that the user's data in the cloud should remain confidential and protected from unauthorized access.[19]So the implementation of the cloud computing architecture must be ensured about the security of its resource nodes. Some of the security issues occur in cloud computing are listed below.[20,21,22,23,24]

1. Cloud Security

This includes organizational and technical issues related to keeping cloud services at an acceptable level of security by ensuring the computing resources available and usable by its authentic users. Security threats to cloud infrastructure would affect multiple users even if only one site is attacked.[20]These risks can be overcome by using encrypted file systems, security applications, data loss software and buying security hardware.

2. Privacy in Cloud.

Privacy is the process of making sure that the user's data remains private, confidential and restricted from unauthorized users. Due to data virtualization the users data may be stored in various virtual data centers rather than in the local computers. So the unauthorized users may access the private information of the authorized users. Data authentication is one of the most popular options of security before putting the sensitive data into cloud.[20]

3. Data integrity and Reliability

In cloud computing, anyone from any location can access the data. Cloud does not differentiate between common data and sensitive data. So an important aspect of cloud services is availability of user's data with reliability. It is necessary for the cloud service provider to ensure the integrity by making their system capable to check over the cloud data from any unauthorized access.

4. Performance and Bandwidth cost.

The major issues that can affect performance in cloud based environment is due to the unethical transaction-oriented and data access applications. So the users who are at a long distance from cloud providers may experience high latency and delay, this is due to the availability bandwidth in the network. Bandwidth cost may be low for smaller Internet-based applications, which are not data intensive, but could significantly, grow for data-intensive applications. The service providers instead of saving money on hardware, they should spend more for the bandwidth. This can deliver intensive and complex application over the network.

VI. SECURITY THREATS

A threat is define as an external force by which the nodes existing in one state transfers into other. A node in the cloud environment stores the data and information and gives the user a platform to use the application in the form of services. There are significant numbers of attacks or intrusions occurs in the cloud based applications. Some well known attacks are listed below.[25-32]

1. SQL Injection Attack.

An SQL injection is a computer attack mostly affects to SAAS model, in which malicious code is embedded with a poorly-designed application, executes unauthorized SQL commands by taking advantage of insecure interface connected through Internet.[19] SQL injection attacks are used to access information from databases, which is protected from public access.SQL injection attacks are avoided by ensuring systems having strong input validation.

2. Abuse And Nefarious Use Of Cloud Computing

In this threat the hackers take the advantages of shortcomings in the authentic registration process associated with cloud. After the successful registration, the cloud service providers offer SAAS, IAAS and PAAS services to the users. But hackers may be able to conduct susceptible activities like Spamming and Phishing. This threat exists in all the three layers of the service models.

3. Net Sniffers

Net sniffer is a type SAAS service model threat in which the attackers use to gain access through applications, which can capture packets flowing in a network and if the data that is being transferred through these packets is not encrypted. Then data can be publicly available and read by any one.

4. Session Hijacking

Session hijacking is a security attack on a user session over a protected network. when a user logs into a website, a session is created on that Web Server for that user, this session contains all this user's information being used by the server so the username and password is not required at every page request. So hackers having adequate knowledge can exploits a valid computer session and gains access to a user's session identifiers through HTTP. The Web server uses a unique identifier (Session Identifier) to authenticate the users for the session. The hackers by using Session Hijacking attack unethically gets the user's session identifier and then gain the illegal access to the user data. the most common Session hijacking attacks are Session Prediction ,Session Sidejacking ,Session Fixation ,Cross Site Scripting and available in SAAS and PAAS.

5. Man In The Middle Attack

Another type of session hijacking is known as a man-in-the-middle attack. Where the attacker uses a sniffer to observe the communication between devices and collect the data that is transmitted. In this the attackers make independent connections with the victim's computer and making them believe that they are connected directly to each other over a private connection. But in fact the entire session is controlled by the attackers. This is a threat to SAAS.

6. Denial Of Services

A Denial Of Services is a attack in the SAAS layer, that attempts to make the network resource and services actually assigned to the authorized users virtually unavailable. As it acts as an interrupt or suspend of services for authorized users temporarily or indefinitely.

7. Flooding Attacks

Flooding is a Denial of Service attack that is designed to increase network conjunctions by flooding it with huge amount of traffic. Flooding attacks occur when a network or service becomes so weighed with packets contains data. It attacks a server or host with connections that cannot be completed and finally fills the host memory buffer with unused and redundant data. Once the buffer is full no further connections can be made. So the result is a Denial of Service. It is available in PAAS and IAAS layer of cloud service model.

8. Privacy Breach

Since data from various users and business organizations available together in a cloud environment, so breaching in cloud environment will attack the data of the authorized users. Hence the unauthorized users can access the private data of the cloud users and do some susceptible activities with the data. This will affect mostly the SAAS users. A list of security threats that occur in cloud service models are given in the Table-1.[28-36]

SECURITY THREATS IN SERVICE MODELS				
SLNO	SECURITY THREATS	SAAS	PAAS	IAAS
1.	Abuse And Nefarious Use Of Cloud Computing	√	√	√
2.	Data And Information Loss	x	x	√
3.	Denial Of Services	√	x	x
4.	Exposure In Network	√	x	x
5.	Hardware Attack.	x	x	√
6.	Insecure Interfaces And APIs	√	√	√
7.	Malicious Insiders	√	√	√
8.	Man In The Middle Attack	√	x	x
9.	Modification And Deletion Of Data.	√	√	x
10.	Modification And Threat To Hardware	x	x	√
11.	Net Sniffers	√	x	x
12.	Port Scanning	x	x	√
13.	Privacy Breach	√	x	x
14.	Session Hijacking	√	√	x
15.	Shared Technology Vulnerabilities.	x	√	√
16.	SQL Injection Attack.	√	x	x
17.	Unauthorized And Unauthentic Use Of Cloud	√	x	x
18.	Unknown Risk Profile.	√	√	√

Table-1: Security threat in various cloud service model

.

VII. CONCLUSION AND FUTURE WORK

Understanding the risks of the security and privacy in the cloud computing environment and developing efficient and effective solutions for it is really a difficult task. Confidentiality, integrity, reliability and availability are widely used terminology for security issues in cloud computing environment. In this paper, we have discussed some trust issues and classify the security threats related to cloud computing service models. As security is the biggest issue, so these issues have to be solved as soon as possible to make maximum benefits of the cloud usages. These threats can be predicted from the attack history or from the vulnerability analysis of the network which requires a considerable efforts and use of resources. Therefore, a prediction method can help to fix these issues.

REFERENCES

[1]. Wikipedia, http://en.wikipedia.org/wiki/Cloud_Computning

[2]. Rafael Moreno-Vozmediano,Rubén S. Montero, Ignacio M. Llorente,” Key Challenges in Cloud Computing *-Enabling the Future Internet of Services*”, Published by the IEEE Computer Society 1089-7801/13/ © 2013 IEEE, IEEE internet computing

[3]. Dimitrios Zissis , Dimitrios Lekkas, “Addressing cloud computing security issues”, 0167-739X/ © 2010 Elsevier B.V. All rights reserved.doi:10.1016/j.future.2010.12.006.

[4]. M.Rajendra Prasad, R. Lakshman Naik, V.Bapuji,” Cloud Computing : Research Issues and Implications ”, International Journal of Cloud Computing and Services Science (IJ-CLOSER) Vol.2, No.2, April 2013, pp. 134~140 ISSN: 2089-3337.

[5]. Francesco M.A and Gianni F. “An approach to a cloud Computing network”, IEEE, August 2008, pp113-118

[6]. Huaglory Tianfield,”Cloud Computing Architectures”, 978-1-4577-0653-0/11/©2011 IEEE.

[7]. Xu Xiaoping, Yan Junhu,” Research on Cloud Computing Security Platform”, 978-0-7695-4789-3/12 © 2012 IEEE DOI 10.1109/ICCIS.2012.238.

[8]. “Understanding Cloud Computing Vulnerabilities”, by the ieee computer and reliability societies 1540-7993/11/ © 2011 IEEE march/april 2011.

[9]. Hassan Takabi , James B.D. Joshi, Gail-Joon Ahn, “Security and Privacy Challenges in Cloud Computing Environments”, by the ieee computer and reliability societies ,1540-7993/10/ © 2010 IEEE , november/december 2010.

[10]. Zhifeng Xiao and Yang Xiao, *Senior Member, IEEE,”* Security and Privacy in Cloud Computing*”,* IEEE communications surveys & tutorials, VOL. 15, NO. 2, second quarter 2013, 1553-877X/13/ c_ 2013 IEEE.

[11]. Peter Mell,” What’s Special about Cloud Security? ”, IT Pro July/August 2012, Published by the IEEE Computer Society, 1520-9202/12/ © 2012 IEEE.

[12]. Jianhua Che, Yamin Duan, Tao Zhang, Jie Fan,” Study on the security models and strategies of cloud computing”, 1877-7058 © 2011 Published by Elsevier Ltd. doi:10.1016/j.proeng.2011.11.2551.

[13]. Xue Jing, Zhang Jian-jun2. “A Brief Survey on the Security Model of Cloud Computing" 978-0-7695-4110-5/10 © 2010 IEEE DOI 10.1109/DCABES.2010.103

[14]. Engr: Farhan Bashir Shaikh, Sajjad Haider,” Security Threats in Cloud Computing”, 978-1-908320-00-1/11@2011 IEEE

[15]. H.Sato,et al., “A Cloud Trust Model in a Security Aware Cloud”, SAINT2010, pp.121-124.

[16]. Mladen A. Vouch, ”Cloud Computing Issues, Research and Implementationsǁ”, Journal of Computing and Information Technology - CIT 16, 2008, 4, 235–246

[17]. Latifa Ben, Arfa Rabai , Mouna Jouini, Anis Ben Aissa , Ali Mili,” A cybersecurity model in cloud computing environments”, 1319-1578 ª 2012 King Saud University. Production and hosting by Elsevier B.V. All rights reserved.http://dx.doi.org/10.1016/j.jksuci.2012.06.002.

[18]. M. Mackay, T. Baker, A. Al-Yasiri,” Security-oriented cloud computing platform for critical infrastructures”, 0267-3649/ 2012 M. Mackay, T. Baker & A. Al-Yasiri. Published by Elsevier Ltd. All right reserved.http://dx.doi.org/10.1016/j.clsr.2012.07.007.

[19]. S. Subashini , V.Kavitha,” A survey on security issues in service delivery models of cloud computing”, 1084-8045/ 2010 ElsevierLtd. All rights reserved. doi:10.1016/j.jnca.2010.07.006.

[20]. Xue Jing, Zhang Jian-jun,” A Brief Survey on the Security Model of Cloud Computing”, 2010 Ninth International Symposium on Distributed Computing and Applications to Business, Engineering and Science, 978-0-7695-4110-5/10 © 2010 IEEE DOI 10.1109/DCABES.2010.103.

[21]. Shigeaki Tanimoto, Manami Hiramoto, Motoi Iwashita, Hiroyuki Sato, Atsushi Kanai” Risk Management on the Security Problem in Cloud Computing ”, 2011 First ACIS/JNU International Conference on Computers, Networks, Systems, and Industrial Engineering, 978-0-7695-4417-5/11 © 2011 IEEE DOI 10.1109/CNSI.2011.82.

[22]. Farhan Bashir Shaikh, Sajjad Haider," Security Threats in Cloud Computing", 978-1-908320-00-1/11 © 2011 IEEE.

[23]. Wentao Liu," Research on Cloud Computing Security Problem and Strategy", 978-1-4577-1415-3/12/©2012 IEEE.

[24]. Eman M.Mohamed, Hatem S. Abdelkader, Sherif EI-Etriby," Enhanced Data Security Model for Cloud Computing ", The 8th International Conference on INFOrmatics and Systems (INFOS2012) - 14-16 May 2012, Cloud and Mobile Computing Track, Faculty of Computers and Information - Cairo University.

[25]. Gurudatt Kulkarni , Jayant Gambhir ,Tejswini Patil ,Amruta Dongare," A Security Aspects in Cloud Computing ", 978-1-4673-2008-5/12/ ©2012 IEEE.

[26]. Su Qinggang, Wang Fu, Hang Qiangwei," Study of Cloud Computing Security Service Model", 978-1-4577-1964-6/12/ ©2012 IEEE.

[27]. Anup Sharma, Robin A. Gandhi, William Mahoney, William Sousan, Qiuming Zhu," Building a Social Dimensional Threat Model from Current and Historic Events of Cyber Attacks", IEEE International Conference on Social Computing / IEEE International Conference on Privacy, Security, Risk and Trust, 978-0-7695-4211-9/10 © 2010 IEEE DOI 10.1109/SocialCom.2010.145.

[28]. Devki Gaurav Pal, Ravi Krishna, Prashant Srivastava, Sushil Kumar, Monark Bag, Vrijendra Singh," A Novel Open Security Framework for Cloud Computing ", International Journal of Cloud Computing and Services Science (IJ-CLOSER) Vol.1, No.2, June 2012, pp. 45~52 ISSN: 2089-3337.

[29]. Y. Jianfeng, C. Zhibin. "Cloud Computing Research and Security Issues" CISE 2010. Dec, 2010

[30]. Ashish Kumar," World of Cloud Computing & Security ", International Journal of Cloud Computing and Services Science (IJ-CLOSER) Vol.1, No.2, June 2012, pp. 53~58 ISSN: 2089-3337.

[31]. Wenjuan FAN, Shanlin Yang, Jun Pei, He Luo," Building trust into cloud ", International Journal of Cloud Computing and Services Science (IJ-CLOSER) Vol.1, No.3, August 2012, pp. 115~122 ISSN: 2089-3337.

[32]. Hemraj Saini, Dinesh Saini. Malicious Object dynamics in the presence of Anti Malicious Software" European Journal of Scientific Research, [ISSN: 1450-216X], volume-18, Issue-3, pp.-491-499, (2007).

[33]. Zhidong Shen, Qiang Tong," The Security of Cloud Computing System enabled by Trusted Computing Technology ", *2010 2nd International Conference on Signal Processing Systems (ICSPS)*, 978-1-4244-6893-5/C 2010 IEEE

[34]. Sylvain P. Leblanc, Andrew Partington, Ian Chapman, and Mélanie Bernier. An overview of cyber attack and computer network operations simulation. In Proceedings of the 2011 Military Modeling & Simulation Symposium (MMS '11) (2011). Society for Computer Simulation International, San Diego, CA, USA, 92-100.

[35]. Hemraj Saini, T. C. Panda, Minaketan Panda. 2011. Prediction of Malicious Objects in Computer Network and Defense", International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.6, pp.-161-171, 2011.

[36]. Xiaojun Yu, Qiaoyan Wen," A view about cloud data security From data life cycle", 978-1-4244-5392-4/10/ ©2010 IEEE