Journal of Engineering Sciences
Vol 11, Issue 1, Jan /2020
ISSN NO:0377-9254

AN EXPLORATION OF SECURITY ISSUES FOR CLOUD COMPUTING

P. Hima Bindu[1], T. Bhaskar Reddy[2]
[1] *Sri Krishnadevaraya University, Anantapur, Andhra Pradesh, India – 515003*
[2] *Sri Krishnadevaraya University, Anantapur, Andhra Pradesh, India - 515003*

***Abstract*---- Cloud computing is a recent advancement all over the world. It is a comprehensive model, which offer access to various pool computing resources like services, applications, servers, storage, and networks on-demand. The advantages like high-performance, high computing power, low-cost of services, accessibility, scalability and availability have made cloud computing very powerful and created higher demand. The present study focus on the fundamental characteristics of cloud computing, threats, security issues and their clarifications. Though cloud computing has various advantages, data security is an important issue. Cryptography has abundant significance for providing data security database server in the cloud. We propose the reorganization of Advanced Encryption Standard, which uses 128-bit size plain text and 128-bit size key for encryption as well as decryption.**

***Keywords*----- Cloud computing, Cloud security, Security mechanisms, Security policies, Service models, Authorization, Advanced encryption, Data security, Encryption**.

1. INTRODUCTION

Cloud is a typical representation for an accessible internet organization which is hidden from users (Aguiar. et.al, 2014). The cloud computing is very much secure since it is a combination of technology which provides storage services and hosting on the internet. Public, private or hybrid are the classification of clouds (Singh.et.al, 2017). The cloud computing works without the direct intervention or control by the user and it can provide on-demand accessibility to data storage, computer system resources and computing power. Cloud computing is a novel technology for processing and transferring data (Lavanya.et.al, 2018) nowadays in almost every computer system. Cloud computing refers data centers which are available to users on the internet. It has features like resource pooling, accessibility for network, rapid elasticity, on-demand self-service, location independent. These characteristics of cloud made it a very prominent tool. Many industries and institutions are able to generate huge profits by exploiting the characteristics of cloud computing. However, maintaining the data security in cloud is a noteworthy constraint in cloud computing. Now a day's cloud security is unique prominent aspects in cloud computing because of the sensitive data from data owner (DO). In this regard, the cloud service provider (CSP) requires issues like privacy and security with high-priority.

2. REFERENCE MODEL FOR CLOUD COMPUTING ARCHITECTURE:

Below model depicts a synopsis of reference (Bayyou.et.al, 2008) architecture (NIST cloud computing) which categorizes into main services, their actions which includes their purposes in cloud (Bayyou.et.al, 2008) computing. This illustration describes the basic high-level architecture, which is proposed to help analyzing the characteristics of cloud computing, requirements, standards and uses.

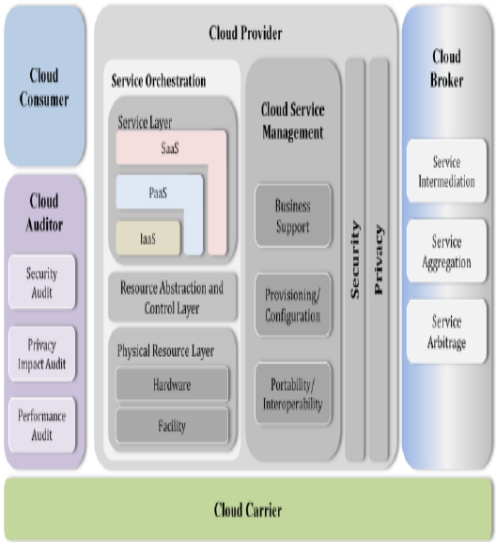

Figure 1. The Conceptual Reference Model

As presented in Figure 1, the reference architecture (Liu. et.al, 2011) NIST cloud computing (Bayyou.et.al, 2008) states five major artists: Provider, Carrier, Auditor, Broker and Consumer. An artist is an individual (a person or an organization) that takes part in a process or transaction and/or performs the task in cloud computing. The NIST clearly depicts 3 sorts of service delivery models, 5 essential characteristics and 4 deployment models that are generally acknowledged. (NIST, 2015).

3. SERVICE MODELS:

Cloud computing consists of three models, namely

- **SaaS**

SaaS gives a complete User Interface to an assistance or a complete programming application to the client. Cloud Service Providers (CSP) compose the hidden engineering like operating systems, servers, system and storage alongside application advancement and support. The End-user just uses this product and is completely oblivious of the cloud design. End-user can access such applications by means of internet browsers from work areas, workstations, PCs, and can likewise utilize the application on handheld gadgets if accessible. In SaaS clients are furnished with access to an application. They have no confinement over the system, equipment, OS or security.

- **PaaS**

In PaaS cloud administration gives devices to application advancement, application programming interfaces, software libraries and every single distinctive help required for complete application improvement. End clients figure out how to create, sending arranging and keeping up application created over the cloud. In PaaS, clients are given the equipment foundation, OS and system to create a hosting environment. After the hosting environment, the client can begin benefits and introduce his applications.

Figure 2. Software as a Service

Figure 3. Platform as a Service

- **IaaS**

Basing upon the prerequisite, IaaS gives computing and storage assets to the client. Computing and storage environment is given for all intents and purposes to the client. The extra room and registering assets, for example, RAM, processor control and so forth are overseen by the client in the virtual space. The cloud service provider deals with the hidden usage. Client can introduce any OS and applications according to need on this virtual space gave on the cloud. In IaaS, clients procure resources like CPU time, arrange data transmission, handling power and storage. When the client gets the infrastructure, then he may control the OS, application, information based security, administrations and so on.

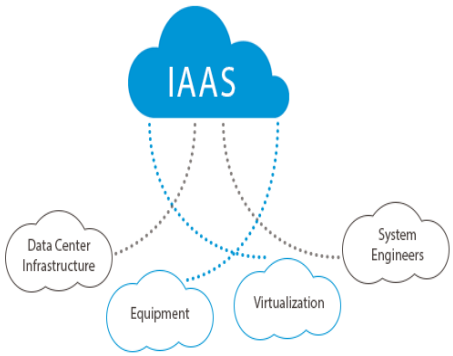

Figure 4. Infrastructure as a Service

ESSENTIAL CHARACTERISTICS

A numerous features of cloud computing are there, yet now around five principle attributes are addressed, gave by the NIST (2015): On-demand self-service: This one empowers buyers to legitimately ask for, oversee and get to the administrations over the web services and the executives interfaces with no human association. Accessibility for broad network: The information as well as administrations remain open in the cloud and must be available over any standard gadget alike cell phones, work area, PC. These gadgets work over some standard conventions and innovation. The strategy of processing a cloud has to handle all the standard protocols completely. Pooling of a resource: The cloud provider gives either physical computing resources or virtual computing resources that are common amongst different clients. These resources are assigned powerfully in a multi-occupant condition. Rapid elasticity: Elasticity is a fundamental feature of any cloud. Utilizing these properties mounted by the consumer requirements. Customers have infinite resources, which are able to be obtained as required in a compensation for every utilization. Measured service: According to the compensation per-use administration, the metering ability of the cloud framework automatically exchanged and ascended the resources.

4.DEPLOYMENT REPRESENTATIONS:

Private cloud: The cloud framework works for a private association. An establishment utilizes it or an outsider and may be present either on-premise or off-premise.

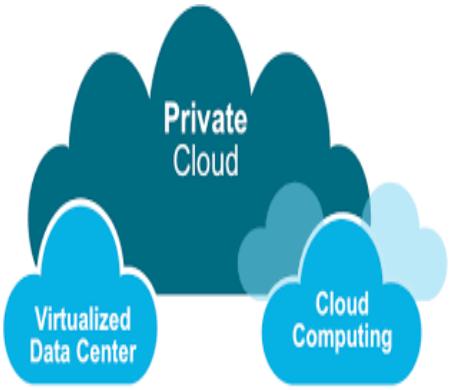

Figure 4. Private Cloud

Community Cloud: Several associations share the cloud foundation and support a particular network that has regular concerns. Associations oversee network cloud and exist on-premise or off-premise.

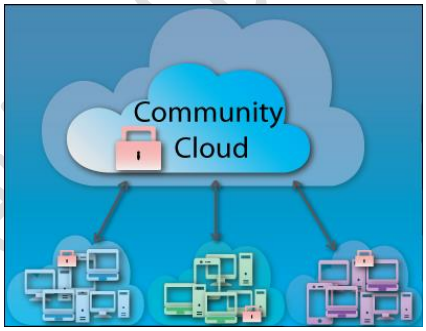

Figure 5. Community Cloud

Public cloud: The open or a huge industry gathering can get to this cloud framework and is constant by an association selling cloud services.

Hybrid cloud: The cloud infrastructure is an arrangement of one or different clouds (private, network, or open) that stay specific units yet are inevitable together by institutionalized or else enlisted innovation that grants information and more application compactness.

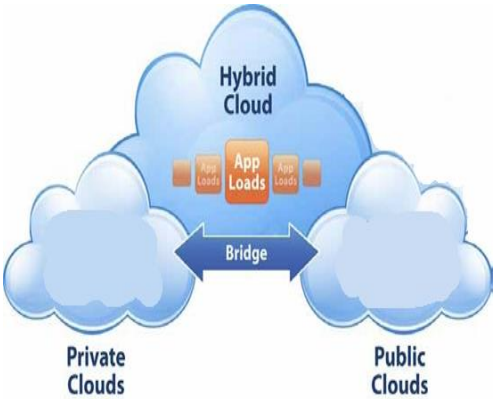

Figure 6. Hybrid Cloud

ADVANTAGES OF CLOUD COMPUTING:

High-performance cloud computing: Is a sort of cloud computing arrangement that incorporates models, methodology and components from distributed computing. HPC2 characterizes the strategies for finishing processing tasks that match the speed of supercomputing from a cloud computing architecture. The total arrangement may contain storage, hardware, and application software gives through the cloud on an on-request premise. Low Costs is allowed after capital consumption. Cloud computing do not spend huge expenses on tools. Availability: Several cloud providers are really dependable in contributing their services, with accuracy. Flexibility: Cloud computing provides an adaptable facility in which it moves up or down as per the constraints of the client.

Security

Security issues for cloud computing has various security issues in such a way that it incorporates numerous innovations such as systems, DB(Databases), OS(Operating System), virtualization, scheduling the resources, exchange the board, load balancing, concurrency control and storage organization. The Cloud Service Provider for cloud guarantees that the client does not drive against any dispute, for instance, damage of information or information theft.

Information Security assumes a critical job in the advanced time. Nonetheless, the information (Jakimoski, K. 2016) stored in internet clouds of different industrial servers, still we have the issues of information theft and fake activities, which draws out the advancement of versatile and novel procedures for better information security in verifying and giving extremely high protection to the information stored in single servers. We apply Data security for improving security. Certain sorts of issues arise even though observing the security of a cloud.

Sensitive data in a cloud computing environment develop as critical matters about cloud-based systems security. When data exists in cloud, people all over the world can access the information by opening the cloud, subsequently data might be shared, private and delicate information in a cloud. Along with these here is a requirement (Kumar.et.al, 2019) for data integrity in cloud computing. Data theft is a serious one of the issue in a cloud computing environment. The data can be lost, harmed, or debased because of, cataclysmic events, and fire. Information location is one of the issues that require effort in a cloud computing environment. The physical area of data location is basic plus crucial. It must to be open to the client. The Cloud Computing Service Provider has to give assurance for client for their individual data is secure from different Providers. Cloud Service Provider should be reliable such that it empowers the supplier to ensure the client's individual information, who is receiving the information and who is holding the server with the goal. In Cloud Computing, the Security come at two levels. One is on the provider level, and alternative is taking place at the client level. From the cloud computing Service Provider client receives the security layer, and the client must guarantee that there may not be a loss of information or stealing or changing of information for new clients who are utilizing a similar cloud because of its activity.

Cloud security

Cloud security is a piece of computer security. It portrays strategies, innovation, and mechanism that are useful to secure the information and facilities. The threats and attacks straightforwardly or by implication affects the cloud framework. Integrity plus availability as well as confidentiality of the cloud resources are features. In this segment, it is meant to investigate a few security ideas, for understanding the cloud security issues.

Cloud security ideas

To know security issues (Singh.et.al, 2017) first, it is indispensable to comprehend the fundamental idea of cloud computing. Cloud security insurances different security issues and dangers. The paper provides various security issues and threats to comprehend the idea of security for a cloud. This area talks about few ideas like virtualization, multi-tenancy, cloud platforms, information re-appropriating, data storage, and trust management, for comprehending the security issues in a cloud.

Virtualization

Virtualization referred as an intellectual process in which services, computing resources, operating system and applications

are extracted from the hardware they run on. The components of virtualization are VM and VMM. A Guest OS is a replica of application software nothing but a virtual machine and acts as a host OS besides it has the power to control several programs running on it but it does not offer hardware for direct access. This resource is available by Virtual Machine Managers, which are responsible for sharing the virtual hardware resources like hard disk, CPUs, memory and network for each Virtual Machine. If a Virtual Machine requires hardware resource then sends a request to Virtual Machine Managers, a replica of that resource is created quickly and allot that resource to the requested Virtual Machine. Virtual Machine Managers is furthermore responsible for connecting multiple Virtual Machines. Finally, Virtual Machines are connected with virtual switches, external as well as internal networks. Some of the virtual features are VMware and vSphere. Virtual Machines Managers controls the process of construction, deduction and distribution of the virtual resources towards the Virtual Machines, that supports the cloud computing features like elasticity etc. Various open Virtual Machine Manager solutions build in VMware Player, Xen, Oracle Virtual Box.

Further commercial paid Virtual Machine Managers like Citrix XenServer, Oracle VM Server, Virtuozzo Parallels Desktop and VMware Workstation and vSphere. The key feature of the Virtual Machine image is preparing the clones, and it can rapidly exchange from one to another place, which are easily retrieved. Cloud provides high available and scalable services to their clients.

Multi-tenancy

Cloud computing environment has multi-tenancy feature that involves sharing of running instances with single or multiple users, which are termed as tenants. It allows multiple users to segment a single cloud platform. Observe an IaaS provider, in which Virtual Machine Managers are mentioned as multi-tenancy distribution policy while Virtual Machines refers to examples. Now observe a Platform as a Service provider in a multi-tenancy environment, Virtual Platform (VP) permits the customer to run numerous requirements like JVM and .NET. If Customer secrete information or data is located at same physical location then multi-tenancy develops in the methods of co-location, co-tenancy, and co-residence attacks. As a result, the attacker can have the right to use neighbor Virtual Machines or applications that are running currently. Accessing various resources has the result of DoS attack, which is additional issue. A human threat is a malicious insider act in place of cloud provider and exists as third party agents, who are functioning in the cloud provider organization. The attack is extreme as they get the accessibility to cloud consumer IT resources.

5.CONTROLLING THE SECURITY

Here the security controls describes countermeasures (Liu.et.al, 2015) for reducing risks. These security controls react to security threats and help to prevent them. The security countermeasures list, the way to access those things and relevant information are given in the security policy. Security policies have group of security rules and applications that have the implementation of security controls in the security plans. The security controls assist users in attaining security of sensitive data at the maximum level.

Security mechanisms

Frameworks with credential data can protect the IT resources, valid info as well as facilities are security mechanisms. For enhancing the security of the system, countermeasures and safeguards are described in security mechanisms.

Security Policies

It is a mechanism with a setup of security instructions and guidelines in security system. It defines implementations of rules and regulations. Example, security policies are useful for knowing the location and accessibility of security mechanisms and controls.

Security services

Fora3 the protection of IT assets cloud security services are collected which are sophisticated techniques. Cloud security (Sood, 2012) services are defined by IT security measures. These services enable users to know the need for security. Essential cloud security services are described below.

Confidentiality is the first security service, defined as only authorized parties or systems have permission for the accessibility of IT

resources. As the number of tenants, devices, and applications increases, the number of access points and threats also increases. In cloud data confidentiality is interconnected with the authentication of user, in such a way that it protects user resources from unauthorized access. Security for the user account from theft is a complex problem and controlling the accessibility of the objects, including software, device, and storage. Integrity is referred as a characteristic in which modification of data has not been done. The alteration of software or hardware or the alteration of data is available only to the authorized party in an authorized approach. The indicated service is accomplished only in keeping IT assets free from omission, alteration, or creation from unauthorized persons. A procedure of confirming an organization or institution or person that whether it supports the principals given to it or not is called authentication. The objective of authentication attack is the verification of their identity, which acts as a legitimate user. Secure authentication is the primary requirement for restriction of unauthorized entrance as well as preserving the confidentiality of consumer financial records on a cloud. Authentication can be compromised with a weak password, method of easy retrieval and apprehensive registration process. In order to overcome this problem, i.e. authentication and authorization, authentication is done first followed by authorization. The inefficient authorization, credential prediction, session completion, and session fixation leads to the get usage of preserved areas above their boundaries. Cloud computing (Thilakarathne.et.al, 2014) has the feature called high availability in which application downloading time is minimized and prevents business disruption. Every IT resource is usable and accessible within the time allocated to it, and it is one and only characteristic of cloud computing. The cloud provider and cloud carrier both can control the cloud environments availability with IT resources.

Cloud platforms

Cloud platforms provide the tools which are essential for building SaaS applications. Here the cloud users arrange their applications and services to the cloud and require few functioning frames that are useful for the deployment of user's applications. For the development of cloud applications, these platforms provide APIs and IDE. All the tools which are provided by these platforms rely on the infrastructure of the platform and respective programming languages.

Trust management

In cloud security, trust is the keynote which is non measurable parameter. This trust is assigned to hardware, data center, self-infrastructure, and network configuration created on the assurance of the decisions taken. Various factors are focused on the trust evaluation process like multi-phased and multi-faced phenomena. Therefore, trust is extremely unpredictable and robust in nature. Due to the data and services of the customer which are located in remote location trust issues are raised in the cloud computing and are handled by a second or third party.

Identification of unique security threats is the most challenging issue at the implementation phase in an IS. Standard security system designing process aims at the identification of security threats followed by finding the security requirements and applies security controls for achieving the high reliability, supportability and maintainability. The building blocks of any security system design has confidentiality, integrity, and availability. These critical security aspects are correlated for completion of a secure cloud. Various security advantages are provided by the cloud architectural design such as high availability, redundancy, data segmentation, centralization and process segmentation.

Requirements of cloud security

Cloud security (Jakimoski, K. 2016) requirements are described in this session. Each business organization selects few security strategies before accessing any of the services. Six security requirements (Thilakarathne.et.al, (2014) are there: authorization, integrity, authentication or identification, confidentiality, availability and non-repudiation. Every model of service requires authorization for public cloud to exclude unauthorized access. More security is provided by the hybrid cloud when linked with the public, and private cloud. Almost all models for security in cloud requires an important requirement called integrity for checking the data correctness. Security for the web and service-based accessible applications are provided by with SaaS

security models. Reliable security mechanisms are requirements in place of high availability as well as integrity of the services in the underlying network.

Storage models

These storage models deal with data storing in the cloud depending upon the availability of storage space. Various storage solutions are provided by the cloud environment. Every solution has its limitations as well as benefits constructed with respect to the requirements, and available data (Rong.et.al, 2013) consumer selects the required storing system.

Standardization and security

Open System Interconnection (OSI) model has a few security components usage, for example, advanced mark required for honesty checking, validation instruments for control information get to and bounteous security conventions. The association gives an elevated level certification to their clients, for this organization certificate authority called International Organization for Standardization (ISO). In the cloud, information handling is an essential errand due to cloud hold large measures of information. Moreover, reliable information stockpiling is another viewpoint. The support approach is additionally required. Mists spread the information into various server farms, and even the cloud supplier is the equivalent. This instrument gives geological repetition to information, implying that a duplicate of this information can be situated in numerous server farms to keep away from a single purpose of disappointment. A file comprises of information that is in envelopes, which are pooled among different clients/has utilized the Internet. Numerous client's entrance the files through standard conventions or capacities.

Database or Table storage system

Numerous enterprises put away their information as Relational Database or Relational Database Management System, consequently they put away as row and column. In the RDBMS, we kept up data integrity and maintain a strategic distance from information repetition. Scaling and execution remain as fundamental issues which are cloud based.

Roles and boundaries of cloud

The cloud gives different sorts of predefined jobs. The accompanying subsection depicts every member job and obligations and in what manner they collaborate through the cloud. Cloud provider alludes to an individual or association that executes cloud assets. The essential duties of the cloud provider are to make and give cloud administrations to the cloud clients, as indicated by SLA ensures. A cloud consumer is a human or an association that devour the cloud IT assets through the cloud provider. A cloud customer or supplier together remain as cloud service owners. The cloud service owners alluded to an individual or association that lawfully possesses a cloud administration. The individual or association that performs organization task for administrations which are depend on cloud, containing cloud assets recognized as the cloud resource administrator.

6.CRYPTOGRAPHY

The specialty of keeping data by changing it into a confused format called cypher text and who possess a secret key to have the option to decode the message into plaintext. In computing, encryption is the system by which plaintext or any new kind of information is transformed from a reasonable structure to an encoded structure that ready to be decoded uniquely by another element if they have the right to use a decryption key. Encryption is one of the essential technique planned for assigning security for information, particularly for a start to finish the security of transmitted information through systems. Encryption is usually utilized on web for securing customer data shared among a program and a server, containing pwds, installment data and additional related data must be viewed as secretive.

Working Principle of Encryption

Decoded information, now and again referred, such as plaintext, is scrambled by utilizing an encryption design and an encryption key. This system produces cipher text that must be seen in its unique structure whenever decoded with the right key. Decoding is the exact inverse of encryption, following comparable advances; nevertheless, it utilizes the keys backwards. The present best-utilized encryption algorithms are two classes: symmetric and asymmetric.

Symmetric-Key Algorithms

These utilizes the secret key for encryption and decryption. Similar mails are available for encryption by the sender and decryption by the receiver. It covers algorithms such as Advanced Encryption Standard (AES), Data Encryption Standard (DES). Symmetric-key encryption remains as quicker Encryption Algorithm. On the other hand, the sender needs to trade the key used to encode the data with the receiver before the receiver can perform decryption on the cipher text. The necessity to safely disseminate and oversee vast quantities of keys involves maximum cryptographic procedures utilize a symmetric algorithm as an occupation to encode data.

Asymmetric-Key or Public Key Algorithms

Asymmetric algorithms utilize various keys. One key (open) is for encryption and other (private key) is utilized for decoding. It has algorithms like Rivest, Shamir, & Adleman (RSA), Digital Signature Algorithm (DSA). In this, the reorganization of AES abbreviation of Advanced Encryption Standard, which is a Symmetric Encryption Algorithm. The AES (Advanced Encryption Standard) is a symmetric block cypher distributed by the National Institute of Standards and Technology (NIST) and began improvement of AES in 1997 when it expressed the requirement for descendant algorithm for brute-force attacks.

This novel, Advanced Encryption Standard Algorithm must be equipped for ensuring delicate government data well into the following century. It is expected to be anything but difficult to execute in hardware and software as well as in limited conditions and offer significant safeguards against various attack techniques.

7 .CONCLUSION

Since the most recent ten years, cloud-based business opportunities are growing rapidly. On the other hand, the cloud risk range also increased rapidly. This review surveys the cloud architectural components, cloud services deployment models, cloud security concepts and cloud-security requirements, This survey gives couple of perspectives on security, privacy to a distributed computing framework and depicts cloud jobs and limits along with Storage models. Encryption is usually utilized on the network for securing client data shared amongst a program and a server, containing PINs, periodical data and other discrete files that must be considered as secretive. AES, which is Advanced Encryption Standard Algorithm, is capable of ensuring delicate government data. For cloud computing environment, security countermeasures ought to be executed in a self-versatile way. The statically opted security mechanism will not be adequate and sufficient to address developing threat vectors. In this way, cloud security, for Cloud Computing frameworks is by all aspects an energizing region for future research that can empower the safe and imaginative business administration contributions from the cloud provider to use mechanical development of Big Data, 5G, NFV SDN, and IoT, based applications and administrations.

REFERENCES

[1] Aguiar, E., Zhang, Y., & Blanton, M. (2014). An overview of issues and recent developments in cloud computing and storage security. *High Performance Cloud Auditing and Applications* (pp. 3-33). Springer, New York, NY.

[2] Jakimoski, K. (2016). Security techniques for data protection in cloud computing. *International Journal of Grid and Distributed Computing*, *9*(1), 49-56.

[3] Kumar, R., & Goyal, R. (2019). On cloud security requirements, threats, vulnerabilities and countermeasures: A survey. *Computer Science Review*, *33*, 1-48.

[4] Lavanya, K., Hari, C,B., & Bhaskar Reddy, S. T. (2018). Data Security Using Nested Randomization and Lossless Compression Techniques. *International Journal of Applied Engineering Research, 13(15), 12373-12378.*

[5] Liu, F., Tong, J., Mao, J., Bohn, R., Messina, J., Badger, L., & Leaf, D. (2011). NIST cloud computing reference architecture. *NIST special publication*, *500*(2011), 1-28.

[6] Liu, Y., Sun, Y. L., Ryoo, J., Rizvi, S., & Vasilakos, A. V. (2015). A survey of security and privacy challenges in cloud computing: solutions and future directions. *Journal of Computing Science and Engineering*, *9*(3), 119-133.

[7] Rong, C., Nguyen, S. T., & Jaatun, M. G. (2013). Beyond lightning: A survey on security challenges in cloud computing. *Computers & Electrical Engineering*, *39*(1), 47-54.

[8] Singh, A., & Chatterjee, K. (2017). Cloud security issues and challenges: A survey. *Journal of Network and Computer Applications*, *79*, 88-115.

[9] Sood, S. K. (2012). A combined approach to ensure data security in cloud

computing. *Journal of Network and Computer Applications*, *35*(6), 1831-1838.
[10] Thilakarathne, A., & Wijayanayake, J. I. (2014). Security challenges of cloud computing. *International Journal of Scientific & Technology Research*, *3*(11), 200-203.

AUTHOR PROFILE

P. Hima Bindu is a fellow Researcher in the discipline of Computer Science and Technology at S.K University, Anantapur, Andhra Pradesh. She has completed her graduation and as well as post-graduation from JNTU affiliated colleges Ananathapuramu. She has 4 years of experience in teaching. Her areas of interest are Cloud Computing, Information Security and Image Processing.
E-Mail:himabindu747@gmail.com

T. Bhaskara Reddy is a Professor in the department of Computer Science and Technology at S.K University, Anantapur A.P. He holds the post of Deputy Director of Distance education at S.K. University and He is the CSE Coordinator of Engineering at S.K. University. He has completed his M.Sc and Ph.D in computer science from S.K. University. He has acquired M.Tech from Acharya Nagarjuna University. He has been continuously imparting his knowledge to several students from the last 17 years. He has published 68, National and international publications, 10 International conferences. 13 National conferences. One UGC Major Research Project. Attended several seminars in 3 countries. He has completed major research project (UGC).
E-mail: bhaskarreddy.sku@gmail.com