International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-8 Issue-6, March 2020

CCEODSP-Cloud Computing Environment Observation for Data Security and Privacy

Ramalingam Sugumar, L. Leelavathy

Abstract: ***Today's world, the cloud computing concepts has developed rapidly in both the private and public area, it is mainly provide the basic services and resources that are open to all kinds of end users on a particular platform through internet on a rented basis have the ability to extend up or down their service necessities or needs. This cloud computing model has numerous benefits including elasticity, scalability, efficiency, flexibility, etc. activities of a business organization. It bids a ground-breaking business concept for organizations to accept information technology enabled services without advance investment. Cloud computing model enables convenient, on-request network accessibility to a shared pool of IT computing resources like servers, services, storage networks, and applications. In this computing model can be speedily provisioned and released with negligible management exertion or service provider interaction. Quick variation of cloud computing had resulted in increasing strictness of privacy and security concerns as well as permissible challenges. In this learning includes various cloud computing issues that weakens of security and privacy of users data, as well as presents on threat that impacts data residing in the cloud and also added with this, a secure cloud computing open issues are noted in paper***

Keywords: Cloud Computing, elasticity, scalability, storage, Security.

I. INTRODUCTION

In this modern world, the IT and mobile communication technology are diligently integrated and develop rapidly. The software and hardware of smart devices upgrade and evaluate continuously. These have promoted the development of Internet, mobile Internet, [1] cloud computing, big data and Internet of things. At the same time, a variety of new service models improve the quality of living greatly, for instance, e-services represented by Amazon, Flipkart, Google, etc. [2] Cloud computing is an Internet hosted Virtual computing using web Interface [NIST definition] .The National Institute of Standards and Technology definition [3] Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. The title comes from the use of a cloud shaped symbol [4] as an abstraction for the complex infrastructure it contains in the given diagram.

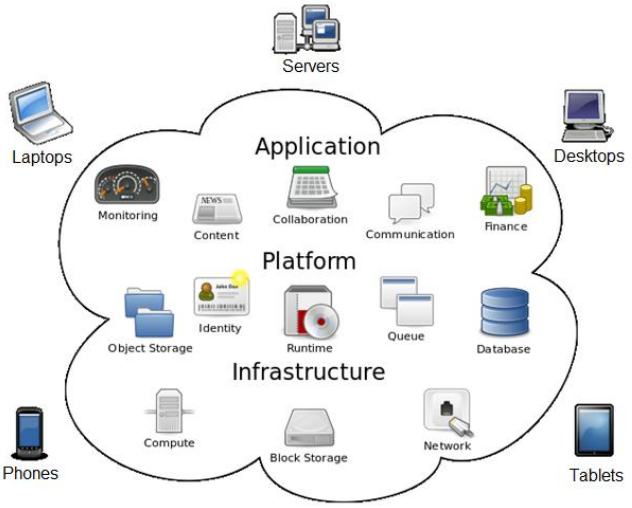

Fig.1: Cloud Computing

Cloud computing is a way to increase the capacity or add capabilities dynamically without investing in new infrastructure, training new personnel, or licensing new software. In the last few years, cloud computing [5] received considerable attention, as a promising approach for delivering Information and Communication Technologies services. With the wild development of processing, technologies, storage, the sensation of the Internet, and computing resources cheaper, more powerful. This technological trend has enabled the realization of a new computing model called cloud computing. From the past few years, the cloud computing has made a tremendous impact on the Information Technology industry, where large companies such as Google, IBM, Amazon and Microsoft struggle to provide more powerful, reliable and cost efficient cloud platforms, and business enterprises seek to find new paradigm in their business models.

1.2 Cloud Computing Models

Cloud computing comes in basic three forms: public clouds, private clouds, and hybrids clouds. Virtual private clouds and Community clouds are few modifications of the basic clouds. Depending on the type of data public, private, and hybrid clouds, can be analyzed in terms of security and management requirement as depicted in [6] figure 2. The Cloud Computing model has three main deployment models [7] which are:

Manuscript received on February 10, 2020.
Revised Manuscript received on February 20, 2020.
Manuscript published on March 30, 2020.
* Correspondence Author
Dr. R. Sugumar, Professor & Director, Department of Computer Science, ChristhuRaj College, Trichy, Tamil Nadu, India.
Mrs. L. Leelavathy, Assistant Professor, Department of Computer Science, Sri Meenakshi Vidiyal Arts and Science College, Trichy, Tamil Nadu, India.

1.2.1 Private Cloud

Private cloud is a fresh term that some merchants have recently used to describe aids that rival cloud computing on private networks. It is set up within an organization's internal enterprise datacenter.

In the private cloud, scalable resources and virtual applications provided by the cloud vendor are pooled together and available for cloud users to share and use. It differs from the public cloud in that all the cloud resources and applications are managed by the organization itself. Utilization on the private cloud can be much more secure than that of the public cloud because of its specified internal exposure. Only the organization and designated stakeholders may have access to operate on a specific Private cloud.

1.2.2 Public Cloud

Public cloud describes cloud computing in the traditional mainstream sense, whereby resources are dynamically provisioned on a fine-grained, self-service basis over the Internet, via web applications/web services, from an off-site third-party provider who shares resources and bills on a fine-grained utility computing basis. It is typically based on a pay-per-use model, similar to a prepaid electricity metering system which is flexible enough to cater for spikes in demand for cloud optimization. Public clouds are less secure than the other cloud models because it places an additional burden of ensuring all applications and data accessed on the public cloud are not subjected to malicious attacks.

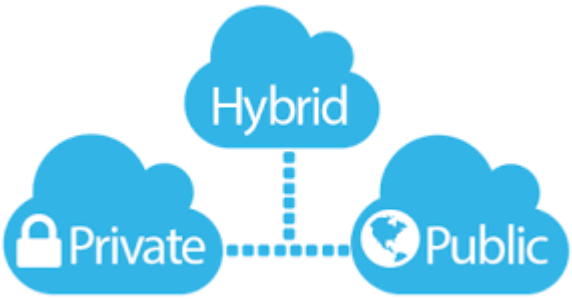

Fig.2: Cloud Computing Deployment Model

1.2.3 Hybrid Cloud

Hybrid cloud is a private cloud linked to one or more external cloud services, centrally managed, provisioned as a single unit, and circumscribed by a secure network. It provides virtual IT solutions through a mix of both public and private clouds. Hybrid Cloud provides more secure control of the data and applications and allows various parties to access information over the Internet. It also has an open architecture that allows interfaces with other management systems. Hybrid cloud can describe configuration combining a local device, such as a Plug computer with cloud services. It can also de-scribe configurations combining virtual and physical, collocated assets -for example, a mostly virtualized environment that requires physical servers, routers, or other hardware such as a network appliance acting as a firewall or spam filter.

1.3. Cloud Computing Services

Cloud computing services are available across the entire computing spectrum. The basic services of cloud have been considered as the following.

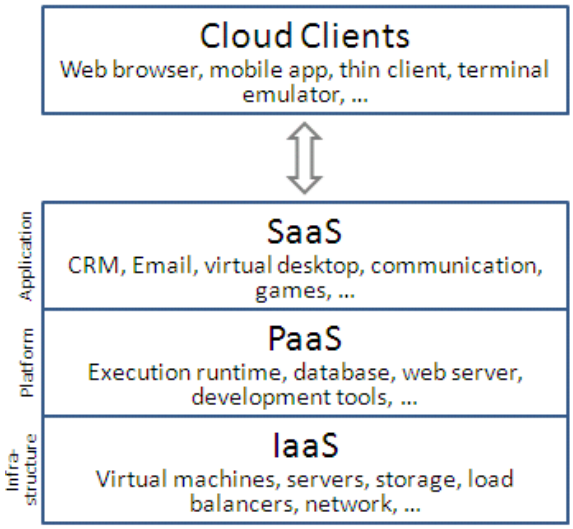

Fig. 3: Cloud Computing Services.

Software as a service (SaaS): SaaS reassign programs to millions of users all the way through browser. For user, this can save some cost on software and servers. For Service provider's, they only need to maintain one program, this can also saves space and cost. SaaS provider naturally hosts and man-ages a given application in their own or leased datacenters and makes it available to multiple tenants and users using the Web.

Platform as a Service (PaaS): PaaS is an application development and deployment platform provided as a service to developers over the Web. Middleman's equipment can be used to develop programs and transfer it to the end users through internet and servers. The cost and complexity of development and deployment of applications can be reduced to a great extent by developers by using this service. So the developers can reduce the cost of buying and reduce the complexity of managing the necessary Infrastructure. It provides all of the services essential to support the complete life cycle of building and delivering web applications and all the services entirely available from the Internet. This platform consists of infrastructure software, a middlware and database and development tools.

Infrastructure as a Service (IaaS): IaaS is the delivery of associated software and hardware as a service. Hardware like server, storage and network, and associated software like operating systems, virtualization technology and file system. It is an evolution of traditional hosting to allow users to provide resources on demand and without require any long term commitment. Different PaaS services, the IaaS provider does very little management other than keep the data center operational and end-users must deploy and manage the software services themselves-just the way they would in their own data center [8].

1.4 Cloud Computing Challenges

Trusting the Cloud Service Provider and their offerings is one of the strongest driving forces behind the decision of a user to move into a cloud system or continue with the legacy system [9]. Trust is based on the assessment as to whether a provider has covered all the risks, including areas of data security,

VM security as well as other government and compliance issues. The three factors that have been considered here for the evaluation of the Cloud system security are Confidentiality, Integrity, and Availability. As the CIA, domain is a widely used convention for determining the security concerns of a traditional information system, the main focus of this section is to generalize the security requirements in an existing Cloud system under this domain. Further sub categorization and fine grained classification of security issues [10] have been presented here which would ease the understandability, mapping and evaluation of the cloud specific attacks and proposed solutions presented in the later sections.

1.4.1 Confidentiality

Confidentiality refers to the protection of some enterprise asset from disclosure to unauthorized users. In a Cloud computing environment that kind of end users may be clients who might want to get unauthorized access to the data of some other individual which is stored in the same table as that of the intruder's data by the CSP. Cloud Service supplier (CSP) [11] maintain that cupboard space and is to blame for the safety and accessibility of the homeowner's knowledge. The Third-Party Auditor is third system where UN agency checks the integrity of restricted information and if the sensitive knowledge hold on cloud storage on facet of the information Owner and fourth one is cloud knowledge Users.

Data Confidentiality

Data [12] residing at the CSP end is often stored and processed in plaintext. Thus CSP is held responsible for maintaining the confidentiality of client data during its entire life cycle. Some cloud specific data confidentiality issues include: A number of Cloud Storage providers allow shared access to online folders that store the user data. This may result is potential loss of data confidentiality. Even when a file is shared in a group using a Cloud storage service the owner must get periodic updates about any changes regarding the group. In short, client data segregation from other data (competitor, unauthorized user) must be handled explicitly by the CSP.

The actual geographical location of the user's data is another factor that affects the data confidentiality. CSP can actually move the data from one data centre to another which in many cases changes the entire set of legal rules enforced. If user processes data in the US, store it on servers in the UK and send it via London, then it becomes difficult to determine the exact laws that should be obeyed and naturally poses a threat to the confidentiality of the user data.

Cloud service providers that do not allow data owners to encrypt their own data or information before deploying them on the cloud, poses a serious threat to the user data confidentiality. Sensitive information such as medical or health records, government or defense data should not be stored in Cloud if encryption options are not available.

Virtualization Confidentiality

In the cloud system the Infrastructure as a service, CSP hosts virtual machines where the user applications are executed. In a Cloud system, anyone with privileged access to the host can read or manipulate the deployed service that resides in each VM. Therefore, users cannot protect the confidentiality of VMs on their own. Thus, the total virtualization layer induces certain security loopholes that appear to be a serious matter of concern when considering Cloud security issues. Few of those are discussed as following:

Virtual Machine migration, particularly live migration, is an expedient feature of Cloud Computing systems environment for fault tolerance, load balancing, elastic scaling and hardware maintenance.

In the virtualized environment of a Cloud system, multiple workloads share the same hardware environment and this gives rise to issues of workload isolation which is highly required by different departments or areas who want to keep their data separate and secure from each other.

1.4.2 Integrity

Integrity raises to the security property of an asset that guarantees that it has not been modified by some third party personnel who is not authorized for such an activity. Thus accuracy and correctness of an asset with respect to its holder is ensured by this property. Usually, append and delete or edit operations are believed to change the integrity of any asset. Since Cloud based services are accessed by users via web browsers, therefore all the web based attacks are highly prevalent in a Cloud system environment that can change the contents of user databases, files, and VM or WSDL files.

Data Integrity

The Cloud system [13] deals with a good number of data centric operations with massive data requirements where massive refers to TB and PB bytes of the users data. Thus data integrity challenges associated with DaaS, SaaS, PaaS, etc. given bellow the some of the issues related to this.

Data outsourcing at the CSP end poses an obvious threat on its integrity. CSP could delete some valid tuples related to a client's data and the client would never be able to establish this fact. **SQL injection attack** is one of the remarkable web-based attacks that could modify the contents of the end user databases by exploiting the vulnerabilities of web servers and injecting malicious codes into the system. **Cross scripting attacks** are another form of malware injection attacks where hackers could insert malicious scripts into vulnerable dynamic web pages. **Metadata Spoofing attack** is one of the attacks which modify the contents of the WSDL files

VM Integrity as conversed earlier, the virtualization layer itself encourages certain security issues which are not confined within the limits of confidentiality alone and also along with confidentiality the integrity of the VM. The VM replication is another important factor which may cause unwanted data leakage. VM rollback is a phenomenon in Cloud computing that may again introduce certain integrity problems in the VM. Rolling back virtual machines can recreate security.

1.4.3 Availability

Availability is one of the most important aspects of security that needs to be maintained by a CSP. Many business organizations use cloud based services to serve their end users must assure the availability. A typical service-level agreement states what the provider has agreed to deliver in terms of availability and response to demand. VMs and availability issues have been addressed in the given bellow:

Service and Data Availability

DoS attack in the Cloud system is one of the main causes of service or data unavailability. The attacker generally sends huge amount of vague requests to a certain service. When the Cloud Computing operating system notices the high workload on the flooded service, it starts providing more computational power to handle the additional workload. Trouble of service by third party WAN providers could lead to temporary service outages or flat certain software bugs could affect multiple copies of cloud data at the same time thus making it unavailable to its original owners. Natural disasters like fire, flood etc. in a data center are likely to affect both the main and redundant copies of data.

Virtualization Availability

As we have previously seen, ensuring high availability covers a number of zones that need to be considered, such as network vulnerability, multisite redundancy and storage failure. But since virtualization is one of the most important aspects of the Cloud system, availability in Cloud should be considered after combining the essence of virtualization with it. One of the most important issues here is of IP failover. The host machine or VMM may crash due to some reason causing all the VMs running on it to fail. Such a situation must be avoided by the CSP by arranging an alternative host machine for all the VMs which were previously running on the failed VMM [14].

1.4.4 Service Level Agreement: Although cloud consumers do not have control over the underlying computing resources, they do need to ensure the quality, availability, reliability, and performance of these resources when consumers have migrated their core business functions onto their entrusted cloud. Typically, these are provided through Service Level Agreements (SLAs) negotiated between the providers and consumers. The very first issue is the definition of SLA specifications in such a way that has an appropriate level of granularity, namely the tradeoffs between expressiveness and complicated-ness, so that they can cover most of the consumer expectations and is relatively simple to be weighted, verified, evaluated, and enforced by the resource allocation mechanism on the cloud. In addition, different cloud offerings (IaaS, PaaS, and SaaS) will need to define different SLA Meta specifications. This also raises a number of implementation problems for the cloud providers.

1.4.5 Cloud Interoperability Issue: Presently, each cloud system offering has its own way on how cloud users interact with the cloud. The main area of interoperability is to realize the seamless fluid data across clouds and between cloud and local applications. There are a number of levels that interoperability is essential for cloud computing. 1st to optimize the IT asset and computing resources, an organization often needs to keep in-house IT assets and capabilities associated with their core competencies while outsourcing marginal functions and activities on to the cloud. 2nd more often than not, for the purpose of optimization, an organization may need to outsource a number of marginal functions to cloud services offered by different vendors.

This paper is prearranged as follows. Section 2 highlights a brief review of literature on security issues in cloud computing and Section 3 presents the conclusion.the final paper but after the final submission to the journal, rectification is not possible.

II. RELATED WORK

The objective [15] is to high spot the principal issues connected to data security that raised by cloud computing environment. These topics was classified into 3 categories: first data security issues raised by single cloud characteristics compared to traditional infrastructure, second data security issues raised by data life cycle in cloud computing, third data security issues associated to data security attributes. For the above said category, the joint solutions used to secure data in the cloud were stressed. In this paper is an overview of data security issues in the cloud computing environment.

Data security and privacy protection are the two important factors in cloud computing. This topics on cloud computing have been investigated in both academics and industries, data security & privacy protection are becoming more vital for the future development of cloud technology in government, industry, and business. These issues are relevant to both software and hardware in the cloud computing environment architecture. To review [16] different security techniques and challenges from both software and hardware aspects for protecting data in the cloud and aims at enhancing the data security and privacy protection for the reliable cloud system environment. A comparative research analysis of the existing research work regarding the data security and privacy protection techniques used in the cloud computing.

A new approach to security that is controlled by the IT Security Specialist (ITSS) of the organization. The approach is based on multiple strategies of file encryption, partitioning and distribution among multiple storage providers, resulting in increased confidentiality since a supposed attacker will need to first get parts of a file from different storage providers, know how to combine them, before any decryption attempt. All details of the plan used for a particular file are stored on a separate file, which can be careful as a master key for the file contents. Also, present each strategy [17] with the results and comments related to the understood measurements.

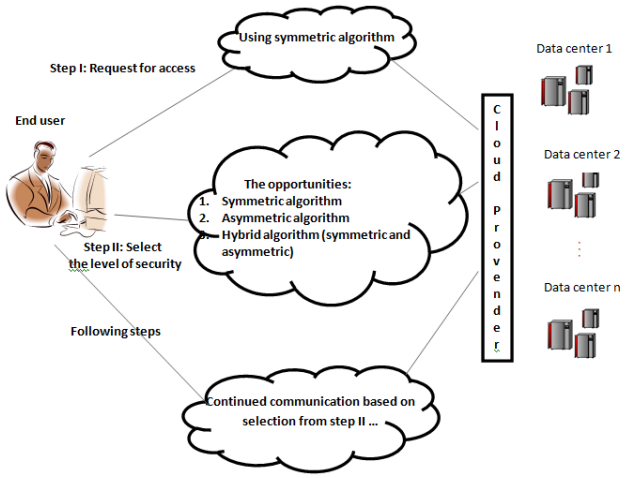

Fig.4.data security

The focus of this model to control data security in the cloud. Recent trends in cloud security have played an important role to attract organizations and companies to deploy sensitive data in cloud. In this setting, the model offers different scenarios based on the level of sensitivity of users data. In another point of view, it increases reliability of clients in cloud computing. This reliability will be increased by offering controls of data security to the end user- ITSS.

The risks and security threats [18] to the end users data in the cloud and given an overview of three types of security concerns. Virtualization is examined to find out the threats caused by the hypervisor. Similarly, threats caused by Public cloud and multitenancy have been discussed. One of the major concerns was data security and its threats and solutions in cloud computing. Data in different states has been discussed along with the techniques which are well-organized for encrypting the user's data in the cloud computing environment. The study delivered an overview of stream & block cipher and also the hash function which are used for encrypting the data in the cloud whether it is at rest or in transfer.

The problem of concurrently achieving finegrained ness, high efficiency on the data owner's side, and standard data confidentiality of cloud data sharing actually still remains unresolved. New attribute-based data sharing scheme suitable for resource-limited mobile users in cloud computing system. The scheme eliminates a majority of the computation task by adding system public parameters besides moving partial encryption computation offline. In addition, a public cipher-text test phase is performed before the decryption phase, which eliminates most of computation overhead due to illegitimate cipher-texts. For the sake of data security, a Chameleon hash function is used to generate an immediate cipher-text, which will be blinded by the offline cipher-texts to obtain the final online cipher-texts. This scheme is proven secure against adaptively chosen cipher-text attacks, which is widely recognized as a standard security notion. Extensive performance analysis [19] indicates that the scheme is secure and efficient.

Data sharing and storage for the similar group in the cloud with high security and efficiency in an anonymous way.

By leveraging the key agreement and the group signature, an original traceable group data sharing scheme is to support anonymous multiple users in public cloud computing environment. On the one hand, group members can communicate anonymously with respect to the group signature, and the real identities of members can be traced if necessary. On the other hand, a common conference key is derived based on the key agreement to allow group members to share and store their user's data securely. A symmetric [20] balanced incomplete block design is utilized for key generation, which substantially reduces the burden on members to derive a common conference key. The theoretical & experimental analyses demonstrate that the scheme is secure and efficient for group data sharing in cloud computing system environment.

Existing privacy preserving schemes cannot provide a systematic preservation. Pay care to the links of information lifecycle, such as information collection, storage, processing, distribution and destruction. The theory of privacy computing and the key technology system, including privacy computing framework, formal definition of privacy computing, four principles that should be followed in privacy computing, algorithm design criteria, evaluation of privacy preserving effect, privacy computing language and so on. [21] Finally, four application scenarios to describe the universal application of privacy computing and prospect of the future research trends. It is expected to guide the theoretical research on user's privacy preservation under open locations.

The Security intimidations involved in cloud computing system, the users hesitate to use its services in spite of the great savings promised by Cloud computing environment. An overview of Cloud Computing system and the security challenges related to Cloud are discussed and also the Cloud security can be improved with the help of many high-tech approaches available but currently there are no answers that can provide all security features and the challenges such as service level agreements for security has to be tackled, also for ensuring answerability in the cloud certain holistic mechanisms should be implemented. [22]

III. RESULT

In this work, we have revealed that cloud computing environment have always been security risks in old-style corporate networks and application architecture as well as emergent cloud computing architecture and also the cloud computing fundamentals to make the paper self-content. Then, presented the analysis of the recent advances in security and privacy issues, security threats, vulnerabilities and countermeasures that are of interest to the entire cloud computing environment and note that the security threats to cloud computing will continue to be persistent and exponentially increase with the applications.

Table1: Type of Vulnerabilities

THREATS	VULNERABILITIES	CONTROLS
Loss of data	Software /hardware Failure , Encryption keys Loss	Backup
APIs -insecure & interfaces	Malicious/unidentified access	APIs –model for security analyze
Dos Denial-of-service	Hx-dos attack	Prevention of ddos
Abuse of cloud services	Illegal use of cloud computing for criminal activities &	Monitor user's network traffic
Technology vulnerabilities	VM hopping & escape	Controls for VM hopping , controls for VM escape

By minimizing the security vulnerabilities, cloud computing can be made harmless place to store and process the data. Numerous of the security vulnerabilities we are having today, were as a result of the contest and insistence to build front-line business solutions.

IV. CONCLUSION

In this paper shelters the necessary security concepts and security requirements of a prevailing Cloud computing system environment. In the above said generalized issues have been presented here to enhance the significance of considerate the security flaws of the Cloud computing environment and suitable countermeasures for them. On a whole, the paper aims at constructing a proper snapshot of the present scenario of securing in Cloud computing environment.

REFERENCES

1. Beaulah A Navamani∗, Chuan Yue†, and Xiaobo Zhou ,“ An Analysis of Open Ports and Port Pairs in EC2 Instances”, 2017 IEEE 10th International Conference on Cloud Computing, 2159-6190/17 $31.00 © 2017 DOI 10.1109/CLOUD.2017.116 IEEE, 2017.
2. Eesa Alsolami, “Security threats and legal issues related to Cloud based solutions”, IJCSNS International Journal of Computer Science and Network Security, VOL.18 No.5, May 2018.
3. Manu A R, V K Agrawal, K N Bala Subramanya Murthy, “An Empirical Hunt for Ally Co-Operative Cloud Computing Utility”, 2017 11 th International Conference on Intelligent Systems and Control (ISCO). 978-1-5090-2717-0/171$31 .00 IEEE, 2017
4. Olumide Olugbenga Malomo, Danda B. Rawat and Moses Garuba “A Survey on Recent Advances in Cloud Computing Security”, Journal of Next Generation Information Technology (JNIT) Volume9, Number1, Mar. 2018.
5. Dr. N. Krishna Murthy1, Dr. R. Selvam “Security Issues and Challenges in Cloud Computing”, International Advanced Research Journal in Science, Engineering and Technology Vol. 2, Issue 12, December 2015.
6. Wg Cdr Nimit Kaura Lt Col Abhishek Lal “Survey Paper On Cloud Computing Security”, 2017 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS), IEEE, 2017.
7. Kirti Ashokrao Tayade, G. S. Malande,” Survey Paper on a Secure and Authorized DeduplicationScheme using Hybrid Cloud Approach for Multimedia Data” ,International Conference on Energy, Communication, Data Analytics and Soft Computing, for Multimedia Data ,(ICECDS-2017)
8. Nazia Majadi “Cloud Computing: Security Issues and Challenges”, International Journal of Scientific & Engineering Research, Volume 4, Issue 7, July-2013.
9. Shazia Tabassam “Security and Privacy Issues in Cloud Computing Environment”, Journal of
a. Information Technology & Software Engineering, Volume 7 • Issue 5, 2017.
10. Hironori Washizaki,” Security Patterns: Research Direction, Metamodel, Application and Verification” IWBIS 2017 978-1-5386-2038-0/17/$31.00 c2017 IEEE, 2017.
11. Tanupriya Choudhury, Ayushi Gupta, Saurabh Pradhan, Praveen Kumar, Yogesh Singh Rathore, “Privacy and Security of Cloud-Based Internet of Things (IoT)”, 2017 International Conference on Computational Intelligence and Networks, 978-1-5386-2529-3/17 $31.00 ©IEEE DOI 10.1109/CINE.2017.28, 2017.
12. P.Priya ponnusamy, Dr..R.Vidhyapriya ,“ Dr..R.Vidhyapriya,” A Survey on Multi-Keyword Ranked Search Manipulations over Encrypted Cloud Data”, 2017 International Conference on Computer Communication and Informatics (ICCCI -2017), Jan. 05 – 07, 2017, Coimbatore, INDIA.
13. Mohammed-Ali Anwar “Data Security Issues in the Realm of Mobile Cloud Computing: A Survey”, PeerJ Preprints | https://doi.org/10.7287/peerj.preprints.27050v1 | CC BY 4.0 Open Access | rec: 24 Jul 2018, publ: 24 Jul 2018.
14. Srijita Basu, Arjun Bardhan, Koyal Gupta,Payel Saha, Mahasweta,“ Cloud Computing Security Challenges & Solutions-A Survey”, https://www.researchgate.net/publication/323566557, Conference Paper · January 2018.
15. Lynda Kacha and Abdelhafid Zitouni “An Overview on Data Security in Cloud Computing”, Advances in Intelligent Systems and Computing, 661, September 2018.
16. Yunchuan Sun, 1 Junsheng Zhang,2 Yongping Xiong,3 and Guangyu Zhu4 “Data Security and Privacy in Cloud Computing”, International Journal of Distributed Sensor Networks · July 2014.
17. Dhuratë Hyseni, Artan Luma, Besnik Selimi, Betim Cico “The Proposed Model to Increase Security of Sensitive Data in Cloud Computing”, (IJACSA) International Journal of Advanced Computer Science and Applications, Vol.9, No. 2, 2018.
18. Ahmed Albugmi Madini O. Alassafi Robert Walters, Gary Wills “Data Security in Cloud Computing”, Fifthe international conference on future generation communication technologies -FGCT 2016.
19. Jin Li , Yinghui Zhang , Xiaofeng Chen , Yang Xiang, “Secure attribute-based data sharing forresource-limited users in cloud computing”, computers & s e c u r i t y 72 (2 0 1 8).
20. Jian Shen , Tianqi Zhou, Xiaofeng Chen,, “Anonymous and Traceable Group Data Sharing in Cloud Computing”, IEEE Transactions On Information Forensics And Security, Vol. 13, No. 4, April 2018.
21. Fenghua Li, Member, IEEE, Hui Li *, Member, IEEE, Ben Niu, Member, IEEE, and Jinjun Chen,Senior Member, IEEE “Privacy Computing: Concept, Computing Framework and Future Development Trends”,
22. Prabal Verma, Aditya Gupta, Rakesh Singh Sambyal “Security Issues and Challenges in Cloud Computing: A Review”, International Journal of Scientific Research in Computer Science, Engineering and Information Technology, CSEIT411832 | Published - 25 April 2018 (4) 1 : 189-196, | March-April-2018.

AUTHORS PROFILE

Dr. R. Sugumar, Professor & Director ,ChristhuRaj College, Department of Computer Science. He has more than 50 publications in reputed journals and holding around 20 years of experience in teaching and research field. His focus includes network security, cloud computing and data minning.

Mrs. L. Leelavathy, working as Assistant Professor, Department of Computer Science in Sri Meenakshi Vidiyal Arts and Science College, Trichy , from 2017 to till date. She has completed MCA.,M.Phil., Computer Science in Bharathidasan University and pursuing Ph.D., in the discipline of Computer Science at Bharathidasan University. She is the Soft Skill trainer. Motivation, guidance and training given to many college students to achieve in their life.