International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-9 Issue-1, May 2020

Assessment of Different Security Mechanisms and Methods to Protect Data in the Cloud Computing Enviornment

Manu Raj Moudgil, Anil Kumar Lamba, Priya Gupta

Abstract:Cloud Computing has a several advantages, but it also carries additional issues like security, application security, virtualization security, authentication, access control and identity management. This paper is focusing on the current research relating on the cloud computing. This paper visualizes and deals on the various areas of security parameters in the cloud computing which includes Risk Management, Framework, Compliance, Interoperability, Lifecycle Management, Internet access Security, Data Centre Operations, Business Continuity, Incident Response, Key Management and Encryption, Access Management and identity, Dynamic access Security and Static Access Security and a lot more. In this paper we use various assessments and classification results to clear the similarities, also to exploring the various differences in the architectural methods of the cloud computing and further to determine the arears demanding with research. This paper provides findings and the assessments which can help the researcher to analysing the finest scenario for designing a well secured environment of cloud computing.

Keywords: Secret Key, Service Provider, Ticket, Trusted Service, Encryption.

I. INTRODUCTION:

The main problem in the network computing and distributed systems is Security. In the environment of distributed computing different servers spreading various services which are distributed among the various places that squash the efficiency of work. Although the technologies of distributed computing are developing so fast but still it is lacking in the safety and information security. Just recent, a new fashion draws the attention of people's, with which the users from the multiple and diverse environments will use distributed computing more competently, just as the use of electric power. That's why the area of cloud computing has idol for meeting the demand. Generally, the world wide web or internet is a collection of various clouds and cloud computing merely meaning is internet computing.

Manuscript received on April 02, 2020.
Revised Manuscript received on April 15, 2020.
Manuscript published on May 30, 2020.
* Correspondence Author
Dr.Manu Raj Moudgil, Professor CGC, Technical Campus,Jhanjeri manu.moudgil@gmail.com
Dr.Anil Kumar Lamba, Professor, CGC, Technical Campus,Jhanjeri anil.lambain@gmail.com
Er.Priya Gupta, Assistant Professor, ACET, Barnala angel.priyagupta@gmail.com

Thus, cloud computing word has emerging as model to enabling a convenient on network demand access for sharing a pool resources of configurable computing, which can be quickly released and provisioned with the service provider and minimum management effort.

At any time and from anywhere without bothering about physical and technical management or issues of maintenance of original resources, cloud computing make consumer to access online resources with the help of internet. Resources of cloud computing are also measurable as well as dynamic. Cloud computing is totally different from grid and utility computing as it is independent computing. The main example of cloud computing is google app, which enables to access the services through browser and can be attached on millions of machines via internet. All across the world at any time and from anywhere the resources are accessible using internet from the cloud. It is cheaper as compare to other models of computing. The maintenance involved zero cost since the availability of services is the responsibility of service provider. The clients are free from management as well as maintenance issues of resource machine. Because of this quality, cloud computing is called as Information Technology on demand and utility commuting. Scalability is the main feature of cloud computing has attained with the virtualizations of servers.

In this latest generation of online-based computing usually uses secured data centres and the remote servers which are protected extremely for the storage of management and data, so as the organizations needs not to pay or to look their inner IT network or solutions. After the formation of the cloud, cloud computing deployment changes the requirements with the references and for that purpose it can be used. Companies which provides cloud uses abilities of self-service of computing with virtualization technology for computing the resources through the network infrastructure. Further in cloud computing environments, deployed virtual machines of various types as infrastructure with the common physical server.

Generally, cloud environment uses three major types of services which includes infrastructure as service, Platform as service and Software as service. The model of cloud has various dimensions that create more difficulty in the problem of security. The model of cloud has two characteristics: Multi tenancy that results in the virtualization boundaries with various services hosted of various tenants, thus it is the need to harden those boundaries by the newest category controls of security and elasticity that requires secure placement service strategies and secure migration services.

In the recent days the mechanisms of security are available for the single cloud owner and for the single user who uses that cloud, in future if cloud moving towards the multi-owner security environment then it will become a very hard problem.

To overcome this problem, we illustrate the various findings and assessment which is carried out by various academician's ad researchers.

II. COMPARISIONS OF VARIOUS EXISTING METHODS:

Mahbub et al [1], in year 2011 presented a mechanism of giving security and trust in SAAS. As per his views the data holder will control the user registration, control data as well as the outsource data accessed. A trust ticket is issued by data holder for the registered user and he also keeps the record of every registered user. The trust ID, capability list to the CSP's and users public key are sent by data holder. Hence, when the registered user submits his request for the cloud service provider, the CPS will identify whether the user is valid or not. Algorithmic protocol is devised for the deployment of data holder to generate trust ticket. This ticket is an idea of trust of a registered user and control of data holder over the data. In this process the data is encrypted by the data holder with KO (secret key) and forwarding those data to cloud service provider (CSP). AT the end of user's registration K0 is shared with user by the data holder. At this time of user's registration, the trust key is issued and distributed by data holder.

In this approach the capability list of the user who is registered will be saved via CSP's as well as by the owner of the data, that can be used for recognising the invalid users, if registered users have submitted different rights of authority. In the Trust Ticket deployment algorithmic protocol, three-way verifications of listed user and also three-way encryptions is established of the data holders. In this data holder can change the access rights of the user and expiration of trust ticket and also updating the data with changes of KO (secret key) with the users. Except a data holder not done any changes. The user who is registered using the KO and trust ticket for data holder's service data from that CSP. They expected, the user registered not share the KO with CSP. Although, they not created an approach or mechanism to encounter such malicious activity of user sharing the KO with CSP.

The 14th international conference on computer and information was held in Dec 2011.[4] It was based on the presentation that explored similar areas. According Ashish Bhardwaj unlike the traditional solution in which physical control, IT service are now going towards cloud. The data management and service might not be totally reliable as the cloud computing goes towards database and the application software to data centres largely. Although, the cloud computing has a lot of advantages, yet privacy and security issues become to be strong barrier for user's acceptance of cloud service and cloud system. To achieve these goals their presentation, propose the idea of deployment of more security strategies in cloud environment, and should also to adjust the new relationship between providers and users by modifying the privacy acts. While designing the service of cloud the privacy should be considered. At the later stage it is not suggested to try to insert security in the design process.

There is probability of customers hold multiple accounts with service providers so they suggested the importance of identity management like google, Ebay etc. To Identify the entities in this scenario there is need to apply intense precautions. In their presentation they discussed that DIMAND (Dynamic mapping association N discovery system) is solution of an identity management for heterogeneous network environment on large scale and it is based on overlay infrastructure of an innovative DHT (Distribute hash table), which unites the routing capability of security profits of IDP (individual identity providers) and DHT networks. In his views with the coming time the problem of identity management will become more difficult and it will have to deal with software components, interconnected device, machines and also with the management of user identities. According to them architectural framework of cloud computing is the security domains that are observed in clouds.

Ling Li Lin Xu Jing Li Changchun Zhang [8] , in today's scenario mostly all the service providers usually thinks to increase the income and this can be done by improving the audit mechanism in the security because internal audits have cost and also by the use of internal team auditing, user can get internal process and behaviour of the service providers. By this process the operating structure of providers will uncovered with the results of audits. In addition to the audit internally, service providers not accept the external audits as auditing is only supporting the static data. That's why DPDP (dynamic verifiable data possession) is introduced by these people, with that the result correctness of the audits will guaranteed strictly.

In the opinion of Ling Li Lin Xu Jing, Li Changchun Zhang, for increasing the service usage of the cloud, two basics are very important. Firstly, the scalability and the availability of space of large storage to all the end users which can use that cloud environment. On the basis of these important basics they have built a platform which is based on the software named Eucalyptus which is open source in the research. That is commonly used in the campus to store convenient supply. They launched one storage cloud architecture service that was the combination of entity users, TPA and service providers. They give a basics for bringing TPA approach with sharing of files system and analysing the system reliability. One important thing is that, it is usually tested only with large storage.

In the view of Joel Ahmed M.Mondol et al in 2011[5], In the security of cloud computing, research strategy with the help of computing with the reconfigurable has explained. To keeping the data secure while allowing the trust computing, they have discussed in their presentation. They explained and discuss the solution which have hardware solutions in all possible ways, which can be used to increasing trust in the cloud computing with providing the data control to the data owner.

Further if physically hardware recognised with the particular user, issues of the secrecy is reduced greatly and also increases the built-in security measures. The devices FPGA are separated from cloud environment and their hardware is related with particular user. The devices like FPGA permits the identity ownership which is not generate-able by any of the clients.

The basic idea behind that security to provide the participation of client directly and acceptance for ensuring the security and also, they are not only depending on security that is provided by the CSV (Cloud service vendors). Generally, the FPGA mechanisms are placed on the client end of computation,

it secures all the malicious clouds internally from tampering the data with IAAS and PAAS layers.

These layers are invisible to all the operators as well as CSV. But their presence with the execution only be agree with both the CSV and CSU. The Hardware of FPGA is essentially tied with the Trust tools which are based on FPGA trust and problems which are related to virtualizations is easily removed. Various solutions which are mentioned like Verifiable attestation, User enabled security groups, Platform of Trusted cloud and data security. These four solutions are applied on the four distinct areas that includes User Enabled Collaboration, Trusted Platform, Finally Data Security, Mechanism using Security Groups, CSV (Cloud Service Vendor) and Cloud Service User attestation. Further, the solutions either can be applied individually on the basis of the individual requirement of cloud user or in the collective way as security suite on cloud. But it must ensure that the client must enables the security and ownership of data.

According to M. Mohamed et al [9] on the basus of Sherif El-etriby had estimated 8 latest techniques of the encryption whose names are RC6, AES, Blow fish,3DES, MARS, Blow fish and RC4 along the platforms which are independent like environment of cloud computing Amazon EC2 and Desktop Computer. By using the testing in the random way these algorithms are testing with the help of Statistical testing and NIST in the environment of cloud computing. The evaluated results using the PRNG (Pseudo Random Number Generator), for examining very useful analysis, way and the technique to all the latest techniques of encryption.

JCE (Java Cryptography extensions) are used for the implementation. With the use of EC 2 Amazon, the results of various latest techniques of encryption which are AES, DES, Blow fish and RC6 were improved as compared with the other methods of encryption. With have the old techniques more P value but they are much safe.

On the basis of their innovations they recommend that DES and blow fish methods are suitable for the time and for EC2 Amazon, Encryption AES method is appropriate.

Same type of the work was proposed by Manish Mundra et al [12], Kanika Lakhani, Uma Somani in the paper, to resolve the problems in the security by the use of cloud computing. Manish Mundra with his team members has proposed a RSA algorithm with digital signatures. Hashing algorithm is used to compress the document and the data in the technique of digital signature. The term know as message digest are come from this with the combination of few lines. By the use of message digest encryption along with private sender key, digital signatures are generated.

For the implementation of this following steps are used:

1. In the document to receive the message digest, Hashing algorithm is used.
2. Message digest which is generated had encrypted by private key of sender.
3. Next, public key from receiver side is used to encrypt the digital signature and then it will decrypt by the receiver side from cipher to the plain text by using the private key which is verified by the public key of sender. It is mainly used for financial transactions for the detection of tampering and forgery of the data

Canh Ngo,Peter Membrey et al [13] In the year 2011, ordered a research on cloud computing in the framework of the security and the services of infrastructure used on demand that came to the aims of providing the infrastructure security for the regular identity management, security context management, trust establishment and access control.

In today's world mostly all types of cloud services those are commercial generally constructed and prepared by the single customer and the single provider by simple trust model and security. Further new models of the architecture have to created, if we using the heterogeneous multi-provider environment. These types of representations provide support to the newest techniques for creating the issues of the security in environment of multi-provider virtualized cloud and also it provides trust relations and the access control along with the different actors of cloud. For the demand services, he designed infrastructure of security that have the identity management, common security service, trust management, SLA Management and authentication management

In the association with clouds, the providers of the cloud must have to provide the services to the customers but it is very difficult for the providers to offer the multitenant services environment for the implementation of the various policies of the security.

As per the reference model of Canh Ngo's security, the service components of dynamic access control are authorization service, identity management, CSSI gateway and DACS management services and the trust is formed by using fundamental hardware like BIOS, after that Operating system and after that the platform virtualization that hosting different DACI and services of virtualization. In the GEYSERS project, DACI implementation is done. Further TPM research includes the implementation of the bootstrapping protocol.

Zhidong Shen, Qiang Tong in 2010, discussed in the second international conference on the signal processing systems [14] for building an environment of computing which is trusted based for the cloud computing. Keeping in my he states that, in the cloud computing environment root is not clearly defined and for the cloud computing the protection and creation certificates are not secure. As on the internet a lot of hackers and threats on the security and we have a lot of work to do for the protection of our information and the data, also in various approaches innovations and researchers provides supports on the creation of the TC (trusted computing systems). Which are embedded along the mechanism of data security in their core modules and have not implementing using add on applications. TCP (Trusted Computing Platform) works on the mixture of hardware and software. Usually manufactures adding few latest hardware with each computer for providing the trusted functions. Then the enabled TC application and hardware mediates with the special operating system of TC. Generally, TCP provides the two most important services that are encryption and authentication boot, which were designed to work with each other.

In this the service, authentication boot monitors that which OS is booted from the computer, it informs other applications about the running operating system. This is done with adding a audit log with the hardware to keep record the booting. During the booting process the Hardware of TC calculates the code by cryptographic hash which is in BBOT ROM, then in the tamper resistant, it writes a log. Before proceeding further to next block,

it computes the next block hash and attaches it to the log of tamper resistant end. In this process when each chunk is added to log, the next hash will load. This procedure worked until the whole operating system is loaded or booted, with which the resistant log records it that which connection is exactly established and what version of operating system running. The integration of various hardware modules along the cloud computing environment is very hard and challenging work which needs a lot of research.

III. ANALYSIS BASED ON DIFFERENT FINDINGS:

Table 1 shows the various mechanisms on the basis of their research and these are generally used to provide the security in the cloud computing network to search the optimum solution to the dynamic security and trusted computing etc. The table also shows the area and the strength of every research and classifies areas which can be improved in the future.

Table 1: Assessment of various Mechanisms on basis of their discoveries

SNo	Year	Name of Researcher	Proposed Mechanism and Algorithm	Strength of the Method or advantages	Problems with method or disadvantages
I	2011	Mahbub et.al.,[1]	Trust ticket deployment by algorithmic protocol	Triple verifications	Data holder have to do hard work for providing the security even after data is on cloud
II	2013	D.Ranjith et.al.,[2]	Model Cloud Secaas	Service oriented method proposed that operated on Interoperability, scalability in loosely coupled system, and enhances the abstraction	In this approach services of identity focuses two only, that not sufficient with growth of scalability
III	2013	Vishal Paranjape et.al.,[3]	Authentication Algorithm by One-time mobile password	Using time-based one-time password OTP with in a particular time frame	Security techniques and standard privacy is absent
IV	2013	Umer Khalid et.al.,[6]	Authorization and Authentication Protocol	Providing authentication access and communication with authorization in the cloud by using protocol & also assign privileges	Comprises data leakage, identity theft and it is integrated by existing system of identity management
V	2013	Iehab ALRassan et.al.,[7]	Fingerprint mechanism for Authentication	It increases the level of performance by enhancing the security in mobile	In authorization, the security level is reduced
VI	2013	JunHu et.al.,[10]	MAC Mechanism	It providing essential management and technical strategies, Data security by access control approach-controlled fetching of the data with only authorized users	Key issues related to security protocol
VII	2014	Nitin Nagar &Pradeep K. Jatavet .al.,[11]	Authentication Mechanism (LDAP)	It Providing secure frame-work by protecting the data of users	It is not focused on the different or other tools of cloud computing

VIII	2014	Younis A.Younis et.al.,[15]	NACM (Novel access control model)	Dynamic access requirements, it is very easy in handling and also it is much better than RBAC and MAC	It has vast space complexity and also take long time to perform
IX	2014	Ahmad Almulhem et.al.,[16]	SGAS (Simple graphical authentication system)	Provides MFA in Friendly system. It combines passwords with text based and combines graph.	Authorization progress is minimal level
X	2015	Primoz cigoj et.al.,[17]	Single sign on (SSO) approach	Strong secure authentication and in cloud it provides unified access point of management	It works only to remove small vulnerability. It also needs secure, flexible interface control of privacy and user data. It is not focused in development of technology
XI	2015	R.Tamilarasi et.al.,[18]	Data and image mechanism (DIM)	It is used for partitioning method as it provides uses three tier data security for authentication, also prevents CSA, Data leakage	It is not valid for all the types of the data as this mechanism works only on suitable data
XII	2016	JyothikaChhetizaet.al.,[19]	Multi factor authentication (MFA)	It providing the verification and some additional security layers	It is some expensive, complex for users and its mechanism is different between the vendors
XIII	2016	Varsha&D. Mali et.al.,[20]	RBDAC Cryptographic trust mechanism	To determine the security of the user as individual	Done trust evaluation for the decision making in dynamic approach
XIV	2016	PunamV.Maitri & ArunaVerma Et.al.,[21]	Steganography LSB approach combines with RC6, AES, BRA and Blowfish algorithm	Data integrity, key information security, confidentiality, authentication, low delay considered. It accomplishes top level security as it uses hybridization by the algorithms of public-key cryptography	It not provides high level security. Also, the algorithm needs 10 to 12 percent less time as compared with the blowfish algorithm
XV	2017	Malik Irkain et.al.,[22]	CC (Comprehensive classification)	It verifies the location of data and the assumptions of the behaviour of CSP	Land-mark based methods are addressed only
XVII	2017	Noelle Rakotondravony et.al.,[23]	VMI (Virtual machine introspection) Mechanism	Invention of the target and It providing the report of statistical analysis	Briefings the basic issues and also lack in solutions
XIII	2017	Rongzhi wang et.al.,[24]	DSTB (Data Secure Storage based on Tornado Codes)	It provides the solution to the problems relating to data tampering	It caries issues of data security detection and the retrieval in availability of data

XIX	2018	Mylara Reddy Chinnaiah et.al.,[25]	Fault Tolerant Technique Frequency of Configuration interactions) (IFrFT) Characteristics & Frequency if interactions	It accomplishes fault tolerance and reliability of the software in the cost-efficient way.	In this, percentage of the successful are usually low and about 25 and 40 percent
XX	2018	Ahmed Nour Moussa et.al.,[26]	CFaaS Model	Providers and consumers independently collect and verifies the equality of analysis uswally resolves all collected results	Appropriate forensic analysis not available for the retrieving directly forensic data
XXI	2018	J.Mahalakshmi and K.Kuppusamy [27]	SAAS (Security-As-A-Service) for Cloud Computing files	Model is developed which encrypts the sensitive data & also works properly with cryptanalytic attacks	Limited key size and only verification of limited parameters

IV. CONCLUSION:

In this paper we explained various methods of the cloud computing with their data security concepts and also the different mechanisms of security which are mainly used for data protection by the academicians and researchers throughout the world. This paper illustrates cloud components and cloud concepts such as platform independence, reliability, low cost, scalability and flexibility. The paper includes the algorithms and techniques which are used by the researchers with their advantages and disadvantages. Based on that, assessment is carried out and we achieve, that the security is not complete in the multi-provider environment of cloud. To accomplish and enhance the security, supervision of TPM must require for security trust work. According to various methods which are prescribed that the control of dynamic access is achieved with help of the DACI approach. It is very much clear that this approach gives the excellent results in ways of dynamic access control with under the environment of multi-provider with comparisons to the other approaches or mechanisms. In the future score we recommend that proposed algorithm strength must be on the basis of secured next block implementation and also joins the log of tamper-resistant. Each time code added to log of next chunk which have to load. The process remains continue till the entire operating system booted and which time tamper log have the record that establish same of the version, which is running the operating system. The integration of various modules of the hardware with the cloud computing environment is very challenging task and also needs deep and additional research that can be done in future.

REFERENCES

1. Mahbub Ahmed, Yang Xiang,Trust Ticket Deployment: A Notion of a Data Owner's Trust in Cloud Computing, IEEE 2011.
2. D.Ranjith,.Srinivasan," Identity Security Using Authentication and Authorization in Cloud Computing"in International Journal of Computer & Organization Trends,Vol.3,Issue 4,May 2013,ISSN:2249-2593
3. Vishal paranjape,Vimmi pandey,"An Improved Authentication Technique with OTP in Cloud Computing",in International Journal of Scientific Research in Computer Science and Engineering,Vol.1,Issue 3,June 2013,E-ISSn:2320-7639.
4. Aashish Bharadwaj, Vikas Kumar, Cloud Security Assessment and Identity Management, ICCIT 2011 22-24 2011.
5. Joel Ahmed, M.Mondol Cloud security solutions using FGPA IEEE 2011
6. Umer Khalid,Misbah Irum,Muhammad Awais Shibli,"Cloud based Secure and Privacy Enhanced Authentication and Authorization Protocol",in Elsevier on ScienceDirect,Vol.22,2013,DOI:10.1016/j.procs.2013.09.149,pp:680-688.
7. Iehab AL Rassan,Hanan Al Shaher,"Secure Mobile Cloud Computing using Biometric Authentication", in IEEE explore on Academy and Industry Research Collaboration Center(AIRCC),Vol.5,Issue 6,pp:41
8. Ling Li Lin Xu Jing Li Changchun Zhang, Study on the Third-partyAudit in Cloud Storage Service, International Conference on Cloud and Service Computing, 2011.
9. Sherif El-etriby, Eman, M. Mohamed, Modern Encryption Techniques for Cloud Computing Randomness and Performance Testing.
10. Jun Hu,Lei chen,Yunhua wang,Shi-hong chen,"Data Security Access Control Model of Cloud Computing", in IEEE explores International Conference on Computer Sciences and Applications,2013,DOI:10.1109/CSA.2013.15.
11. Nitin nagar,Pradeep K.Jatav,"A Secure Authenticate Framework for Cloud Computing Environment",in GoogleScholar on International Journal of Advanced Computer Research(IJACR),Vol.4,No.14,2014,pp:266-271.
12. Uma Somani, Kanika Lakhani, Manish Mundra, Implementing digital signature with RSA algorithm to enhance the data security of cloud in cloud computing,IEEE 2011.
13. Canh Ngo,Peter Membrey, Security Framework for Virtualized Infrastructure Services Provisioned On-demand 2011.
14. Zhidong Shen, Qiang Tong, The Security of Cloud Computing System enabled by Trusted Computing Technology IEEE 2010.
15. Younis A.Younis,Kashif kifayat,Madjd merabti,"An Access Control Model for Cloud Computing",in Elsevier,Vol.19,Issue 1,Feb 2014.
16. Ahmed Almulhem,"A Graphical Password Authentication System",in IEEE explore on Researchgate, Apr 2011.
17. Primoz Cigoj,Borka Jerman Blazic,Tomaz Klobucar,"An Authentication and Authorization Solution for a Multiplatform Cloud Environment",in Researchgate on Information Security Journal A Global Perspective,Aug 2015, DOI:10.1080/19393555.2015.1078424.
18. Tamilarasi R,Prabhu S,Swarnalatha P,"An Approach for Data and Image Security in Public Cloud using Segmentation and Authentication(CSA) Protocol Suite",in MAGNT Research Report,Vol.3(8),pp:133-141,2015,DOI:dx.doi.org/14.9831/1444-8939.2015/3-8/MRR.05.
19. Jyothikachhetiza, Nagendrakumar,"Emerging security issues and Authentication Mechanism in cloud environment with focus on Multifactor Authentication",in IJARCSSE International Journal of Advanced Research in Computer Science and Software Engineering,Vol .6,Issue 5,May 2016,ISSN:2277 128X.

20. VarshaD.Mali,Prof.Pramod Patil,"Authentication and Access Control for Cloud Computing using RBDAC Mechanism", in International Journal of Innovative Research in Computer and Communicationngineering,vol.4, Issue11,Nov2016,DOI:10.15680/IJIRCCE.2016.
21. Punam V.Maitri ,Aruna verma ,"Secure File Storage in Cloud Computing using Hybrid Cryptography Algorithm",in IEEE explore on WiSNET Conference, Sep 2013,DOI:10.1109/WiSPNET.2016.7566416.
22. Malik Irain,Jacques Jorda,Zoubir Mammeri,"Landmark-based data location verification in the Cloud :Review of approaches and Challenges",in Springer on Journal of Cloud Computing,Dec 2017.
23. Noelle Rakotondravony,Hans P.Reiser," Visualizing and Controlling VMI-Based Malware Analysis in IaaS Cloud",in IEEE explore on 35th Symposium on Reliable Distrbuted Systems,2017,DOI:10.1109/SRDS.2016.33.
24. Rongzhi Wang ,"Research on data security Technology based on Cloud Storage", in Elsevier on Procedia Engineering,Vol.174,2017,DOI:10.1016/j.proeng.2017.01.286,pp:1340-1355.
25. Mylara Reddy , ,Nalini Niranjan,"Fault Tolerant Software Systems using Software Configurations for Cloud Computing",in Springer on Journal of Cloud Computing :Advances Systems and Applications ,2018,DOI:10.1186/s13677-018-0104-9.
26. Ahmed Nour Moussa,Norafida ithnin,Anazida zainal,"CFaaS:bilaterally Agreed Evidence Collection",in Springer on Journal of Cloud Computing Advances,Systems and Applications,Jan 2018,DOI:https://doi.org/10.1186.
27. J.Mahalakshmi and K.Kuppusamy, "Security-As-A-Service for files in Cloud Computing-A Novel application Model", IEEE Digital Xplore, DOI: 10.1109/ISCO.2016.7726889, November 2016, pp: 1-5, IEEE.

AUTHORS PROFILE

Dr.Manu Raj Moudgil, is working as a Professor in the department of Computer Science & Engineering at Chandigarh Group of Colleges, Technical Campus, Jhanjeri,Mohali. (Punjab).He is having rich experience of more than 15 years in teaching of graduate and post graduate classes of Engineering students, also currently guiding and guided many M.Tech thesis and Phd Students for the research work. He has more than 50 quality research publications in International Journals/Conferences and his area of research is Natural Language Processing, Machine translation systems, High level Languages and Computer Networks. Beyond this he has got many awards like Teacher of the Year for the session 2008-09 and 2010-11 for the Excellency in Teaching. He is written a book OOPS paradigm using C++ and some in process He is also awarded excellent research paper many times in the international conferences, recent one in Melbourne, Australia in 2018.

Dr.Anil Kumar Lamba, is working as a Professor & Head in the department of Computer Science & Engineering at Chandigarh Group of Coll eges, Technical Campus, Jhanjeri, Mohali(Punjab). He is having rich experience of more than 22 years in teaching of graduate and post graduate classes of Engineering students, also currently guiding and guided many M.Tech thesis and PHD Students for the research work. He has more than 20 quality research publications in International Journals/Conferences and his area of research is Security in mobile adhoc networks, High level Languages. He had written international book on load distribution in peer to peer networks and some more in progress.

Er.Priya Gupta, is working as Assistant Professor in the department of Computer science and engineering at Aryabhatta Group of Institutions, Barnala (Punjab).She is having an experience of three years in teaching of graduate and post graduate classes of engineering students. She has two quality research publications in international journal/conference and her area of research is Cloud computing and big data analytics. Beyond this she got appreciation for best efforts in Teaching. She is written a book on fundamentals of information and technology, C++ and some in process. She is also awarded excellent research paper in the International conference in 2019.