In Retrospect of Cloud Security Issues

Jvs. Arundathi, K.V.V.Satyanarayana

Abstract -Popular computing technologies like Distributed ,Parallel ,Grid etc., have already reached their peaks in providing services and now a hybrid aspect is capturing the focus which is a combination of traditional computing technology and network technology and termed to be "Cloud Computing ".A desperate demand for data sharing and handling enterprise applications have called upon for cloud computing .A blocking wind for leveraging cloud computing technology is the aspect of security .But the passion towards adopting cloud have overridden the security threats. This paper glances over various security threats, risks, challenges along with their resistance capabilities to overcome the vulnerabilities in the cloud and also some of the encryption techniques that are used in the cloud.

Keywords: Encryption, Threats, Attacks ,cloud computing

I. INTRODUCTION

According to NIST "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". In addition it has some other advantages like contributing low cost infrastructure ,flexibility ,scalability, collaboration and ease of use and also on-demand access from anywhere through the internet is being used by commercial entities and also by conventional users.

Characteristics of cloud computing

As stated in NIST definition ,the cloud computing services have some aspects : Broad Network Access ,On-Demand Self Service, Rapid elasticity, Measure Service Resource Pooling[1][15] As per NIST cloud computing is described using four Deployment models and three service models

Deployment Models : There are four Deployment models in cloud[11][13].

A. **Private Cloud** is used with in the organization and its services and data cannot be accessed from the outsiders of the organization
B. **Public Cloud** has mega scalable infrastructure. It is retained and organized by academic, government or business organizations which provides services of the cloud open for the use of public.
C. **Hybrid cloud** is a combination of both private and public cloud usually private for sensitive data and strategic applications
D. **Community cloud** has a framework and services that can be provisioned for the use of specific community of the customers.

<span>Revised Manuscript Received on December 30, 2019.</span>
* Correspondence Author

Jvs. Arundathi*, Phd Scholar, Department of Computer Science and Engineering, Kl Deemed to be University, Guntur, India.
Dr. K. V. V. Satyanarayana, Professor, M. Tech Coordinator, Department of Computer Science and Engineering, Kl Deemed to be University, Guntur, India.

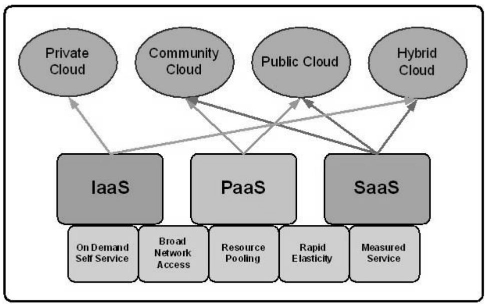


Figure 1: Cloud deployment model

Cloud service models

There are three types of service models in he cloud environment. User can select any one of the three services[10][13] based on their need ,They are:

A. **SaaS(Software as Service)**: It is giving the ability to remotely use the software and its services on demand through the internet .It purges the huge responsibility of organizations such as setup, handling the installations, maintenance , and daily preservations. Ex: Face book, Whatsapp, Gmail etc.
B. **PaaS (Platform as Service)**: it can be described as application development environments offered by the cloud provider as a service. It is the ability to deploy the user application on to the clouds infrastructure of provider. The development execution environment should be programming language, operating system and database. Example: Google App Engine.
C. **IaaS(Infrastructure as Service)**:It provides the infrastructure such as hardware, servers, router ,storage and other modules of the networking to the users.

Figure 2 : Cloud Service models

The remaining paper is organised into sections. Section II discusses The cloud architecture, section III surveys various security open issues and threats,

section IV reviews security techniques ,section V describes existing security algorithms . Finally section VI concludes the paper and future research scope.

II. CLOUD ARCHITECTURE

Cloud computing is a pool of resources which can be availed on demand based. It is available over the internet in a self service model without the service provider interaction

Cloud provides various products and services with technical , innovative opportunities. As per NIST's cloud computing reference architecture[2] there are five important actors[2] that can be influenced by cloud computing along with its security implications.

A. ***Cloud Consumer*** – An organization or a person that maintains a business relationship with , uses services from cloud providers

B. ***Cloud Provider*** – An organization or a person or entity responsible for making a service available to interested parties.

C. ***Cloud auditor-*** A party that can conduct independent assessment of cloud services. information system operations , security and performance of cloud implementation

D. ***Cloud Broker*** – An entity that manages the use, delivery and performance of cloud services and negotiates the relationship between consumers and providers of the cloud.

E. ***Cloud Carrier-*** An intermediary that provides transport and connectivity of cloud services from the cloud providers to cloud consumers [2]

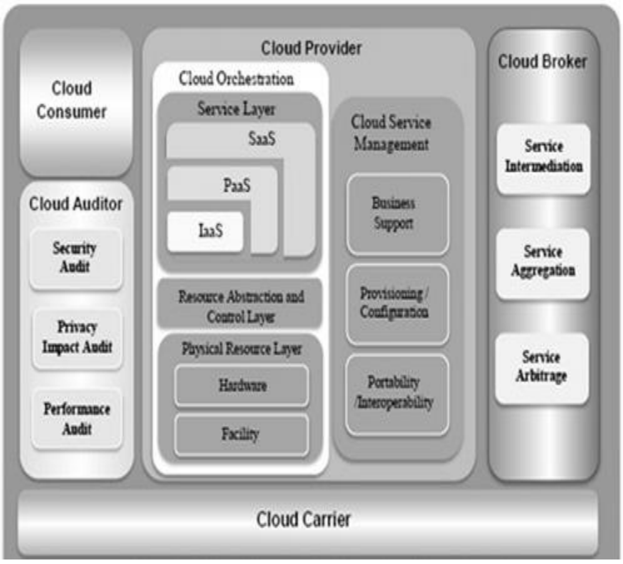


Figure 3: NIST reference cloud architecture[2]

III. SECURITY OPEN ISSUES AND THREATS

The adaption of cloud has been reached to the peak point and it is expected that more workloads will move to cloud from traditional local storage, ranging from the internet users to commercial organizations. While there are many security problems to be identified and analysed in various aspects like 1) Privileged User Access Management 2) Regulatory Compliance 3) Data Location 4) Data Segregation 6) Data protection and recovery support 7) Long Term Viability 8) Investigative support.

Cloud computing provides many benefits on other side it suffers from security issues which cannot be ignored. In the recent report of ENISA , thirteen technical risks were identified

As per NIST's report cloud computing is facing some security challenges which are resulting from the cloud's wide range of outsourcing , Network Dependency, multi tenancy ,and scalability.

Fernandez et.al.[3] [6]provided complete retrospect of the research literature to define security challenges and open issues of cloud.

Main security challenges are

- Shared technologies vulnerabilities
- Data breach
- Account or service traffic hijacking
- Denial of service (DOS)
- Malicious insiders

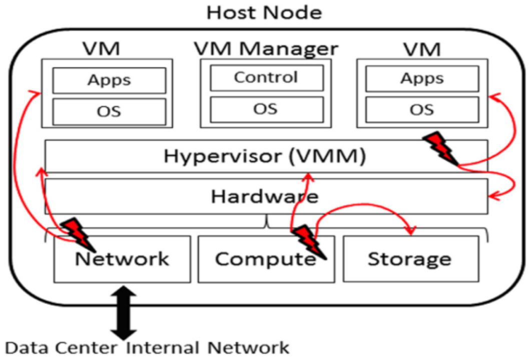


Figure 4: cloud platform attack vectors[6]

The above mentioned open issues can be generated by three main vectors of attack : Hypervisor ,Computing Hardware and Network[12] and the various attackers are internal users, External users and cloud provider (malicious employee)

Network is one of the most important vector in cloud platform with which the application can run

Hypervisor: It is a program that can enable you to host various distinct Virtual machines on a single hardware. The Hypervisor is also known as Virtual Machine Monitor(VMM).The Hypervisor presents the guest operating Systems with a virtual operating platform and it handles the execution of the guest operating systems. Hypervisor is the fundamental part that guarantee the multi tenancy feature in the cloud computing, The memory bus, disk bus, data and instruction caches and other VM instances are some of the physical recourses.[6]

External users can attack against the cloud infrastructure through the network. They can effect data confidentiality , integrity by tampering the communication channels. They can effect the availability of cloud provider data centres.

Internal Users (owners of VM instance) can exploit the hypervisor to attack another VM instance which is by the multi tenancy feature ie both the invader and the victim share the same host ,which can breach the confidentiality of sensitive information[6]

The Cloud provider[8] itself might be an attacker. The employees could exploit their privileged position to steal the sensitive user information either by logical or physical manipulation of hardware platform .

Table 1: [4] Cloud threats and attacks

	TYPES	EFFECTS	SOLUTIONS
Threats	Distinct service receiving/delivery model	Control loss of cloud infrastructure	Contributing the monitoring and controlled services
	Misuse of cloud computing	Loss of validation, attack due to unidentified sign-up ,deceit service	Provide secured registration and verification mechanisms by observing the status of the network
	Unsure API and interface	Imprecise validation and verification, data breach	Use encryption during data transmission, robust access control and verification methods
	Harmful insiders	Permeating resources, demolishing the assets, productivity loss, etc..	Notify the breaches, report the agreement ,use the transparent security management technique
	Issues due to Shared technology	Obstruction of user services by negotiating hypervisor	For administrative task use strong verification and access control methods, Audit vulnerability and configuration
	Leakage and Loss of Data	Destruction, corruption, modification or deletion of sensitive data	Provide data backup and storage techniques
	Hijacking of Account /Service	Hijacking user credentials, cloud critical area access, conceding the service security to the attacker	Following the substantial verification mechanisms, secured policies, and secure link.
	Delineation of Risk	Policies, operations related to internal security, etc..	Using monitoring and altering system to secure the data
	Piracy of Identity	An intruder can get identity of the valid user and misuse that.	Using robust multi-tier passwords and verification methods
Attacks	Zombie attack(DoS/DDos)	The availability of service may be affected	Robust verification and validation
	Service Injection	The integrity of the Service will be distressed, instead of valid service malicious service will be provided	Robust isolation mechanisms between VMs, To check service integrity use hash function
	Attack on Hypervisor /Virtualization	Access the user credentials and control	Need security solutions of a hypervisor, monitor its activities, VM isolation needed
	Attacks from user to root	Affect the privacy of user's sensitive information and services	Use robust password, better verification mechanisms
	Port Scanning	Abnormal behaviour of the service, service availability is affected	Required robust port security
	Man_in_the middle	The security and privacy of the data is invaded	A proper (SSL)secure Secure Socket Layer architecture is required
	Metadata Spoofing	Abnormal behaviour of the service, privacy of the service may be affected	The functionality of the Service and other details should be encrypted, robust verification mechanism is needed to access the required file
	Phishing	The privacy of the user credentials will be affected	Use HTTPS
	Backdoor Channel Attack	Affects the availability of service , data privacy	robust verification, and isolation mechanisms are needed

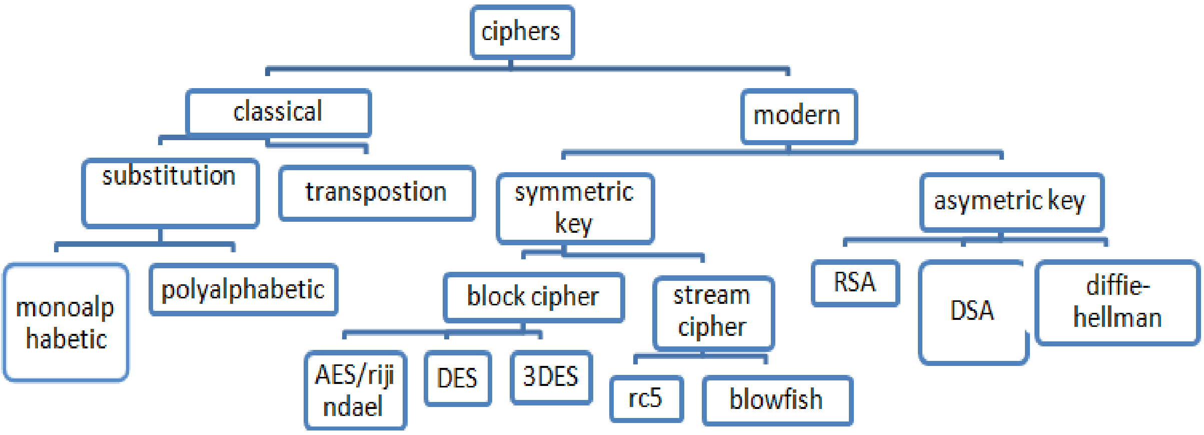
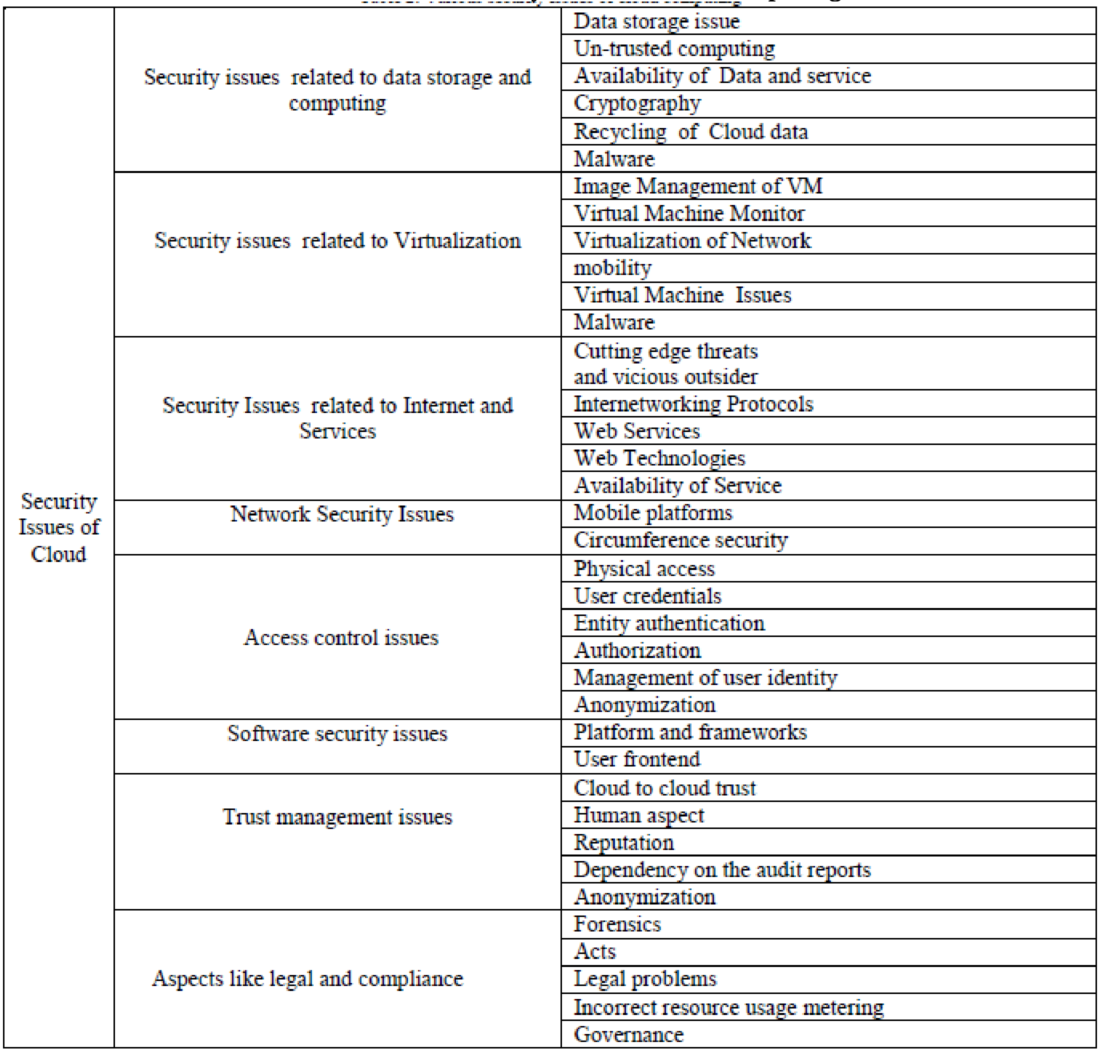


Figure 5: classification of encryption methods

Table 2: Various security issues of cloud computing



Security Issues of Cloud	Security issues related to data storage and computing	Data storage issue
		Un-trusted computing
		Availability of Data and service
		Cryptography
		Recycling of Cloud data
		Malware
	Security issues related to Virtualization	Image Management of VM
		Virtual Machine Monitor
		Virtualization of Network
		mobility
		Virtual Machine Issues
		Malware
	Security Issues related to Internet and Services	Cutting edge threats and vicious outsider
		Internetworking Protocols
		Web Services
		Web Technologies
		Availability of Service
	Network Security Issues	Mobile platforms
		Circumference security
	Access control issues	Physical access
		User credentials
		Entity authentication
		Authorization
		Management of user identity
		Anonymization
	Software security issues	Platform and frameworks
		User frontend
	Trust management issues	Cloud to cloud trust
		Human aspect
		Reputation
		Dependency on the audit reports
		Anonymization
	Aspects like legal and compliance	Forensics
		Acts
		Legal problems
		Incorrect resource usage metering
		Governance

Table 3:Security challenges and risks

Threats	Description of Risk
DoS	In this attack, the invader will perform flooding on the server to make the services and/or resources to be unavailable to the users of the cloud.
DDoS	A Distributed DoS attack is an attempt to generate services that are unavailable by devastating it with traffic from various machines that are scattered over theInternet.
MitM	A Man-in-the-Middle attack is a type of eavesdropping attack where an invader involves himself in a communication between two parties, steals important information from the users, and then passes to the third party.
IP Spoofing	IP Spoofing is a process to gain access to the server in unauthorized manner ,thereby an intruder unjustifiably impersonates the IP address of trusted host to conceal his identity.
Packet Sniffing	The analyzer or Packet Sniffer is used to determine the problems related to network.. However, an intruder can capture and analyze all transmitted sensitive information and also he can use it.
Port Scanning	Attacker sends queries to search for vulnerable ports on the server and attempts to identify kind of used service.
Session Hijacking	An attacker can hijack an active session and masquerade as one of the conversation parties.
Phishing	Phishing is the attempt to steal sensitive user data such as credit card details and passwords, usernames.

IV. SECUTIRY TECHNIQUES

In the present era various number of applications are relying on internet such internet banking ,online shopping , digital bill payment, stock trading etc., All these public networks need to have the end to end connection in a secured manner which should also be confidential in order to ensure data authentication, confidentiality ,availability integrity as well as accountability.

“As per NIST computer security can be defined as the protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity ,availability of confidentiality of information system resources”(inclusion firmware, hardware, software, data /information and tele-communications)

Security is the process of protecting the services and information from an unauthorised access, modification or destruction. In networking the security can be obtained by using cryptography (one of science and art) is of transforming the messages so that they can be protected by attacks.

Encryption: is one of important mechanism which can ensure the security of sensitive information. The encryption algorithms are classified into two groups: asymmetric key(public key) and symmetric key(secret key) and [5][7][9]

Symmetric key: is also known as conventional encryption, is a form of cryptosystem in which encryption and decryption performed using the same key[5][7][9]

Asymmetric encryption : In which encryption and decryption are performed using different keys ie., public key, private key[5][9].

V. EXISTING ALGORITHMS FOR SECURITY

In data communication encryption plays a major role to secure the data. The encryption algorithms[7][14] used in cloud computing are

A. Symmetric encryption algorithms:

In this method sender and receiver use a single secret key which is used to encrypt and decrypt the messages. Some of the encryption algorithms are

a) ***DES(Data Encryption Standard***): It is a symmetric key algorithm used to encrypt the information. It was developed by IBM in 1975. In DES algorithm block cipher is of 64bits and key is of 56bits. Now a days this algorithm is insecure for lots of applications.[5][14]

b) ***3DES(Triple Data Encryption algorithm*)**: It is developed to overcome the flaws of DES without designing a new crypto system. It was developed by IBM in 1978. 3DES extends the key size of DES by applying the algorithm 3 times in succession with 3 different keys. The combined key size is thus 168 bits(3times to DES(3*56)).TDEA uses three 64bit keys K1,K2,K3 in Encrypt-Decrypt-Encrypt(EDE) mode. 3DES is slower than other block cipher methods.[5][14]

c) ***AES(Advanced Encryption Standard)*****:** Is one of the new encryption standard recommended by NIST to replace DES in 2001. The AES can support any combination of data (128bits) and key length of 128,192 and 256 bits. During encryption and decryption process AES goes through 10 rounds for 128 bit keys, 12 rounds for 192 bit keys and 14 rounds for 256 bit keys to deliver final cipher text. The draw back of this algorithm is difficult to implement.[5][7]

d) ***Blowfish*****:** It is a symmetric key algorithm designed by Bruce Schneier in 1993. It is a basic algorithm developed an option to DES algorithm to overcome many problems that come with many other algorithms. This algorithm is available in public domain. And can be available to free to every one.[7].The key size is 32-448 bits and 16 rounds.

e) ***RC5(Rivest Cipher*****)**: It is a symmetric key algorithm. Mainly known for its simple execution. This is developed by Ronald Rivest in the year 1994. The speed of algorithm is slow comparative to remaining algorithms

B.*Asymmetric Algorithms*:

These are public key algorithms which generally make use of different keys for encryption and decryption. These algorithms are most important because these can be used for transmission of encryption keys.

a) ***RSA (Rivest-Shamir-Adeleman)*****:** Is the most simple and common asymmetric algorithm used for both encryption and decryption of digital signature. It has fast encryption key[5][14. It was developed by Ronrivest,Adi shamir,and Leonard Adleman in 1978.

b) ***DSA*** **:** It is an important algorithm for processing the digital data. It was given by the NIST in 1991.

c) ***Diffie-Hellman*** **:** It is the earlier asymmetric data standard algorithm developed in the year 1976. This algorithm most widely used key exchange algorithm[14]

VI. RESULT ANALYSIS

Table 4: comparison of performance of various algorithms[19].

SNO	Algorithm	Key size(bit)	File size(bytes)	Avg Encryption time(msec)	Avg Decryption time(msec)
1	AES	256	329	287	293
			778	299	304
			2048	300	297
2	BLOWFISH	128	329	293	290
			778	287	278
			2048	283	279
3	DES	56	329	284	280
			778	292	282
			2048	303	317
4	RC4	64	329	282	286
			778	283	280
			2048	313	292
5	RSA	1024	329	462	499
			778	541	450
			2048	488	491

The experimental result for some of the encryption algorithms like AES,Blowfish,DES,RC4 and RSA have been implemented on several file sizes:329,778 and 2048 bytes respectively. The encryption and Decryption time are calculated in milliseconds and input size is taken in kilo bytes

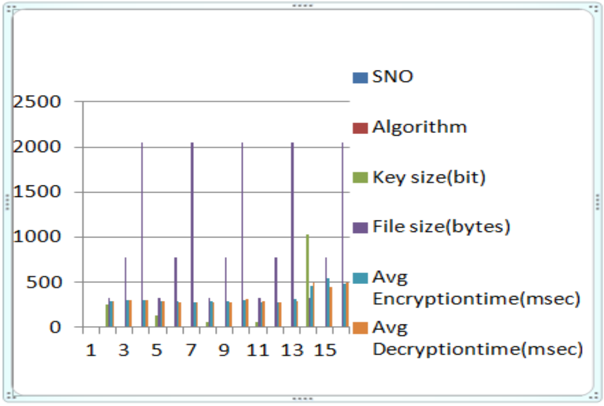


Figure6: Encryption time of different algorithms[19].

From the above figure we can conclude that the asymmetric encryption /decryption techniques are slower than the symmetric encryption /decryption techniques. All the algorithms except DES and RSA algorithms there is a proportion relation between input file size running time. As the input file size increases the running time of DES and RSA changes slightly. Compare to all the algorithms RSA will take more time for both encryption and Decryption.

VII. CONCLUSION

Cloud computing provides a various assets of cloud services and resources in various fields. However Cloud security issues linger the extensive obstacles that may hinder the massive adoption of cloud computing. Security engineering is one of the best practices to provide the best mechanisms and approaches for establishing services and systems for sustainability, security and resiliency. In this paper the overview of various security threats, attacks with solutions, security issues , challenges , risks and some of the encryption techniques were also discussed, which are facing some problems regarding speed and key length. It can be solved by using some hybrid techniques. As cloud services have huge number of domains, deployment models and respective algorithmic approaches since there is a problem in cloud security to avail the services (storage, infrastructure etc.)there is a huge scope for research.

REFERENCES:

1. K.H.A-Ai-shqueerat,et al.,“Cloud Computing Security Challenges in Higher Educational Institutional –A Survey” IJCA – volume 161,No 6, march 2017 page no22- 29.
2. Gururaj Ramachandra et al., “A Comprehensive Survey on Security in Cloud Computing”, Elesevier – procedia Computer Science(2017) pp no : 465-472.
3. Fernandes D.A. etal., “Security Issues in Cloud Environment a Survey” April 2014:13(2):113-70.
4. Ashish Singh, Kakali Chatterjee,et al., “Cloud Security Issues and Challenges: A Survey” Journal of Network and Computer Applications2015.
5. Supriya,GurpreetSingh “A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security”, International Journal of Computer Applications (0975 – 8887) Volume 67– No.19, April 2013.
6. Luigi coppolino,Salvator D'Antonio,Giovanni Mazzeo,Luigi Ramano “Cloud security: Emerging threats and current solutions”, Elsevier-computer and Electrical Engineering 000(2016) 1-15.
7. Geetha V,Lavanya N,Priyadharshiny S, Sofeiyakalaimathy C” Survey on Security Mechanisms for Public Cloud Data”,2016 IEEE.
8. Subhashis Sengupta,Vikrant Kaulgud,Vibhu Saujanya Sharma,” Cloud computing Security-Trends and Research Directions” ,2011 IEEE.
9. Tanvi Agrawal,S K Singh,” Analysis of Security Algorithms in Cloud Computing”,2016 IEEE.
10. Saurabh Singh,Young-sik Jeong,Jong Hyuk park,” A Survey on Cloud Security :Issues, Threats and Solutions” ,Journal of Network and Computer Applications-Elsevier 2016.
11. Pankaj Singhai, et.al” ASurvey on Cloud Security Issues and Challenges”,IJIRCCE,Vol.5,Issueue 5,May 2017.
12. Umar Mukhtar Ismail,Syed Islam “Towards Cloud Security Monitoring :A Case Study”2016 Cyber and Cyberforensics Conference,2016 IEEE.
13. Mohammad Ubaidullah Bokhari,Qahtan Makkishallal”Security and Privacy issues in cloud computing”,2016 IEEE.
14. Er Ashima Pansotra et.al “Cloud SecurityAlgorithms”,Inetrnational Journal of Security and its Applications,vol.9,No.10(2015) pp.353-360.
15. R Sharma and R K Trivedi-Literature Review: Cloud [16]. Syed,Heena I and Naghma A Baig “Survey on Cloud Computing“IJETAE,2013.
16. Mazhar Ali,SAmee U.Khan,Athanasios V,Vasilakos,”Security in Cloud Computing:Opportunities and Challenges”Accepted Manuscript,Elsevier,2015.
17. R.Barona,E.A.Mary Anita,”A Survey on Data Breach Challenges in Cloud Computing Security: Issues and Treats”,2017,ICCPCT,IEEE.
18. Prachi Garg,et al,”Security Techniques for Cloud Computing Environment,ICCCA2017,IEEE.
19. Md.Alam Hossain, et al.,” Performance Analysis of Different Cryptography Algorithms” ,IJARCSSE,Vol2,206

AUTHORS PROFILE

Ms. J V S ARUNDATHI, is currently a PhD scholar in the Department of Computer Science and Engineering, KL Deemed To Be UNIVERSITY, GUNTUR, INDIA. Her research interest includes Information Security and Cloud Computing Security, IOT.

Dr. K.V.V. SATYANARAYANA ,is a Professor and M. TECH Coordinator in the Department of Computer Science and Engineering, KL Deemed To Be UNIVERSITY, GUNTUR, INDIA. His research interest includes Information Security and Cloud Computing Security. He is the Senior Life Member of Computer Society.