JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

A Review on the Risk and its Countermeasures in Cloud Environment

***Sourav Kumar Upadhyay*[1], *Dr. S.C. Dutta*[2], *Dr. Prakash Kumar*[3]**
[1]*Research Scholar,* [2]*Associate Professor (HOD),* [3]*Assistant Professor (HOD)*
[1]*BIT Sindri, Dhanbad, India*
sourav.cs.rnc@gmail.com[1], *scdutta@bitsindri.ac.in*[2], *mail.drprakash@gmail.com*[3]

Abstract: **The majority of application software and data are moved to cloud computing data centers, network service providers, and all other Application development, data management, and upkeep tasks are completed by the companies that offer cloud computing services. In this paper, we have discussed the Cloud computing application architecture, risk in cloud environment, latest threats that may affect the working of cloud, and how to mitigate those threats in real time environment.**

Index Terms- Cloud Computing, Cloud Security, Threats to cloud security, Countermeasures to cloud threats.

I. INTRODUCTION

One of the primary reasons people use modern Internet-based technology nowadays is cloud computing. The National Institute of Standards and Technology (NIST) [1] states that cloud computing provides on-demand, useful, all-encompassing, and reliable network access to significant configured shareable computing resources that can be easily managed and utilized with interaction from cloud service providers and little effort [2]. Modern information system techniques allow for dynamic resource sharing across the Internet and provide financial benefits [3]. The Pay as You Go (PYAG) concept, in which you pay only for the services you use, serves as the inspiration for cloud computing [4].One of the most notable benefits of the PAYG approach is that we might reduce our utilization by supplying specific assets when needed. According to their needs, clients can choose the operating system, RAM, CPU, networking, and access control. On the client's or end-request, user's assets are delivered [5]. Researchers are interested in cloud since it benefits both individual users and business greatly [6]. The cloud's services are indicated by the terms XaaS and X=[S, P, I] and are used for task execution through the internet. The cloud provides the resource pooling facility to improve service availability and shorten execution times [7]. As shown in figure 1, cloud computing allays concerns about resource shortages by providing a variety of services adapted to the needs of clients [8] at several levels, such as Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). Cloud services deliver various programmers without requiring the client to install them on their machine. Developers and application designers now have the option to create applications without investing on a server. It also offers virtualized copies of the actual hardware resources. These cloud-based services can all potentially cut expenses and processing power [10], but they also expose themselves to security risks. One of the most important problems that could seriously impact both the tenant and the cloud service providers is a data breach. Many other types of data, including personal data (such as social security numbers, private messages, credit card numbers, and addresses) and commercial data may be stolen. In the current situation, the cloud user, who may be the service or data owner, totally relies on the service provider for information security and privacy [11].

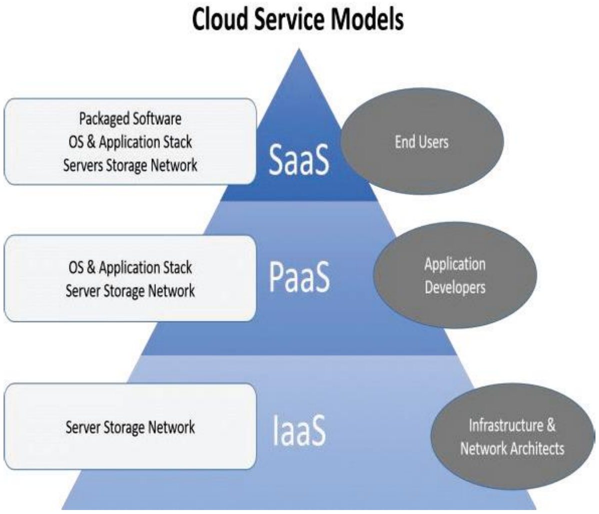

Fig.1. Services of Cloud [11]

II. PREVIOUS WORK

Cloud computing encompasses any hardware and software that provide user services. According to the University of California, the hardware and software in the computer network that make up the data resource pool are referred to as the "cloud" in this context. Cloud computing is a brand-new sort of computer model. Despite its obvious advantages, it also has a few drawbacks, with security being the biggest. Some firms have highly strict requirements for the protection of their data due to the specific nature of some industry. If the data is lost or deleted, the organization will suffer severe consequences. The second problem is one of reliability. Making sure that the data records are accurate and reliable is the only method to improve data transfer security and the company's reputation. A significant issue is the regulation of cloud computing. Businesses can only operate properly and healthily with effective regulation that is well-organized. Consumers that use IaaS have direct and flexible access to resources like hardware devices in the form of services, enabling them to perform computing and storage tasks. The dynamic nature of user applications and release nodes is one of its primary characteristics. Additionally, this service is a type of demand-based billing service, and users can pay to rent the service online in accordance with their specific work requirements.

In the age of big data, cloud storage systems are targeted at public users, who have higher expectations for system performance in addition to increased storage capacity. Additionally, the larger user base is forcing the storage system to boost throughput in order to swiftly respond to user demands. Three distinct benefits of cloud storage over conventional storage include:

a) *Adaptation:* This mainly applies to personal clouds. Cloud service providers will develop a cloud storage solution that fits their unique qualities in accordance with customer expectations. While private clouds offer users great storage options, they also lessen some security risks to storage services because of their secrecy.

b) *Low prices apply:* Many small and medium-sized businesses currently incur significant expenditures for data storage, and those prices will only climb as the volume of data grows. However, the introduction of cloud storage services has opened up new opportunities for these businesses. To resolve this issue and avoid the expense of building their own data center, they will need to store the data transmission to the cloud through the cloud storage service provider.

c) *Simple to manage:* This point can actually be summed up as the cost advantage. After transferring the necessary storage data to the cloud, the organization no longer needs to upgrade and maintain the system; these tasks are taken care of by the service provider, easing the enterprise's financial strain. Additionally, based on the prior strong expansion performance of cloud storage services, enterprise users can expand the storage space according to their own demands when the data of enterprise user’s surges, meeting demand. Figure 2 is a cloud computing diagram [12].

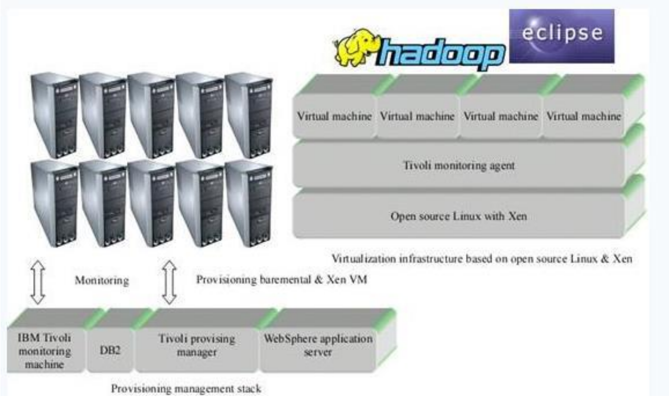
hadoop
eclipse
Virtual machine
Virtual machine
Virtual machine
Virtual machine
Tivoli monitoring agent
Open source Linux with Xen
Virtualization infrastructure based on open source Linux & Xen
Monitoring
Provisioning baremental & Xen VM
IBM Tivoli monitoring machine
DB2
Tivoli provising manager
WebSphere application server
Provisioning management stack

Fig.2. Sketch of the cloud computing architecture [12].

III. RISK FACTOR IN CLOUD ENVIRONMENT

A. Risks of Cloud Computing by Deployment type

It is helpful to evaluate the risks specific to each of the cloud deployment models in order to get ready for cloud migration and the necessary contract negotiation. The private, community, public, and hybrid cloud models are among them.

1. Personal Cloud

A single customer's distributed computing infrastructure is known as a personal cloud (as opposed to the more common multitenant environment, typified by a public cloud). A personal/private cloud can be set up by a business (which would operate its own data center and offer cloud services to its staff, suppliers, and customers) or it can be hosted by a provider. In other cases, the provider will be the owner of the hardware hosting the private cloud in their data center. The customer will have exclusive use of that particular hardware; no other customers' clouds will be hosted on the same hardware**.** Sometimes, the hardware that is physically housed inside the provider's data center belongs to the client (often referred to as a co-lo, or collocation center). For customer firms that operate in highly regulated sectors or that handle a sizable volume or degree of sensitive information, the private cloud might be a better cloud alternative because it enables much more precise customer control over security controls and overall governance. While theoretically having infinite capacity, the private cloud's capacity will naturally reach a maximum of whatever components are allocated to it, making it more expensive (in terms of the amount paid to the provider) than the public cloud model. The following dangers are faced by all private cloud providers:

a) *Employee Threats:* This covers both purposeful and unintentional dangers. The administrators of the provider continue to be out of the customer's control if a managed provider or data center is used.

b) *Natural catastrophes:* Natural disasters might nevertheless affect any deployment or service strategy.

c) *Outside Attacks:* These assaults can come in a variety of shapes, including illegal access, listening in on conversations, distributed denial of service (DDoS), and denial of service (DoS) attacks.

d) *Noncompliance with Regulations:* Even though consumers have much more control over setup and controls in private cloud architecture than they have in a public cloud, regulators will nevertheless enforce regulations.

e) *Malware*: Depending on where the illness originated, this can be regarded as an internal or external hazard. Although none of these dangers are particular to the private cloud, having more clarity and control may offer the consumer more confidence in addressing them.

2. Community Cloud

In a community cloud arrangement, resources are distributed among an affinity group and shared among them. Infrastructure can be owned and/or operated in any combination and mixture of these ways: collectively, individually, centrally, throughout the community. Each of this deployment model's advantages carries associated risks:

a) *Resiliency through Shared Ownership:* The ecosystem is more likely to survive the loss of a considerable number of nodes without harming the others since network ownership and operation are dispersed among users. Since each node serves as its own point of entry, this poses extra dangers because vulnerability in one node might allow an infiltration into the others. Of course, this makes it nearly hard to have baselines and configuration management work together (and very difficult to enforce). Decentralized ownership entails distributed administration and policy decision-making.

b) *Shared Cost:* Each community member contributes to overhead and infrastructure costs, but also to access and control costs.

c) *There is no requirement for centralized management of performance and monitoring:* Although this alleviates many administrative responsibilities, it also undermines the validity of centralized, uniform criteria for performance and security monitoring.

3. Public Cloud

This deployment strategy is the one that receives the most attention in the CCSP CBK and is most likely to benefit the biggest number of cloud customers. In the public cloud, a business provides cloud services to any entity interested in using them, including people, businesses, governments, and other organizations. The public cloud faces many of the same dangers as the private cloud, including staff threats (both intentional and unintentional), external threats, natural disasters, and more. The public cloud's resemblance to the community cloud eliminates some of them, including dispersed infrastructure, shared expenses, and a decreased requirement for administrative capability. These same advantages, meanwhile, also come with more risks associated with the public cloud. The company will lose all assurances associated with keeping an internal private cloud, including control, oversight, auditing, and enforcement.

4. Hybrid Cloud

A hybrid cloud is just two or more of the previous models together. Of course, hybrid cloud configurations come with all the dangers associated with the many models they integrate. A company thinking about using a hybrid cloud system should be aware of all the dangers mentioned in the preceding sections that apply to their specific hybrid decision.

B. Cloud Computing Risks by Service Model

1. Infrastructure as a Service (IaaS)

The customer will have the most control over their resources in the infrastructure as a service (IaaS) model, which may allay certain worries about relying on the provider or lacking understanding of the environment. Although they are typically not exclusive to that configuration, there are nonetheless hazards associated with the IaaS conception:

a) *Employee Threats:* Again, an insider (working for the provider) who is malicious or careless may have a serious negative effect on the client, in large part because they have physical access to the resources in the data centre where the client's data is kept.

b) *Outside Threats:* Malware, hacking, DoS/DDoS, man-in-the-middle assaults, and other examples are some of these.

c) *Lack of Particular Skills:* There will be a heavy strain on the customer's administrators and staff to handle both operational and security functions in IaaS because so much of the environment will be governed by the customer and all access will be via remote connections. A company that does not have enough employees that are qualified and experienced to carry out these jobs in a cloud environment is significantly increasing the risk to its operations.

2. Platform as a Service (PaaS)

In addition to the hazards present in the IaaS paradigm, the platform as a service (PaaS) model will also provide additional risks. They consist of the following:

a) *Issues with Interoperability:* The customer's software may or may not operate correctly with each new change to the environment because the OS will be managed and updated by the supplier.

b) *Continuous Backdoors:* As a result of the customer's ability to install any program (production or tested) over the infrastructure (hardware and OS) within the cloud environment, PaaS is frequently utilized for software development and development operations (DevOps) initiatives. This model is well suited to acting as a trial run for fresh applications. It can simulate the production environment by taking a structured sample of all the systems from the operational enterprise, and it can distribute the test over numerous OSs and platforms to evaluate how different platforms interact with one another. Despite all these advantages for DevOps, it's crucial to keep in mind a big danger that this sector entails: backdoors left by programmers after the release of the final product. In order to avoid having to start the program from scratch in order to discover the specific function that has to be fixed, these are utilized for effective editing and test cases. However, if they are found and used by malicious parties, backdoors can also be used as attack vectors. The zero-day exploit of tomorrow will be today's development tool.

c) *Virtualization*: Because most PaaS offerings utilize virtualized OSs, the threats and risks associated with virtualization must be considered in this model

d) *Resource Sharing:* The customer's applications and instances will occasionally run concurrently on the same hardware as those used by other customers. It is important to take into account the risk of information bleed and side-channel attacks.

3. Software as a Service (SaaS)

The software as a service (SaaS) environment still entails all the hazards inherent in the PaaS and IaaS models in addition to these extra issues:

a) *Exclusive Formats:* The provider can be gathering, keeping, and displaying data in a format that is solely theirs. This may reduce portability and result in vendor lock-in.

b) *Virtualization***:** In the SaaS scenario, where there will be even greater resource sharing and concurrent multi-tenancy, the dangers associated with virtualization are increased.

c) *Web Application Security:* The majority of SaaS products will rely on browser-based access and some sort of application programming interface (API). Web apps' potential flaws present a wide range of risks and dangers.

IV. THREATS IN CLOUD ENVIRONMENT

Although many of the risks associated with cloud computing are similar to those we encountered in traditional IT operations, they could also present more of a threat or take different forms. The risks to the private, communal, public, and hybrid cloud models will be discussed in this section. This material should only be viewed as a tool to inform the reader and prompt awareness of potential security behavior; it is by no means comprehensive or prescriptive.

Threats	Description
Malware	Data loss, device loss of control, business interruption, and other issues can all result from malicious software that has been downloaded from the Internet or uploaded to the internal network. In a SaaS setting, this is less likely because the consumer cannot install software.
Domestic Threats	These could be the consequence of employees or others with access acting maliciously or unintentionally (such as contractors and maintenance personnel).
External adversaries	The network may be targeted by outside parties for a variety of reasons, such as monetary gain, hacktivism, political objectives, perceived grievances, and so on. DoS/DDoS, data leak, legal implications, simultaneous flooding, brute force, and other effects are only a few of the many forms and manifestations of these attacks.
Man-in-the-Middle Attacks	This is the slang phrase for any attack in which the perpetrators place themselves in the path of the recipient. This can involve basic eavesdropping to gather data or a more sophisticated attack, including the attacker impersonating a participant to obtain additional access or control or altering data flow to include false or destructive information in the communication. Compared to historical deployments where all network access was restricted to internal users, a private cloud's capacity to support remote access increases the susceptibility to this type of danger.
Loss or Theft of Devices	Once more, the comfort and improved operating capability of remote access also bring with them new dangers. Particularly in a BYOD setting, the theft or loss of a user's Smartphone can result in unauthorized access to and use of the company's cloud network.
Regulatory Offenses	Nearly all IT operations are impacted by regulations, but a private cloud increases the risk that the business won't be able to maintain compliance. The likelihood of breaking any applicable laws also rises as a result of the greater opportunity and effectiveness for information dissemination.
Natural catastrophes	Natural disasters have the potential to disrupt any enterprise, and no place on earth is completely safe. They only differ

	geographically. The nature and frequency of catastrophes, such as hurricanes, floods, wildfires, tornadoes, earthquakes, volcanoes, mudslides, and so on, are determined by location and climate.
loss of policy influence	In the cloud, ownership is decentralized, therefore centralized policy promulgation and enforcement is typically not a possibility.
Loss of Control Physically	Physical security is inversely correlated with physical control. If ownership is divided among multiple users in a community cloud, this vulnerability may be amplified
inadequate audit access	Conducting audits in a dispersed setting may be difficult or impossible due to the loss of physical control.
Unreliable Administrator	The insider threat has been amplified in this way. The public cloud introduces the risk that an insider with more privileges than necessary could behave maliciously or carelessly. A rogue actor or negligent employee who poses as a network/system architect, engineer, or administrator could inflict significantly more harm than a user in the legacy environment because public cloud providers will be in charge of managing your systems and data.
Increase in Privilege	The insider threat category has been expanded in this way. When authorized users attempt to raise their level of access or permissions—whether maliciously or for practical purposes—threats are posed. (Attempts to increase privileges are not always malevolent in intent. Some users are willing to break the rules in order to improve their own productivity or to get rid of bothersome or onerous controls. Because users must deal with not just one, but at least two sets of governance—that of their own organization and that of the provider—in the cloud, the possibility of this kind of attack rise. Delays in requests to change or provide extra access or authorization may result from this, which may prompt user attempts to violate rules.

Table 1: Threats in Cloud Environment [13]

V. METHODOLOGY OF COUNTERMEASURES

The dangers to each of the cloud models covered in the previous sections are described along with some potential countermeasures in the paragraphs that follow. This material is not intended to be thorough or prescriptive; rather, it is meant to inform readers and encourage them to think about potential security action

Methods	Description
Malware	Applications and agents for anti-malware can be used on both physical host devices and virtualized instances. All users can receive specialized training on the techniques used to introduce malware into a cloud environment and how to stop it. To identify unusual activity and performance declines that might be signs of infections, network traffic and baseline configurations should be continuously monitored. It is important to include regular updates and patches, possibly even ones that automatically verify virtual machines as they are created at each startup.
Domestic Threats	The company should perform thorough background checks, resume/reference checks, and skills and knowledge assessments before recruiting new employees. The company should have the right personnel policies in place to handle the risks related to current employees. These rules could include extensive and ongoing training, required vacation and job rotation, and two-person integrity when it makes financial and practical sense. Separation of roles and least privilege are important components of sound workflow policies. Programs for active physical and electronic surveillance and monitoring may be deployed. Data should be hidden so that no one who doesn't need to work with raw data directly can see it. Monitoring of egress should be used as well (using DLP solutions).

External adversaries	Hardened physical devices, hypervisors, and virtual machines with detailed configuration and change management procedures, robust access restrictions, and maybe even outsourcing to a third party like a cloud access security broker are some examples of countermeasures (CASB). It's also critical for the business to understand how its enemies view it; this information can be used to analyze dangers, identify them, and even provide some predictive capabilities, which might lead to a much more prompt response than a purely reactive approach to handling threats. Services for threat intelligence provide this feature.
Man-in-the-Middle Attacks	Encrypting data in transit, including authentication activities, is one method of reducing the impact of these attacks. Additionally, you can impose secure session technologies.
Loss or Theft of Devices	A few countermeasures include remote wipe or remote kill switch capability for portable devices, encryption of stored data to lessen the effectiveness of theft, strict physical access controls, limited or no USB functionality (up to and including physically destroying USB ports), detailed and thorough inventory control and monitoring.
Regulatory Offenses	Hire knowledgeable, skilled workers with the appropriate skill sets. Regarding system planning and management, defer to general counsel. Activate IRM solutions. Use masking, obfuscation, and encryption as needed.
Natural catastrophes	All systems and services for the data centre, including ISPs and utilities, should have numerous redundancies, according to the cloud provider. The cloud customer can plan a disaster backup offline, with another cloud provider, or with the original cloud provider.
loss of policy influence	Strong contractual clauses that guarantee the provider is adhering to a security program that is at least as extensive and effective as what the customer would implement in an organization the customer owned and controlled should be used. Customers or a reliable third party should conduct thorough audits that are in-depth and detailed.
Legal Seizure	Legal action (whether for prosecutorial or litigatory objectives) may cause the organization's data to be lost or disclosed unexpectedly or without warning. The firm may think about adopting data encryption or data dispersion (spreading the data across various logical and physical places). This issue should be taken into account in the updated BIA, and we should think about using encryption for cloud-based data.
inadequate audit access	The customer must rely on a reliable third party if the provider won't let them audit the facility themselves. The client must insist on contractual safeguards if the provider restricts access to comprehensive third-party reports in order to shift as much of the financial responsibility for security failures to the provider as is legally feasible, including additional punitive damages.
Unreliable Administrator	The following controls are added for all privileged accounts and personnel as additional physical, logical, and administrative safeguards against internal threats: locked racks, real-time monitoring of physical access to devices, the use of video surveillance, thorough and secure logging of all administrative activities, and financial oversight of privileged personnel (where legally allowed).
Increase in Privilege	Tools and procedures for extensive access control and authentication should be used. Along with automated tools like SIEM/SIM/SEM solutions, further countermeasures include periodic examination and evaluation of all log data by knowledgeable employees.

Table 2: Methodology of Countermeasures [14-21].

VI. CONCLUSION

While cloud computing has many benefits, security issues are currently a problem. These days, clients' top worry is security. In order to fully benefit from cloud computing, the customer must assure the security of their data, infrastructure, and applications. In this work, we present a review of all possible threats and its possible countermeasures for cloud security that can protects both physical and virtual assets for organizations [22-23].

REFERENCES

[1] The NIST definition of cloud computing, available at: https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-145.pdf.

[2] D. Nister; Scalable recognition with a vocabulary tree in pattern recognition and computer vision, 2006 available at: https://ieeexplore.ieee.org/document/1641018

[3] W. Kim; Cloud computing architecture, available at: https://www.academia.edu/42414263/Cloud_computing_and_Infrastructure.

[4] S. Subashini and V. Kavitha; A survey on security issues in service delivery models of cloud computing, 2011 available at:.

[5] C.-Y. Ku and Y.S. Chiu, ―A Novel Infrastructure for Data Sanitization in Cloud Computing (Research Paper), in Diversity, Technology, and Innovation for Operational Competitiveness: Proceedings of the 2013 International Conference on Technology Innovation and Industrial Management, 2013, p. S3_25-28.

[6] N. Fotiou, A. Machas, G. C. Polyzos, and G. Xylomenos, ―Access control as a service for the Cloud,‖ J. Internet Serv. Appl., vol. 6, no. 1, pp. 1–15, 2015.

[7] S. S. Gill et al., ―Transformative effects of IoT, Blockchain and Artificial Intelligence on cloud computing: Evolution, vision, trends and open challenges,‖ Internet of Things, p. 100118, 2019.

[8] R. Buyya, J. Broberg, and A. M. Goscinski, Cloud computing: Principles and paradigms, vol. 87. John Wiley & Sons, 2010.

[9] D. Villegas et al., ―Cloud federation in a layered service model,‖ J. Comput. Syst. Sci., vol. 78, no. 5, pp. 1330–1344, 2012.

[10] D. Bermbach, ―Quality of Cloud Services: Expect the Unexpected, ‖ IEEE Internet Comput., vol. 21, no. 1, pp. 68–72, 2017.

[11] S. Basu et al., ―Cloud computing security challenges & solutions-a survey,‖ in 2018 IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC), 2018, pp. 347–356.

[12] Wang Xiaoyu, Gao Zhengming, Research and development of data security multidimensional protection system in cloud computing environment, international conference on advance in ambient computing and intelligence, 2020, School of Computer Engineering, JingchuUniversityofTechnology,Jingmen448000,China

[13] Wang Xiaoyu, Gao Zhengming, Research and development of data security multidimensional protection system in cloud computing environment, international conference on advance in ambient computing and intelligence, 2020, School of Computer Engineering, JingchuUniversityofTechnology,Jingmen448000,China

[14] Increasing Safety and Robustness in Traffic Controlling Circumstances Using WSN" **IJCRT**, Vol. 6 | Issue 1, Jan 2018, ISSN 2320-2882, pp. 16-21.

[15] A Review on various Security Issues and Challenges in VANET", **IJCRT,** Vol. 6 | Issue 1, Feb 2018, ISSN 2320-2882, pp. 396-40.

[16] Dr. Prakash Kumar, International Journal of Computer Science and Mobile Computing, Vol.6 Issue.12, December- 2017 | ISSN 2320–088X, pp. 157-163.

[17] Dr. Prakash Kumar, International Journal of Creative Research Thoughts, Volume 6, Issue 2 April 2018 | ISSN: 2320-2882,pp. 428-434.

[18] Dr. Prakash Kumar, Security Issues in Vehicular network" in **JESMT** Vol. 2 | Issue 1, 2012, ISSN 2231- 1521.

[19] "Survey on Tools & Technologies used in Semantic web and IOT" **IJCRT,** Vol. 6 | Issue 2, June 2018, ISSN2320-2882,pp. 302-306

[20] "A Novel Software development life Cycle Model for Developing Software Project", **IJCRT,** Vol. 6 | Issue 2, April 2018, ISSN 2320-2882,pp. 428-434.

[21] "Security Aspects in Social Networking Model "**IJCRT,** UGC Approved, Vol.6| Issue 1, Jan 2018, ISSN 2320-2882.

[22] "Cloud Database Services improve using load balancing Technique" in **JETIR** Vol.8| Issue 1, 2021, ISSN 2349-5162,pp.822-826

[23] Sourav Kumar Upadhyay, Dr S.C. Dutta, Dr. Prakash Kumar; Impact of the Internet Shutdown in Ranchi, Jharkhand: A Survey, 2022. Available at: http://www.jetir.org/view?paper=JETIR2207676

[24] Purushottam Kumar,Dr. Prakash Kumar; A survey on Load balancing in Cloud Computing. Available at: http://www.jetir.org/view?paper=JETIR2207664