iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 5 **Issue:** VII **Month of publication:** July 2017

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor:6.887
Volume 5 Issue VIII, July 2017- Available at www.ijraset.com

A Survey: Threats for Data Security and Solution Approaches in Cloud Computing

Mandeep Kaur[1], Gurbahar Singh[2]
[1,2] *Computer Science Department, BBSBEC, Fatehgarh SahibMaharaja Ranjit Singh Punjab Technical University*

Abstract*: *In order to fulfill the requirements of the users like availability of data or information on a single server, which is accessible to the interested user, the concept of cloud computing is developed. But with the high availability of the data over the internet leads to the issue of data security due to which the security of the data is at an alarming. In case of cloud computing the security of the data is a major issue because here data is dispersed over the various geographic locations. Data security and data privacy are two major concerns of the users of cloud computing. Various data security techniques have been developed since last few years. This work provides an overview of the concept of security and privacy of data in cloud computing along with various measures that should be taken to resolve the issue. This paper gives an overview to the various security issues and countermeasures in this direction.

Keywords: Cloud computing, Security, LZW, Data security, huffman encoding

I. INTRODUCTION

Cloud computing is an advanced technology which facilitates large number of users to work in a pool. It provides various services to its users in different terms and means. Cloud computing is a solution to the issues of lack of resources, data storage devices etc which are faced by various industries and organizations with high volume of data. Cloud computing is a kind of distributed [1] computing which provides business possibilities to both consumer as well as service providers. Service Providers are organizations which are responsible for the cloud services which are provided to its users such as IaaS i.e. Infrastructure as service, PaaS i.e. Platform as a Service and SaaS i.e. Software as a Service[2]. A user can only utilize these services if the system is able to access the internet. These services are defined as below:

A. IaaS (Infrastructure as a Service)

it provides a virtual network, server, router, storage and many more as services to the users. All of the above defined modules are required to create an infrastructure for accessing cloud services [3].

B. PaaS (Platform as a Service)

This module or facility is accountable to testing, development, deployment of web applications or software on the cloud. Hence the whole SDLC process takes place on this service.

C. SaaS (Software as a Service)

Last but not the least, deliverance of software application services to the end users on an on-demand basis is operated by SaaS service [4].

Definitely, cloud delivers the services to its users without any interludes through cloud service provider. Thus several persuasive features make it attractive for the researchers as well as business owners. Some of them follow as[5]:

1) Virtualization
2) Reliability
3) Security
4) Maintenance
5) Agility

As cloud Service supplier gives virtualization of systems. Subsequently worrying about keeping up the product is completely isolates. Finally, in Agility, QoS (nature of administration) in the cloud gives speedy response time. At the end of the day, adaptability of the Cloud Service Provider can be controlled by its response time i.e. how prior it react to the end user in peak loads too as far as memory, storage, and system resources requests[6].

II. DATA SECURITY CHALLENGES

Distributed computing security is the real worry to be tended to these days. In the event that safety efforts are not given legitimately to information operations and transmissions then information is at high hazard [7]. Since distributed computing gives an office to the clients to get the put away information there is a chance of having high information hazard. Most grounded safety efforts are to be executed by recognizing security test and answers for handle these difficulties.

As the generation is shifting towards the internet based cloud computing the focus is lying on the security of the data. Data security here refers to the security of the data from various hazardous elements such as third party intervention, attacks to the data, data tempering, hacking etc. If the data is leaked out or becomes accessible to the unauthorized entity that it can leads to the great [8] loss for the organization since the attacker can manipulate or misuse the data for its benefit. Hence the prevention of data leakage, data tempering and access of unauthorized access has gained so much attention from last few years. Data Security has the following challenges:

A. Security

The aspect of the security covers the three modules in it like Confidentiality, availability, integrity. The security is at high risk in such cases where there are multiple entities to access it. Hence there is a need to maintain the security of the data over the cloud by introducing the [9] concept of authentication and authorization of the users. The three modules of security are as follows:

1) *Confidentiality:* It depicts that the specific information will never be released to the unauthorized person or node. The deliberate or strategic information need to be keeping secure or confidential from enemy or third party [10]. If this kind of information is leaked or revealed to the third party then it can lead to the overwhelming consequences. In this case the malicious users can be cross-site scripting, access control mechanism etc.
2) *Integrity:* refers that the transferred message will never be corrupted and will remain reliable till it reaches to the destination [11]. The message or data can get corrupted due to malicious attacks on the network in order to have an unauthorized access to the information.
3) *Availability*: is a property which defines that the server can be capable to work even in the state of denial of service attack [12].

B. Locality

In cloud computing the data is dispersed over the large number of locations since the users are located on the various geographical locations [13]. Therefore it becomes difficult to find out the location or source of the data. With the variation of the geographical location of the data the laws or rules or format of the data also gets changed. Hence it leads to the problem that the data privacy [14].

C. Access

Data access is the main module which leads to the security broken easily. Because if the third party or unauthorized users gets access to the data by using their hacking skills then it will be a great loss for the business or generator of the information. Hence there is a need to make such policies so that the data could not be easily available or accessible by unauthenticated persons [15]. This can only be done by generating a valid user name and password corresponding to each user of the data which can makes data available to only those persons who have a valid user name or password or identity [16].

D. Data Breaches

Data a breach is referred as the main security issue in concept of cloud computing. While the cloud computing facilitates the large number of users to store the data over the cloud server hence this facility can leads to the chances of entering the malicious or unauthorized users in the cloud environment which can bring the whole cloud on the high security risk. Breach can take place because of unplanned transmission issues or problems due to internal attacks [17].

E. Storage

As we know that the cloud computing provides a virtual storage environment for the user to store the data. The virtual machines are required to keep in a physical location which may leads to the security of secured data at a risk of getting data to be losses [18].

F. Data Center Operations

The data center operations are initiated in order to resolve the data transmission issues since the organizations wishes to protect or secure the user's data without any bottleneck. Hence this can be achieved [19] by managing the data in a perfect way. If it is not done in a manner then it can lead to the data loss or tempering and the cloud providers will be responsible for this act.

III. SOLUTION TO DATA SECURITY

After reviewing the above section of this study it can be said that it becomes mandatory to make the secure from unauthorized users or various attacks. In order to secure the data the concept of compression and encryption is referred as best solution [20].

The compression reduces the size of the data and encryption converts the data in an encrypted format which is in a coded form hence it becomes difficult for the unauthorized user to read the encrypted data even if he gets access over it, hence the data becomes secure. There is various compression and encryption techniques have been developed which makes it easier to compress and encrypt the data. Some of these techniques are as follows:

A. LZW (Lempel-Ziv-Welch) Coding

LZW is a dictionary based coding in which each character is initialized with the 256 values of the ASCII table. This technique is based on the occurrence of multiplicity of character sequences in the string to be encoded. The file is divided into strings of bytes. Strings that are encoded in the file is compared with the dictionary and if the string is not present, it will be added in the dictionary. Encoding and decoding is performed with the stream of information. In the encoding process [21], the algorithm goes over the stream of information and performs coding. If the encoded string is not smaller than the longest word in the dictionary then the string is transmitted whereas in the decoding process algorithm redefines the dictionary in the opposite direction. LZW is divided into two categories i.e. static and dynamic. In static dictionary coding, encoding and decoding does not affect the dictionary.

B. Run Length Encoding

This type of technique is used to remove the redundancy of data. It works by replacing the sequence identical symbol or pixel [22]. Thus, it is known as run by shorter symbol. Representation of run length code is by sequence (Vi, Ri) where Vi represents the intensity of pixels and Ri shows the number of consecutive pixel with intensity.

Eg:- [70 70 70 7 70 12 12 90 90 90]

{70,5},{12,2},{90,3}

C. Huffman Coding

In this technique, each pixel is treated as symbol. It is based on the frequency of occurrence of a data item. Symbols having frequency assigned small number of bits whereas the symbols having less frequency assigned the large number of bits. This technique consists of a code book that stores code which may be constructed for each image or set of images [23]. The technique performs in such a way

1) Divide the image into 8x8 blocks
2) Each pixel or block is treated as a symbol i.e. to be coded
3) Compute the Huffman codes for set of block
4) Lastly, encode blocks.

IV. RELATED WORK

A. Shankar Nayak Bhukya, et al, "Data Security in Cloud Computing and Outsourced Databases", [1]

With the advent of big data era, clients lack of computational and storage resources tends to outsource data mining tasks to cloud computing providers in order to improve efficiency and save costs. Generally, different clients choose different cloud companies for the sake of security, business cooperation, location, and so on. However, due to the rise of privacy leakage issues, the data contributed by clients should be encrypted under their own keys. This paper focuses on privacy-preserving k-nearest neighbor (kNN) computation over the databases distributed among multiple cloud environments. Unfortunately, existing secure outsourcing protocols are either restricted to a single key setting or quite inefficient because of frequent client-to-server interactions, making it impractical for wide application. To address these issues, we propose a set of secure building blocks and outsourced collaborative

kNN protocol. Theoretical analysis shows that our scheme not only preserves the privacy of distributed databases and kNN query but also hides access patterns in the semi-honest model. Experimental evaluation demonstrates its significant efficiency improvements compared with existing methods.

B. Ni Zhang et al, "A Research on Cloud Computing Security", [26]

this paper gave an overview on security of cloud computing. To simplify cloud security, a definition and scope of cloud computing security was represented. An ecosystem of cloud security was presented to demonstrate what each role in industry can do in turn. Then security effects of cloud security for both customers and operators were analyzed. To overcome challenges from cloud security, many state-of-the-art technical solutions, e.g., continuation protection mechanism, IDM, data security, and virtualization security were discussed. Finally, best practices on perspective of operator were summarized and a conclusion was conducted.

C. Rabi Prasad Padhi et al, "Cloud Computing: Security Issues and Research Challenges",[27]

this research paper summarized what cloud computing is, the different cloud models and the main security risks and concerns that are currently present within the cloud computing industry. This research paper also examined the key research and experiments that happen in cloud computing and delivered best services to service providers as well as enterprises expecting to influence cloud service to enhance their bottom line in this severe economic climate.

D. Suruchi V. Nandgaonkar, "A comprehensive study on cloud computing", [28]

this paper provided a comprehensive analysis on the motivation aspects of adopting cloud computing, review the several cloud deployment and service models. It also explored certain advantages of cloud computing over traditional IT service environment involving scalability, flexibility, reduced capital and higher resource utilization were considered as adoption reasons for the environment of cloud computing. This paper also included security, privacy, and internet dependency and availability as avoidance problems. The later contained vertical scalability as technical challenge in cloud environment.

E. Monjur Ahmed et al, "Cloud Computing And Security Issues in The Cloud", [29]

Cloud computing has designed the conceptual and infrastructural basis for tomorrow's computing. The global computing infrastructure is swiftly moving towards cloud based architecture. While it is vital to take benefits of cloud based computing by means of deploying it in diversified sectors, the security factors in a cloud based computing environment remains at the core of interest. If security is not robust and consistent, the flexibility and plus points that cloud computing has to offer will have little credibility. This paper provided an outline on the concepts of cloud computing and security concerns inherent within the context of cloud computing and cloud infrastructure.

F. Yunchuan Sun et al, "Data Security and Privacy in cloud computing", [30]

this study was to review various techniques of security and challenges from both software and hardware characteristics for protection of data in the cloud and targeted at improving the data security and privacy protection for the trustworthy cloud environment. In this paper, a comparative research analysis of the existing research work was made regarding the data security and privacy protection methods used in the cloud computing.

G. Keiko Hashizume et al, "An Analysis if security issues for cloud computing", [31]

cloud computing provides a business to consumers by using the internet. The cloud computing is the most prominent technology which is used at a very large scale nowadays. It has various advantages such as assured delivery of the data, cost effective etc. but the only problem that cloud computing suffers from is security related issue. The reason behind this is availing the services from third parties. Various technologies like virtualization, SOA are covered by cloud computing, it also grasps various security issues of same technologies. This study shows the various securities related threats that occur in cloud computing. The objective behind this work was to detect the security issues so that the proper action to solve the issue can be taken.

H. Michael armbrust, "A view on Cloud computing", [32]

Distributed computing, the long-held dream of figuring as an utility, can possibly change a vast piece of the IT business, making programming much more appealing as an administration and forming the way IT equipment is composed and acquired. Engineers

with inventive thoughts for new Internet benefits at no time in the future require the substantial capital costs in equipment to send their administration or the human cost to work it. They require not be worried about over provisioning for an administration whose notoriety does not meet their expectations, in this way squandering exorbitant assets, or under provisioning for one that turns out to be uncontrollably well known, accordingly missing potential clients and income. Additionally, organizations with huge bunch arranged assignments can get comes about as fast as their projects can scale, since utilizing 1,000 servers for one hour costs close to utilizing one server for 1,000

I. Ling Qian,"Cloud computing-An overview", [33]

the greatest number of client and versatile administration with the base asset, the Internet specialist organization designed the distributed computing. Inside a couple of years, rising distributed computing has turned into the most sweltering innovation. From the distribution of center papers by Google since 2003 to the commercialization of Amazon EC2 in 2006, and to the administration offering of AT&T Synaptic Hosting, the distributed computing has been advanced from interior IT framework to open administration, from cost-sparing devices to income generator, and from ISP to telecom. This paper presented the idea, history, upsides and downsides of distributed computing and in addition the esteem chain and institutionalization exertion.

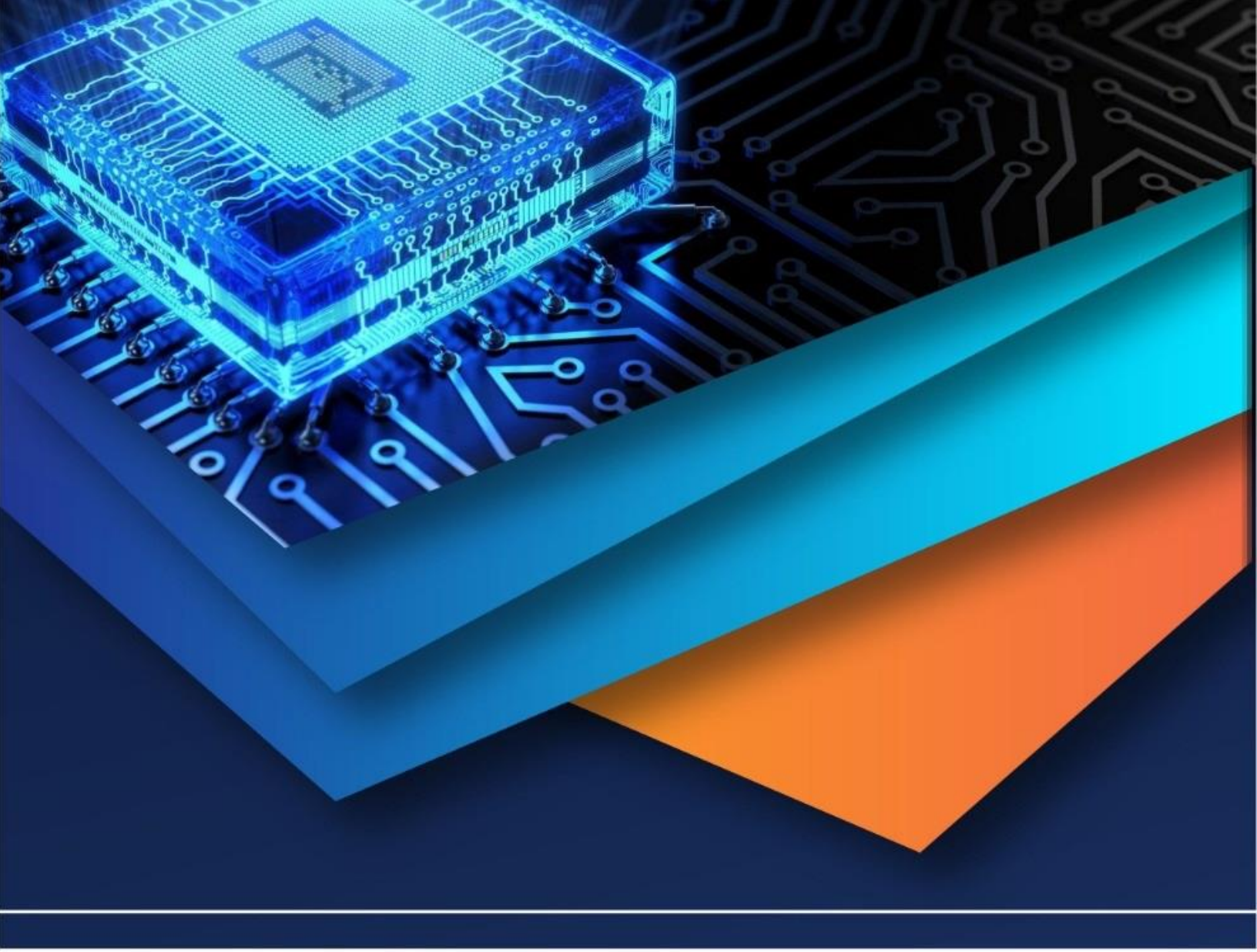
V. CONCLUSIONS

Cloud computing is one of the trending concept among various researchers. Cloud computing also suffers from various issues like security of data that travels from one device to another. This study is a review study that provides a brief introduction to the various concepts such as cloud computing, security in cloud computing, various algorithms that can be used to secure the data in the cloud. On the basis of the related work that is explained by this study it is concluded that most of the research had been conducted by using traditional mechanisms such as encryption, cryptography, RSA algorithm, LZW technique etc. Therefore in future more advancement can be done by using some prominent artificial intelligent schemes such as ANN, KNN etc.

REFERENCES

[1] Shankar Nayak Bhukya, et al, "Data Security in Cloud Computing and Outsourced Databases", IEEE, Pp: 2458-2462, 2016.
[2] Mrinal Kanti Sarkar, et al, "A Framework to Ensure Data Storage Security In Cloud Computing", IEEE, Pp: 1-4, 2016.
[3] Ahmed Albugmi, "Data Security in Cloud Computing", IEEE, Pp:55-59, 2016.
[4] K. B. Priya Lyer, et al, "Analysis of Data Security in Cloud Computing", IEEE, Pp: 540-543, 2016.
[5] Zoltan Balogh, et al, "Modeling of Data Security in Cloud Computing", IEEE, Pp: 1-6, 2016.
[6] C. Linda Hepsiba, et al, "Security Issues in Service Models of Cloud Computing", IJCSMC, pp: 610-615, 2016.
[7] R. Velumadhava Rao, et al, "Data Security Challenges and its Solutions in Cloud Computing", ELSEVIER, Pp: 204-209, 2015.
[8] Kamal Kumar Chauhan, et AL, "Homomorphic Encryption for Data Security in cloud Computing", IEEE, Pp: 206-209, 2015.
[9] Ashok Kote, et al, "Cloud Data Security Challenges and its Solutions", IJCCER, 2015.
[10] Pin Zhang, et al, "Access Control Research on Data Security in Cloud Computing", IEEE, Pp: 873-877, 2015.
[11] Sushil Kr Saroj, et al, "Threshold Cryptography Based Data Security in Cloud Computing", IEEE, Pp: 202-207, 2015.
[12] S. Raju, et al, "Data Security in Cloud Computing using Cramer-Shoup Cryptosystem", IEEE, Pp: 343-346, 2015.
[13] Neha A Puri, et al, " Deployment of application on Cloud and enhanced data security in Cloud computing using ECC algorithm", IEEE, Pp: 1667-1671, 2014.
[14] Mrudula Sarvabhatla, et al, "A robust ticket-based mutual authentication scheme for data security in cloud computing", IEEE, Pp: 62-67, 2014.
[15] D. Gnanavelu, et al, "Survey on Security and Solutions in Cloud Computing", International Journal of Computer Trends and Technology, Pp: 126-130, 2014.
[16] Aws Naser Jaber, et al, "A study in Data Security in Cloud computing", IEEE, Pp: 367-371, 2014.
[17] M. Sugumaran, et al, "An Architecture for Data Security in Cloud Computing", IEEE, Pp: 252-255, 2014.
[18] Manas M N, et al, "Cloud Computing Security Issues and Methods to Overcome", IJARCCE, Pp: 6306-6310, 2014.
[19] T V Sathyanarayana, et al, "Data Security in Cloud Computing", IEEE, Pp; 822-827, 2013.
[20] Huda Elmogazy, et al, "Towards healthcare data security in Cloud Computing", IEEE, Pp: 363-368, 2013.
[21] Ms. Disha H. Parekh, et al, "An Analysis of Security Challenges in Cloud Computing", IJACSA, Pp: 38-46, 2013.
[22] Du Meng, et al, "Data Security in Cloud Computing", IEEE, Pp: 810-813, 2013.
[23] Prashant Rewagad, et al, "Use of Digital Signature with Diffie Hellman Key Exchange and AES Encryption Algorithm to Enhance Data Security in Cloud Computing", IEEE, Pp: 437-439, 2013.
[24] Abhinay B. Angadi, et al, "Security Issues with Possible Solutions in Cloud Computing-A Survey", IJARCET, Pp: 652-661, 2013.
[25] Nidal M. Turab, et al, "Cloud Computing Challenges and Solutions", IJCNC, Pp: 209- 216, 2013.
[26] Ni Zhang et al, "A Research on Cloud Computing Security", IEEE, PP 370-373, 2013,
[27] Rabi Prasad Padhi et al, "Cloud Computing: Security Issues and Research Challenges", IRACST, Vol 1, Issue 2, Pp 136-146, 2011
[28] Suruchi V. Nandgaonkar, "A comprehensive study on cloud computing", IJCSMC, vol 3(4), Pp 733-739, 2014
[29] Monjur Ahmed et al, "Cloud Computing And Security Issues in The Cloud", IJNSA, Vol 6, Issue 1, Pp 25-36, 2014

[30] Yunchuan Sun et al, "Data Security and Privacy in cloud computing", HINDAWI, Vol 2014, Pp 1-9, 2014
[31] Keiko Hashizume et al, "An Analysis if security issues for cloud computing", SPRINGER, Vol 4, Issue 5, 2013
[32] Michael armbrust, "A view on Cloud computing", communication of the ACM, vol 53(4), 2009
[33] Ling Qian, "Cloud computing-An overview", springer, Pp 626-631, 2009



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY