Cyber Security Laws: With Reference to Cloud Computing Paradigm Implementation there of in Telangana Region

Authored by:
GUNDU SRINIVASA RAO M.C.A.
Ph.D. Research Scholar,
Department of Computer Science,
Dravidian University
Kuppam, A.P. (India)

Guided by:
Dr. U.PATTABHI RAMIAH
LL.M.(Gold Medalist),
Ph.D.(Law) O.U., Ph.D.(Law) SRTMU,
M.A.(Sociology),O.U,M.A.(Political Science), O.U
B.J.(Journalism)-O.U., "Visharad", "Bhushan"-
ADVOCATE -HIGH COURT OF TELANGANA

Abstract:-Cybersecurity is one of the most major issues being confronted today in this era of a technological sweep. In this technology-based cybersecurity arena what is getting more important is a due emphasis on the lifestyle of the people and their complete interdependence systems. There exists a major threat in protecting their data and it is not only limited to private individuals, but also to organizations, corporate governance areas, defense related, commercial and business organizations arenas who store a large amount of specific data and resort to some transactions online as per their routine requirements.

This threat is not only going to affect major devastations in terms of data storing and data loss but also can damage the very foundations of laid down infrastructure. There is a need for stronger legislative enactment to avoid such criminal hacking activities.

Telangana state has made out a safe cybersecurity policy assuring the end-users and the investors to feel more secure and that they are group to be well protected due to the cyber security-enhanced innovative ultra-modern updated devices, procedures and policies.

***Keywords**:- Cyber Security, Technology, Cyberspace, Software, Confidential Data, Networks.*

I. INTRODUCTION

In the recent - As per projections from NASSCOM, our country has become more susceptible to cyber-attacks. Almost all organizations including the Government and private sectors are showing intense interest in the digitalization of all their transactions. Financial, banking and educational sectors are just a few examples. India is globally recognized as a preferred destination for all their outsourcing works. India also provides shared services and technical support services.

II. DIGITAL INDIA

Recently India has started a new program called Digital India. This program focuses on service delivery with efficiency, for all the government transactions. It has an innovative inspired vision to improve the accessing facility to the educational and health-related schemes such as those that reach the common man. This has not only made an incredible growth but also won the hearts of the people across the nation. Subsequently, alongside it has also made the situation quite vulnerable, where the criminals too could exploit the opportunities for their selfish ends.

Presently there are many number of cyber attacks vehemently on Indian cyberspace, and perhaps this has too increased in these days. Some other countries too have developed an excellent reputation as stronger cyber secured mechanism oriented countries such as Israel.

The government of India is striving hard to avoid situations of complete rout and devastation like mounted cyber attacks. Now newly emerged Telangana state is emerging as a digitally connected state to assure as a secured cyberspace provider to ease the comfort and economy for safer and fearless methods of attacks. The investors can make without any doubt as well as the users can share their data, now.

III. INCREASE IN CYBER CRIME IN THE YEAR 2015

More than 95% of computational firms have the problem of threats in their cyberspace. Unfortunately, the majority of them are not considering this threat as a major problem still.

There is a growth in the cybercrime rate for the last five years. The technology has increased dramatically. In response to this, cyber crimes also increased.

While launching the Digital India program in 2015 the Prime Minister of India Sri. Modi said that the human civilization has developed the warfare systems, which he described as the bloodless war process.

He also mentioned that it would make un-recoverable damage to the cyber world. Mr. Modi also described devises safeguarding from such vulnerabilities. A few years ago thousands of attempts were made to hack MasterCard databases every day. Many other large companies have faced similar attacks. Due to many reasons, Cyber Security works are coming India's way and substantially till now no state Government has done a well paced organized effort to avoid such cyber attacks.

Today India has emerged as a sophisticated global elite power in the segment of Cyber Security providers. This has not happened overnight, but is evolving slowly.

(i). Stage - 1: Protection from Viruses: In the first level, it was focused on Virus attacks. These acts lead to develop anti-virus applications. These anti-virus applications are developed to sell as commercial goods to make every individual capable to install in their respective systems, laptops, etc so that such devices to get protection from the virus attacks. Generally, these antivirus applications have assured the IT Firms and their clients to feel that they are more safe and secured effectively.

(ii). Stage - 2: IT and Network Security: In the second stage the focus has widened to such areas as protecting from the individual systems heading to the network systems in the form of network security. Firewalls were developed to avoid unwanted malware. Network security applications are developed to enhance security at the distributed level.

(iii). Stage - 3: Cyber Space Security: In the third stage security of cyberspace is more widened since the enhanced systems also have threats from more complexed attacks and there is there a dearth need to assure the clients and the investors that they will be safe from any attacks which would lose their data, the security is improvised thoroughly.

IV. CYBER ATTACKS IN 2015-16

Cyber attack threats have become quite common and they are getting increased day-by-day as with the growing computational updations, and Computational criminals such as hackers, some government-sponsored professional people hired by North Korea and China increased, leading to more finding need to explore orientations.

Today many countries are confronting cyberspace methods and some of those countries are on the way to make their opponents to get attacked. Safeguarding from such attacks and when there is any possibility to indulge in the attack of the opponent is the strategy: such new courses are emerging and following today in the cyberspace. This philosophy has made the digital space to be seen as more complex and complicated. Financial transactions and the economy are getting a stronger threat from these activities today. Hence there is a need particularly to safeguard cyberspace in this field too, from these complexed environments, and crimes.

Digital attacks are strongly motivated for some confirmed reasons. They are technologically and strongly supported and highly supported financially. Generally, these digital attacks are made to hack on Government devices, to safeguard private organizations and sometimes private individuals due to many reasons such as to gain popularity, financial frauds and also for personal revenge. Attacks are either to damage the data stored or to spoil the online transactions. Perfect safer cyberspace should always be ready to face such attacks and protect their data and their operations from such eventualities. Two such attacks are noteworthy to mention which are: the first attack was made to stop working on a power grid which affected 225,000 Ukrainians. The second attack was made in 2016 on the Bank of Bangladesh.

The objective of the Government in any country is getting to protect more vulnerable phases today since they need to safeguard the data from the cyber-attacks in this technological era, much to the desired levels.

Fortunately today the state of Telangana is safer and assures from the unforeseen attacks and this got established as a protected environment zone, applauded by all.

V. INDIA AND THE DIGITAL SECURITY CHALLENGES

(i). The necessity of Indian National Cyber Security Architecture – In India for an appropriate cyber architecture is very lacking with has not too well defined norms and conditions which are necessary for this peninsula to protect the Indian infrastructure from such infamous digital attacks [3].This is going to erupt and show signs of a vital step back in the coming years to the Indian government, if not alerted to find newer horizons and ways.

(ii). Lack of Skilled Professionals Team –India is lacking in the highly skilled workforce to handle the cyber sphere in reference to the cyber attacks. Indian youth might be spending much of their time on mobiles and they all are not technically upgraded to have computational effective richness talents and the minimum computational knowledge. Many of them are computational illiterates much to the disgrace of our capabilities.

(iii). Deficiency of a Worldwide Centralized Initiative: In order to respond and reciprocate on this there is a need of a well established centralized agency which would communicate with the local and international bodies whenever it is required in case of digital attacks such as in case of any paramount important infrastructures like defense segments, financial transactions, and insurance sectors. There must be cooperation between different organizations to work cohesively to curb the effect of the cyber attacks and preventing it from un expected another series of attacks. They must always plan to revert any digital attack identifying the eventualities with their pre-estimated calculations.

(iv). India is lacking a Regulatory Policy: This tune around for the Digital Security many of the Indians are not aware of cyber laws and its legislations are lacking at the organizational and private individual levels. All private individuals are needed to know the full length of cyber laws and their legal framework [6] as since they generally tend to use the internet for all their personal and financial transactions in their routine life. These people must be either properly guided or mentored for their online works, or else the consequences would be hazardous and dangerous.

(v). Deficiency of common device frameworks and Internet Connectivity- All ages and groups of Indians are almost using phones today, but only a few people use technologically sophisticated mobile phones that are not appending and requisite to the occasion and choice.

Only a few people are technically upgraded and know the consequences of the cyber attacks. Many of the sophisticated mobile phones do not suit the appropriate technical standards and hence the proper security measurements would not be possible to protect their data on the phones.

VI. CYBER LAW AND RELATED LEGISLATION INTELANGANA STATE TO BE FORMULATED

The main aim of the framework related to the legislation is to send a stronger message to the cyber misusers to inform them of due consequences by the establishment of the Crash resistant legal frame work, with the help of a cohesive statutory work team.

Telangana State has the collaboration with National Academy of Legal Studies and Research (NALSAR), The Hague Security Delta, Cyber Cell, and TIPCU, etc.

With this aid and help non - Cyber Security Acts may also be dealt with such copyrights violation cases, defamation cases, etc.

Telangana Intellectual Property Crime Unit (TIPCU) is an organization established by the State Government of Telangana teamed up to curb criminal activities in cyberspace including the pirated cases.

Complaints and Grievances related to the crimes are resolved under the IT Act by a specially trained cybercrime cell (CCC). The CCC works under the direct supervision of Assistant Commissioner of Police (ACP) rank police official, along with the support of four numbers of inspectors of police. The progress of the cases is traced from time to time by the concerned officials. Some of the cyber crimes include cases such as harassing the women in cyberspace, spreading child pornography, etc. The government of Telangana has taken much serious concern and steps to curb these issues in cyberspace, are in place and are ongoing.

State Government of Telangana is too interested to establish digital forensics lab in order to analyze and investigate cybercrime while alongside on its way to help the recovery pieces of evidence and preservation of digital evidence in cyberspace. The recovery data laboratory is planned to establish to help the corrupted governance and any such mal practices.

VII. VISION OF THE CYBER SECURITY POLICY 2016

Telangana Government has a commitment to developing a place has the assurance to make it safer cyberspace in order to promote the empowerment of Telanganites to have a protected cyber environment and a safer infrastructure.

It has a noble vision almost extracting a place in our country to etch for itself:

(i).To make Telanganites to aware about the safer cyberspace techniques

(ii).To promote safe cyber practices to the people of Telangana

(iii).Avoid cybercrimes in the region of Telangana wholly

(iv).To collect information related to criminals on cyberspace by regulatory devices.

(v).Making ready for cyber security expert group to work cohesively with the Government of Telangana and also the sum to be a destination hub of IT revolution and exploration practices.

(vi). To promote cyber security products like anti-virus gadgets.

VIII. CYBER SECURITY POLICY FRAME WORKS ARE SUCH AS THESE:

Creation of Cyber Space - It is a complexed environment having communications among the netizens, software [1], and the services, highly supported by a distributed network of ICT and its related devices.

Provisioning Cyber Security - can be defined as an activity by which the information and telecommunication systems and which has have the protection from un-authenticated usage of resources or the modification or misusage of resources or even prevention of damaging the computational resources.

Ambling for Critical Information Infrastructure (CII) - can be defined as a computational resource, the destruction of such which will make a greater impact on the national security, national economy, and such type of major segments of the national importance.

On Cyber Crime - can be made a definition such as a crime by which a computer works as an object of the crime namely hacking, and phishing activity or spamming is used as a tool to do an offensive act to spread the child pornography, theft of women well being peace harassment, etc activities which are defined clearly as the crimes in the physical world such as the given here below.

(i).Digital crime: can be described starting from the basic level crimes for instance online harassment to the highly calculated attacks for instance such as financial frauds and financial crimes.

(ii). Digital terrorism: Any action of terrorism-related activity via the internet or computational resources can be defined as digital terrorism.

(iii). Digital harassment: harassing anybody in any form, for instance, usage of derogatory words on a particular individual, community or religion or even a specific region or gender using computational resources can be defined as cyber or digital harassment.

(iv).Digital extortion: either an E-Mail server or a computer machine is either hacked or even made attack by a DOS attack, asking in return to pay some money such as blackmail can be called as digital extortion.

(v). Placing offensive content: using the cyberspace for the use of keeping the offensive material or content which falls and comes under a punishable offense.

IX. CLOUD COMPUTING DEVICES GALORE

The Cloud Computing has furnished new instructions within the field of IT and IT-Enabled Services. Cloud Computing [7] is providing 3 Environments which include Software-as-Service (SaaS), Platform-as-Service (PaaS), Infrastructure-as-Service (IaaS) as per NIST in digital Cloud Environment.

Cloud itself works at the ideas of resources Virtualization and presents the provider step tool with the demand and Pay-in line with-Use model. Ultimately Cloud Computing offers the user a cheaper and at Economic rates such quotes to use the Computing Resources, for making a better, useful resource allocation control. Efficient resource allocation will keep away from both underneath utilization or overutilization of sources.

Resource allocation in a better way and scheduling in a higher manner aren't only the important things and obvious necessities to offer higher services to the consumers. However the important factors to evaluate the overall cloud computing device's overall performance are also revolutionary need of hour.

It is needed to check the present load balancing algorithms, also examine the digital system and offer a higher algorithm technical device. Although there couldn't be a high-quality load balancing our efforts are on to make a higher algorithm. May be very a good deal needed. In cloud computing, it is allowed for cloud provider vendors to proportion the computing sources on the net. With this act cloud stands as the ever-growing generation, no longer simples these days. However additionally there is need in future to getting access to the new upcoming technologies. Due to the virtualization, a danger exists for range facts facilities. Cloud Computing does not work on assigning the computing tasks to the neighborhood computers or remote servers; of sometimes possibly it assigns too many heterogeneous disbursed computer systems too.

X. CLOUD COMPUTING DEPLOYMENT MODELS:

The deployment model defines the types of access to the cloud akin to public, private, and hybrid models.

(i) *PUBLIC CLOUD MODEL*: General public could access in this model. It can be made available at a lower cost. Ex: Google, Amazon, Microsoft. These services are available with the help of internet. Advantages of this model are, it will have less costs, reliable, flexible, location independent and highly scalable processes. It has disadvantages also such as these have less security, less privacy, and less control on systems.

- Advantages: 1.Less cost, 2.Risk-free, 3.Flexible, 4. Location independence, 5.Excessive Scalability.

(ii) *PRIVATE CLOUD MODEL*: This deployment model is available for fewer people such as for private use models. It takes more cost and better security methods can be provided. This deployment model is intended within an organization. Advantages of this model are high level privacy, more control. It has disadvantages also such area restricted, inflexible, and limited scalability opportunities

- Advantages: 1.Excessive protection, 2.Excessive privacy, 3. High efficiency.
- Disadvantages: 1.Restricted area, 2.Inflexible, 3. Restricted scalability.

(iii) *HYBRID CLOUD MODEL*: Amalgamation public and also private Phased Models. Cost for this establishment is almost medium and the security it provides is moderate. Advantages of this model are scalable, flexible, cost efficient expedient and secured. It has disadvantages too which are in the area of network issues, security compliance, and infrastructural dependency.

- Advantages: 1.Scalability, 2.Price effectiveness, 3.Protection.
- Disadvantages: 1.Security Compliance, 2. Infrastructural dependency.

XI. CLOUD COMPUTING PURPOSES

(a).*SaaS (Software as a Service)*: This would offer the software for the end user as a service. SaaS makes the software available over the internet. It is controlled by the cloud services provider or the one who markets it. The real time examples of SaaS models are a).Salesforce.com b).Microsoft 365

(b).*PaaS (Platform as a Service)*: models a platform as a service. It offers browser based development environment, provides built in security web services interfaces and , it is a simple provider in order to interact with other application programs within the identical cloud computing technology platform, it would also provide web technological services to interface to connect other applications which are on other platforms. Ex: Google App Engine. Generally, there will be less administration control and these are not portable.

(c). *IaaS (Infrastructure as a Service):* provides access to basic computing resources for example computers, virtual machines, load balancers, IP addresses, and software bundles. Ex: Amazon web services.

XII. SECURITY OVER THE CLOUD

To explore and to look incisively into the possibilities of threads in the cyberspace and the field of cloud computing with some of the aspects needing attention are as below here.

(a) Security at the Infrastructure level: in this basic level it is needed to be assured that the cloud-based data centers and its computational devices such as the servers. This is the fundamental requirement as of now of security assurance phases [10].

(b) Security at the Network level: generally in the public, cloud the security restrictions would be more whenever it is being connected or making the transactions to and from the public model-based cloud computing. It must be assured to get a safer and protected cyberspace for all its transactions in the web sphere that is available as of now.

(c) Security at the Application level: and processing security level: It becomes much more important than all the applications that need to be safer and alongside distinctively also committed to protection from offensive eventualities. Cloud applications need to be avoided from all offensive happenings like hacking, usage of SQL injections, etc illicit operations. The user needs to take much more precautions to avoid such eventualities. Firewalls and security applications need to be updated and enough stronger to protect from any such mal adventures on cyber space.

(d) Security at the Data level: The major data which is doling out in the public domain is kept with trust and must be safeguarded in the cloud computational environment.

There should be a proper storage facility and all the data need to be taken back up from time to time. Improper handling of data for that matter in spheres such as unauthorized access to the data is not only unethical but also it is a punishable offense, and this can be prosecuted in the court with proper evidenced pieces [8] by convicting the un-ethical user and the cloud provider for the mishandling.

Therefore all the cloud providers must take all the security measurements to avoid the risks related to the unforeseen possibilities. They must also take care of the possible technical failures that may arise in the services to the end-user. It must be taken care of with regard to confrontations such as mentioned here below.

XIII. DATA RELATED ISSUES

The integrity of the data: When a person using a system with standalone application software it becomes very easy to use with the existing single database.

But in case of a distributed environment with as many numbers of servers and their databases connected to make a data to be portrayed it obviously becomes much more complexed and this should be done using some of the given guidelines such as following the ACID properties to assure the data integrity. Many more databases support ACID operations and they protect and safeguard the data integrity. Data that is generated by the cloud computing transactions are made to be kept within the cloud servers. Therefore making it to be put in the cloud data servers can be thought of as having the possibilities of an unauthorized access to data which may result in loss of data, damage to a part of data or the loss of whole data.

Availability of the Data: The availability of the data is a conspicuous issue. Generally, the data is kept in some server which is existing in some remote locations. When the owner of such particular data needs to have such data, it becomes harder and even difficult some times when the service provider's system gets a failure or due to some other technical failure. It should be taken care to provide that the data around this time becomes available such as availability of data to the user. It is recommended to have the multi-tier architecture, in this specific time.

Location of the Data: Generally the end-user of the cloud computing when not aware of the correct location of the data center and the location where ever their data is stored, the popular data centers have their own data centers around the world and their data center's operations are not restricted to some domains. Lack of control over physically accessing this data is some never way to make it any issue for a solution.

Privacy of the data: data privacy becomes a major issue in the cloud environment. Information or the data kept in the cloud is available across the world. Government based restrictions and their jurisdiction do not make much impact, any more in today's technological Spree.

In the league of paddling new preventive devices we are exposing the data beyond its limit which may become sometimes an un resolved issue. Cloud service providers sometimes may get convicted due to such problems, which are needed to find ways to thwart.

XIV. CYBER SPACE USER'S RESPONSIBILITIES

The consideration of the stakeholders can be visualized stated as the end-user and the cloud service providers. It should be noted with a whole candid intention that both the parties need to agree specifically and to follow the acts of the policies Government for the safer and secured environment to provide collection of dependable data.

Netizens: The people who use internet-based applications especially the people of such a state become a part of such a region are needed to follow the rules and regulations made for such cyber sphere activities. They must be aware of the possibilities of convictions and the eventualities those may arise due to their misuse of the computational resources. By installing proper applications it becomes protected from such possibilities of a good lot of un- necessary attacks.

XV. CONCLUSIONS

Since smart mobile phone usage has considerably increased in India, the people of India are getting more technology oriented [2]. IOT, AI and Cloud usage matters are on its way. Digital financial transactions have started a bit later in India to improvise. At the same time, there is a possibility of mishandling of their data; hence innovative orientations are the only solutions. Many times it is witnessed that the cyber thefts and the improper usage of computational mishandling like hacking becomes a matter of concern. There is a need to curb such activities. There is an absolute lack of useful skilled workers in India, hence provide groundwork for these lacunae. End-user and the cloud service providers also need to know about the legal framework of the cyberspace tracks that are available now. Telangana State Government has taken an initiative to make the requirements to meet the stirring waters of cyber crimes as silent as even as a noble endeavor as of now, with a slew of good measures.

ACKNOWLEDGEMENT

Inspiration and Mentor for this Paper: I express my sincere and a deep sense of gratitude to my Mentor, research scholar and a legal practitioner Dr. U. Pattabhi Ramiah who has guided me for exploring more to in the qualitative content about the Cyber Security Laws pertaining to the paradigm of cloud computing. He suggested that without delving or relying on past laurels on this subject to lay specific focus on futuristic sterling devices that can protect cyber crimes in the years to come that which can be counted upon like not the years in your life that counts, but it is the life in your years. His talent thrives and successfully transforms a person into future ready professional. Preparing for this paper with critical examination and an in-depth seriating made me to learn more about the field of Cyber Security in view of Cloud Computing Paradigm in the global context.

REFERENCES

[1] G.W. Van Blarkom, J. B. (2003). Handbook of Privacy and Privacy-Enhancing Technologies - The case of Intelligent Software Agents. Retrieved from e-Europe: ftp://ftp.cenorm.be/PUBLIC/CWAs/e-Europe/DPP/CWA15263-00-2005-Apr.pdf

[2] Prof. Ian Goldberg, D. W. (n.d.). Privacy Enhancing Technologies for the Internet. Retrieved from University of California, Berkeley:www.cs.berkeley.edu/~daw/papers/privacy -compcon97-www/privacy-html.html

[3] Brands, S. (2000). Rethinking Public Key Infrastructures and Digital Certificates: Building in Privacy.The MIT Press; ISBN 0-262-02491-8.

[4] Cavoukian, A., & Abrams, S. T. (2010). Privacy by Design: essential for organizational accountability and strong business practices. www.globalprivacy.it/Allegati_Web.

[5] The Danish Data Protection Agency. (2010). Processing of sensitive personal data in a cloud solution. Retrieved from www.datatilsynet.dk/processing-of-sensitive-personal-data/

[6] ENISA. (2009, Nov.). Cloud computing info. assurance framework. Retrieved from ENISA: www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-information-assuranceframework

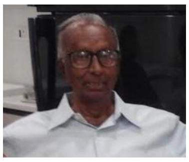
[7] Bertion, E., Paci, F., & Ferrini, R. (2009). Privacy-Preserving Digital Identity Management for Cloud Computing. IEEE Computer Society Data Engineering Bulletin, pp. 1-4, March 2009.

[8] Biggs & Vidalis (2009). Cloud Computing: The Impact on Digital Forensic Investigations. In Proceedings of the 7th International Conference for Internet Technology and Secured Transactions (ICITST'09), London, UK, November, 2009, pp. 1-6,

[9] Blaze, M., Kannan, S., Lee I., Sokolsky, O., Smith, J. M., Keromytis, A.D., & Lee, W. (2009). Dynamic Trust Managmnt. IEEE Computer, Vol 42, No 2, pp. 44-52, 2009.

[10] Bruening, P.J. & Treacy, B.C. (2009). Cloud Computing: Privacy, Security Challenges. Bureau of National Aff, 2009.

Mentor's Profile:



Dr. U.Pattabhi Ramiah, is leading Advocate and a Legal Consultant in the High Courte of Telangana, Hyderabad. He has done his M.A.(Sociology) , M.A.(Political Science), Bachelor of Journalism from Osmania University. He is the recipient of two Gold Medals in his LL.M. He has done his Ph.D in Law from Osmania University-Hyderabad, and Ph.D in Law from SRTMU from Nanded, Maharashtra. He has completed successfully his "Visharad" and "Bhushan" from Hyderabad Hindi Prachar Sabha. Guide Professor Mr. Vector Rosenblum, Northwestern University-Chicago-USA, Guide Professor Mr. Avatar Singh –Lucknow University-UP(India), Guide Professor Mr. S.P. Sathe – Pune University. He has Diploma in Public Admin Roosevelt University, Chicago-USA. He is the Former Legal Advisor for Zuari Industries Ltd-Cuddapah, APSFC-Waranga, NRI Collaboration Units (USA). He is presently working as the Advocate in the High Court of Telangana. He is the author of 12 Law books on Arbitration Conciliation, Negotiation and Mediation. He is the former Professor & HOD Law Department at ICFAI. He is the former Consulting Editor of ADR's International LAW Journal.

Author's Profile:

Mr.G.Srinivasa Rao pursued Bachelor of Science from Osmania University in 2006 and Master of Computer Applications from Osmania University in year 2013. He has submitted his Ph.D. Thesis, in the Department of Computer Sciences, Dravidian University, and awaiting for VIVA VOCE Examination. Presently working as Senior Software Trainer in Key soft Computer Education, Hyderabad. He is a member of Internet Society Global Member, also the Member of International Association of Engineers, Associate Reviewer & Member of the International Board of Reviewers International Journal of Community Development and Management Studies (IJCDMS) of INFORMING SCIENCE INSTITUTE. His main research work focuses on Load balancing, Cloud computing. His Research Interests also includes Mobile Cloud Computing, Data Mining, Big Data, Artificial Intelligence and Internet of things. His publication record as follows,published paper in relevance to the current research in Web of Science -1 Paper, and published papers in UGC Approved Journals -3, published papers in IEEE Conferences in relevance to other topic-2, Published papers in relevance to other topic- 1, and attended 14 Conferences.