Journal of Theoretical and Applied Information Technology
15th March 2021. Vol.99. No 5

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

EXPLORATION OF VARIOUS VIEWPOINTS IN CLOUD COMPUTING SECURITY THREATS

T.A MOHANAPRAKASH[1], DR.V.NIRMALRANI[2]

[1]Research Scholar, Department of Computer Science and Engineering, Sathyabama Institute of Science and Technology, Chennai 600119, Tamilnadu, India.

[2]Associate Professor, Department of Information and Technology, Sathyabama Institute of Science and Technology, Chennai 600119, Tamilnadu, India.

E-mail: tmohanaprakash@gmail.com[1], nirmalrani.it@sathyabama.ac.in[2]

ABSTRACT

The cloud technology has demonstrated an outstanding performance in last few decades. It has been able to reduce the upfront investment requirements of enterprises in order to provide a seamless service with the introduction of Infrastructure as a Service, Software as a Service and Platform as a Service. This provides a wide variety of options and instant deployment of selected services. The prime component of the cloud computing is the virtualization of the shared computing resources among multiple clients. Even though the cloud computing has outperformed the traditional computing methodologies it has a few backlogs in terms of security. The security threats associated with cloud are but not limited to data integrity, network breach, insider attacks, virtual machine side channel attacks etc. Now a day's 70% of the industries using cloud, because of this threat becomes a serious concern to the cloud service provider and to the clients. In this paper analysis about the recent security threats of cloud in regards to data security, network security, environmental issues and virtualization issues. Also this paper discuss and analysis roles of various algorithms used in cloud computing for security.

KEYWORDS: *Cloud computing, Data security, Virtualization threats.*

1. INTRODUCTION:

The cloud computing is the recent evolving paradigm. Its allows the users to communicate with the data stored and spread all over the world.This serves as a platform which offers the computing resources as services to the clients. The cloud service providers allow the "pay per use" model which enables the user to utilize on-demand service. Its extremely efficient and useful for all types of companies ranging from start-ups to large organizations. It vastly reduces the costs involved in setting up the premises for servers.In general, the cloud computing offers different types of services namely Software as a Service(SaaS),Platform as a Service(PaaS), **SaaS**: The SaaS permits the cloud users to make use of the softwares developed by the cloud service provider.The user can utilize these services by means of Application Programming Interface(API). The data storage and management is done in accordance with the Service Level Agreement(SLA) [1].

IaaS: This service provides instant computing infrastructure facilitated and maintained over the internet. This can be scaled as per the requirements of the demanding situation. It aides in averting the cost involved in buying and installing complex equipment and infrastructure expenses related to data centers [1][2].

PaaS: The PaaS can be accessed over the internet which allows the developers to create an entire application with a web browser. The PaaS usually includes developement tools, middlewares, operating systems,database management systems ,business intelligence services, support for rogramming languages. This reduces the expenses related to the software licenses.

The entire software development life cycle activities can be managed by this service.[1][2] of attention. This security issue has been acting as a barrier for the potential users to adapt the cloud systems. This paper discusses about the security issues related to the cloud computation.

These types of services can be deployed as public, private or hybrid cloud as per the requirements of the organization. Having said about services and functional competence of the cloud, the security issues related to the developing cloud computing has gained a lot

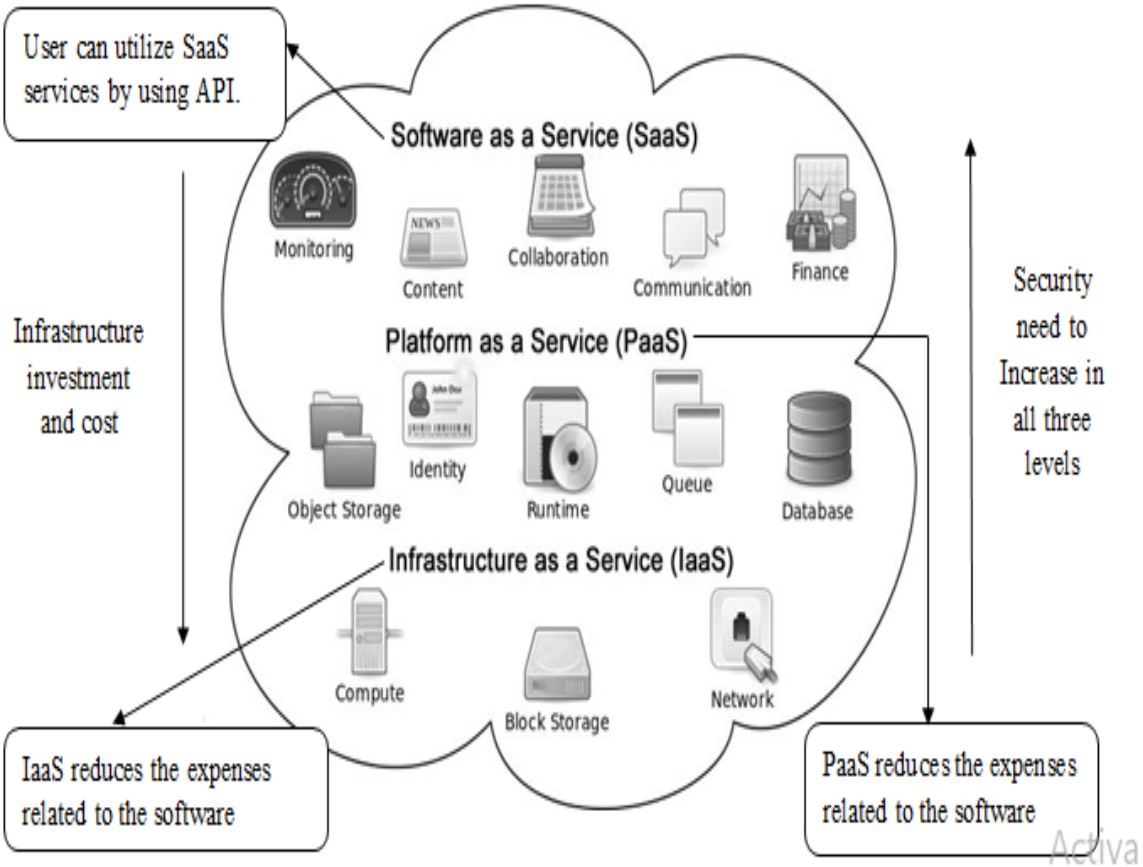

Figure 1: Infrastructure As A Service(Iaas)

2. THREATS IN CLOUD SECURITY:

The virtual environment of the cloud provides access to enormous computation power which supports development of various applications in multiple fields but the method of data transmission is done through the internet and used throughout the cloud which raises concerns regarding the security and privacy of the data. The traditional methodology of providing security to the data using anti-virus software and firewalls is not greatly useful in virtualized environment.

2.1: Common threats in cloud computing:

The threats that the cloud computing faces can be categorized as Data, Network and cloud environment related threats.fig-2

2.1.1: Data threats:

so does the data of the client. The protection of the client's data has became the primary concern of

the service providers. Some of the considerable security threats are data breaches and data loss.

One of the principle assets of any enterprise is the data. As time passes by, the client base of the cloud service providers is increasing an

A Data Breach:

The data breach can be defined as the leakage of client or enterprise data though non-authenticated access to the company's server. These kind of data breach affects the companies reputation as well as the financial state of the company. Recently the most popular social media "Facebook" has been reported of a leakage of its client's data through one of facebook's third party companies. Several companies like Zomato, Zyngaetchas been a victim of data breach.

B Data Loss:

The data loss is significantly another type of data threats where the client's or company data is lost due to malicious deletion of data by unauthorized users, crash of harddisk leading to data corruption, Loss of data due to natural disasters.[3]

C Data Integrity issues:

The data integrity ensures that the data of the client does not get compromised(modification and deletion of data). The manipulation of the data is possible through an attacker or even by a malicious insider. However, there has not been a universal rules for maintaining data integrity which leads the clients to bestow their data based on the establishment of trust with the cloud service provider.

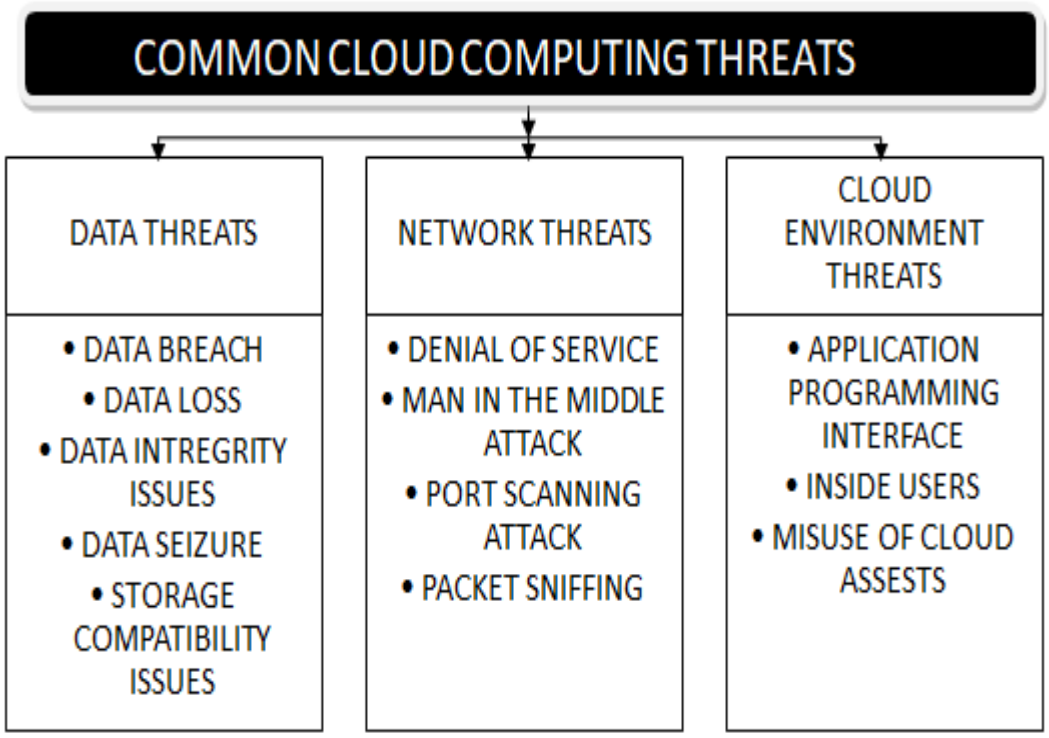

Figure 2 : Cloud Computing Threat

D Data Seizure:

One of the prime advantages of using the cloud is the cutback of the upfront investment by the companies. Enormous number of start-up enterprises use the affordable public cloud in which multiple clients share the same computing resources. Even though the cloud service provides a isolated environment, if the government seizes the properties of one of the clients it leads to the seizure of the entire physical server.

The federal laws does not complies with the newly implemented environment technologies, the cloud service providers advices their clients to store their data as encrypted files. Since the cloud service providers are obliged to the law the complete data present in that physical would be provided to the investigation department but would not be able to decrypt the files since the cloud service provider does not possess the decryption keys.

E **Issues with storage compatibility of data:**

Multiple cloud service providers offers their own custom developed storage management services. In the traditional servers, the storage services offered by hosting platforms allows the clients to migrate from one hosting to another host provider seamlessly. In the cloud, the storage services offered by one CSP is not compatible with the other providers. If one CSP goes down(bankruptcy) the task of data migration becomes difficult for the users.

2.1.2: Network threats:

The network plays an influential role in the cloud computing. The efficiency of the cloud service provider can be determined by the networking methodologies used to provide faster and efficient data routing and storage. The networks threats are equally important to that of data threats. There are a few notable network threats which are as follows:

A **Denial of Service**

One of the most common traditional networking threats is Denial of Service(DoS). The DoS attack prevents the authentic users from utilizing the services offered by the company. This can be done by sending numerous request to the host server(Centralized server) up until the point where the server crashes. As the server side as evolved, the DoS have also evolved to Distributed Denial of Service where multiple sources spread throughout the world are utilized for the transmission of enormous amount of dummy pings up until server crash point.

B **Man in the Middle attack:**

The man in the middle attack is termed to be an active eavesdropping attack where the attacker continuously monitors the data transmission between the sender and the receiver. The data relayed between the sender and the receiver passes through the attacker's system without their knowledge. In order to overcome this the SSL(Secure Socket Layer) was advised to be made use to ensure end to end encryption and secure transmission of the data.

C **Port Scanning Attack:**

The ports are considered to be the doors of access to the server. When a client sets a particular port to handle all types of requests it becomes vulnerable to port scanning where the attackers scans every data passing in and out through the ports. Its difficult to trigger an alert of port scanning for the online servers because its the inherent nature of the internet servers to allows access to data through the specified ports.

D **Packet Sniffing:**

The data is sent in the form of packets from the sender to the receiver.In the traditional computing the packet sniffing is one of the common network threats which involves the attacker scanning the packets of data send in through the network. The detection of packet sniffing is hard since the packets are routed through multiple routers and switches on its path to the destination and the attacker might be present in any of these traffic handling devices. This does not seems to be a problem in the virtual network since the VMM routes the packets directly to the specified virtual instance. That being said, the

cloud service providers offer additional protection to ensure the prevention of packet sniffing.

2.1.3: Cloud environment threats:

The cloud environment threats are limited to the interfaces(API), shared data environment and vulnerable cloud services. Some of the concerning cloud environment threats are as follows:

A API: Most of the services provided by the cloud can only be accessed through the usage of application programming interface(API). Such API accessible services include but not limited are SaaS, PaaS and IaaS. These API's are used in the management of infrastructure , storage platforms and software applications. These API's are mostly handled by third party companies. A weakly designed API could allows access to company's confidential information.

B Inside workers: Considering the number of threats in the cloud computing not every threat is due to an unauthorized user(hacker), sometimes it can be caused by a malicious insider of the company. This insider is provisioned with authentication to secure files which they use to carry out unprivileged activities.The cloud service provider must also do a wide spread surveillance on the activities of their authorized users.

C Misuse of Cloud assets: In order to increase the client base the cloud service organizations use the traditional marketing method of providing a limited period demo of the product. Occasionally a few clients might utilize the power demo hardware provided by the cloud service provider to perform malicious process.

2.1.4 Insufficient resource and experts:

Many enterprises are migrating from traditional computation to cloud computing. Yet this migration remains to be a great challenge to the enterprise due to the lack of human resources with the skills of cloud technology. Several employees of the IT companies are considering multiple path to gain the knowledge of working in a cloud environment. Some enterprises are accelerating the process of migration by hiring people with competence of cloud technology and coaches their existing employees to impart the knowledge of cloud.[20]

2.1.5 Cost management of cloud resources:

One of the major profits in using cloud computing is the cost efficiency. Despite the flexible cost structure of the cloud computing, some enterprises seems to be increasing their expenses due to inefficient handling of the cloud resources. For example, an employee might forget to turn off the unwanted cloud instances which indeed increases the cost. A few companies have overcame this challenge of by employing a full time cost management team.[21] [25] [26]

3. VIRTUALIZATION AND ITS ASSOCIATED THREATS:

3.1 Types of Virtualization Threads

The Virtualization is the cutting-edge technology that has made it possible for the cloud technology to attain at-most efficiency in data management with least investments. Its has paved way to run multiple isolated operating systems in the same physical server.One of the prime components of the virtual environment is the hypervisor alternatively known as virtual machine monitor(VMM). This acts as an interface between the virtual environment and the physical platform. The hypervisor makes use of the resources such as storage, CPU and memory provided by the physical server. The virtual machine monitor allows sharing of resources(physical server) by multiple clients with isolated environment for each client. In traditional computation the application running on the server might use around 40% of the server's capacity 60% is unexploited . By the implementation of shared resources, the other 60% of the server is used by multiple clients which leads to full utilization of the server. One of the merits of virtual machine is that it provides complete isolation from the other virtual machines in such a way that even if one virtual machine fails it does not affect the others but if one physical server fails it affects all the virtual machine that were running in it.[4] The virtualization of the system can be done in two different ways. They are as follows:

❖ **Virtualization based on operating system**:

In this type, the virtual machines are based on the operating system which runs directly on the physical resources. This is commonly referenced as bare-metal hypervisor. There a some serious threats associated in this method of virtualization.There is a better chance in attacking the kernel of the operating system which might compromise the entire virtual machine. Some examples of hypervisor are VMware, Hyper-V.[4][5]

- **Virtualization based on hypervisor**:

The hypervisor is made available during the boot time by the existing operating system. Since the hypervisor allows the functionalities such as shared resources and isolation, it provides an environment which is more controllable in nature. Since the virtual environment is created over the hypervisor the calls to the physical machine are made by the underlying operating system. The virtual machines that runs over the hypervisor is named as guest virtual machine. These guest VM makes calls to the host operating system by using the API(Application Programming Interface). Some examples of hypervisors of such type are: Microsoft Virtual PC, Oracle Virtual Box, KVM.[4][5]

3.2: Threats in virtualization:

Having said about the convenience of using virtual machine, it has also raised a few security challenges of its own. Some of them includes but not limited to are Denial of Service(DoS), Cache side channel attacks, malwares, unauthorized intrusion, hyper visor jacking and hyper visor escape [7]. Fig-3 A brief description of the threats in virtual environments is as follows:

Attack amongst virtual machine: One of the prime functionalities offered by the virtual machine is isolated environment which can be prevented from attacks based on the policies framed for access control. Having said that, if one of the many virtual machines in a host is compromised it wouldn't be very difficult in accessing the other virtual machines in the same host which indeed provides full control over the machine.[6]

VM Migration: In the virtualized environment, the scalability feature requires shifting of the VM from one physical host to another. This transportation of the VM takes place seemlessly in the background without the knowledge of the client which could introduce a threats posed by the malicious insider who values the data of the client to be profitable.There are multiple modes of transportation of the stolen data by until this day there ain't a mode of transmission which hasn't left out a forensic clue of the theft.This paper [10][20] has made high tech as well as low tech analysis in data transmission. Some of the predicted methods of high and low tech attacks are as follows:

- Cloning of the hypervisor and use it in the remote location with the intent of obtaining the user data.
- Creating a copy of the datastore.
- Possibility of attacking the network(such as man-in-the-middle, packet sniffing) during the transit of the VM in-order to nab the host and the vmdkfiles.One of the ways to avert this attack shall be encrypting the files that are to be transmitted over the network.[9].
- **VM cloning**: The virtual machine cloning is a reflection of the existing virtual machine which is present in the same network as that of its parent VM. This process is done in-order to reduce the time required in installation and setup of a group of similar virtual machine and as well as to manage the increasing workload. A typical example would be cloning a production environment virtual machine to a testing environment for checking the compatibility of the newly developed features. There are three types[8] of cloning which are as follows:
- Full cloning: Here the cloned VM is completely independent from the parent VM.
- Linked cloning: In this type the cloned machine shares the same virtual memory as that of the parent virtual machine.
- Instant clone: The time required to create a instant VM clone is extremely low when compared to the other two methods of cloning. In this method the cloned VM uses the in-memory of the currently running parent VM and the copy of data to the memory is done upon write operation only.

However though the cloning seems to be a viable solution to compensate the increasing workload, there are few threats associated with this method. Since the clone is usable by multiple similar VM, Obviously the configuration(entropy pool) of all these virtual machines are similar. This could lead an attacker to guess the crypto keys that are used in the process of VM encryption and decryption [8].

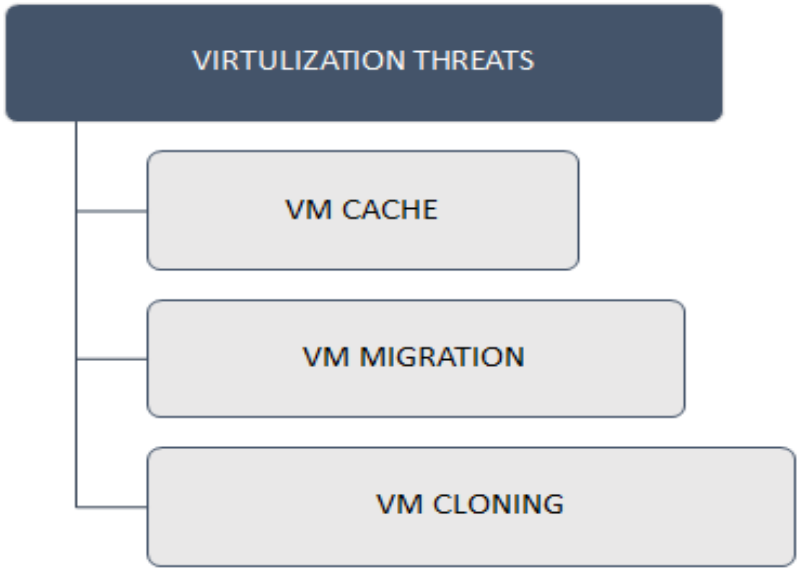

Figure 3 : Types Of Possible Virtualization Threats

VM CACHE: One of the noticeable attacks made due to vulnerable shared technologies is the cross virtual machine side channel cache attack which uses the data available in the shared cache of different virtual machines. In general VM becomes a victim to the side channel attacks when a competitors malicious virtual machine shares the same hardware resources as that of the victim and performs activities such as man in the middle attack and awaits for sensible information such as encryption and decryption keys etc . In the cache side channel attack, the malicious VM performs observation in the shared resources and analysis the cache access behaviour, execution time of operations etc. There are a few techniques used by the attacker in the past few years. They are as follows:

i) Prime and probe attack: Here the attacker places eviction sets in the cache which they choose to monitor.

ii) Flush and reload attack: In flush and reload attack, the attacker places spy processes which are programmed to observe the accessed pages in the shared memory. By this process, the attacker traces the memory path used by the victim and performs data extraction.

The cache side channel attacks are categorized into three. They are as follows:

i) Time-driven attack: Here the attacker tries find the relation between the operations and the cache miss. Upon continuous observation, the attacker tries to establish a pattern inorder to extract the victim's information.

ii) Access-driven attack: Here the spy process is executed in parallel inorder to gain the knowledge about the behaviour of the victim. The cache sets accessed by the victim are confirmed by the attacker when the victim experiences a cache miss.

iii) Trace-driven attack: Here the attacker observes the cache lines that are been utlized by the victim. In this method, the attacker follows the memory lines which has resulted in a successful cache hit rather than cache miss.

In order to evict the cache based side channel attacks it requires architectural level changes in hardware,software and hypervisor. [7].

4. ROLE OF HASHING ALGORITHMS IN CLOUD COMPUTING:

There is always a concern about the data integrity and authenticity since the storage location of the data is widespread throughout multiple servers. There are multiple cryptographic methodologies to preserve the data integrity and reliability which includes the process of encryption, decryption and generation of hash values. Lets us discuss about some of the hashing algorithms which can be used to check the integrity of the stored data.[22][23]

4.1 Message Digest 5(MD5):

The MD5 produces an output of 128 bit when given an input of size 512 bits. Its faster when compared to the other digest algorithms. This 128 bit output is produced by the combination of four 32 bits blocks.

Step1: Appending the padding bits: The padding is done until the length of the word is equivalent to 448%512. The first padding bit is 1 and the remaining padding bits are assigned the value of 0.

Step2: Appending Length: The length of the original input is measured after the padding bits are added. The message length is now in multiples of 512.

Step3: Message digest buffer: The Message digest buffer consists of four registers each of size 32(in bits). These registers are initialized with predefined values.

Step4: Processing the message in 16 word blocks: The auxiliary functions of MD5 takes three 32 bits values and produces a single 32 bit output value. *Step5*: Display Output: The output is displayed based on the order of the byte ranging from lower to higher. The values from the four registers are combined to form the final 512 bit hash value [11][12]

4.2 Secure Hashing Algorithm(SHA):

The secure hashing algorithm was developed by keeping MD4 as the base.It has been developed by NIST(National Institute of Standards and Technology).Its been utilized by multiple security application. [24] Lets us take a look into the working steps of SHA-512:

Step1: Padding Bits: The given input message is padded until the length of the input message is congruent to 896 mod 1024. The first padding bit is 1 and the remaining padding bits are assigned the value 0. The padding is done regardless of the length of the input data.

Step2: Padding length: The unsigned 128bit is added to the initial input value.

Step3: Intialization of hashing buffer: The 512 bit buffer is used to hold the intermediate and the final results of the function. Each register in the buffer is 64 bits.

Step4: Processing of the message: The message processing is done in 80 rounds with every round taking three inputs: a word of 64 bits, the output of the previous completed round and a constant. The SHA constant is formed by taking the first 64 bits of the fractional part of cube roots of first 80 prime numbers.

Step5: Displaying the Output: After successful completion of the previous process, the hash value of length 512 bits is obtained.

The SHA-2 consists of a group of SHA algorithms that works in a similar way as SHA-512. The

comparison of MD5 and SHA-512 shown in [11][12][13].

4.3 Secure Alert systems through the combination of blowfish and RC6 algorithm:

This paper[14] has proposed an alert system though the combination of advantages of blowfish and RC6 algorithm.In the encryption process the system generates a digital signature which is obtained using sha-256 and blowfish algorithm encrypts using the digital signature and the plain text using key 1 which is randomly generated. A second key namely is generated for encryption using RC6.

The output of blowfish is encrypted using RC6 with key 2. This combined encryption utilizes the advantages of both SHA-256 and RC6. During the decryption process, the user is prompted to enter both the keys and the number of wrong inputs is tolerated until the preset threshold value. The alert is sent when the number of trails increases the threshold values.

4.5 Attribute based algorithm:

The privacy protection and data security assured by the cloud service providers are the key components to the prominence of cloud computing. The cryptographic algorithms have been the guardians of the user data from being exposed. There are multiple public key cryptography methodologies among which the attributed based encryption has gained a recent popularity.

In the attribute based algorithm the authenticity of the user is verified based on the private key as well as other parameters of user such as their location, user's account type etc. Lets us dive into the working process of attributed based cryptographic methodology.[15][16][19]

Step1: Generation of public and master key: The trusted centers generates master key and the public key. Step2: Generation of private key: The private key is generated through the combination of user attributes by the trusted authority.

Step3: Encryption: The algorithm used for encryption is provided with the message to be encrypted, user attributes and a number(generated randomly). The message is encrypted with these three parameters.

Step4: Decryption: The encrypted message and the user attributes are sent as input to the decryption algorithm [15][27].

Having said about the pros of Attribute based algorithm, there exists a few cons that needs to be addressed. They are inefficient and challenging revocation mechanism, usage of invariable attributes to control access to data and challenges in key escrow and coordination.

The Cipher Policy-Attributed based encryption is setup on the base on attributed based algorithm. This paper[17] has proposed a system which uses CP-ABE with user revocation function. In the CP-ABE only a set of authorized users can perform the decryption function.

For Example, in the software team the project code is accessible to the members of the team but if one of the team member "B" moves out of this project team, the project code is inaccessible by "B" eventhough "B" still works for the same company. The CP-ABE is almost conceptually similar to the role based access control but contains the features of ABE.The CP-ABE follows the below steps:

Step1: Setup of parameters: The setup algorithm provides the public key and master secret key based on the security parameters of the user.

Step2: Key generation: The keygen algorithm takes the master secret key and user attributes and provides the private secret key(PVT) for every user.

Step3: Key encryption key(KEK): This algorithm takes a set of users and provides KEK.

Step4: Encryption: The encryption algorithm takes the message to be encrypted, the private key and the access structure of the user to provide a ciphertext. Step5: Decryption: The decryption algorithm takes the cipher text, private secret key of

the user(PVT) and set of group attribute keys and provides the decrypted message.

Table 1 : Comparison Table Of MD5 And SHA-512

	MD5	SHA-512
Message block size	512 bits	1024 bits
Output size	128 bits	512 bits
Collisions	Yes	No
Speed	Faster, 64 Iteration only	Slower, 80 Iterations
Execution time (in milliseconds) given File size of 500KB	35	48
Throughput	5.44 mb/sec	5.03 mb/sec

Table 2 : Performance Analysis

	ABE	CB-ABE
Encryption	$\|AT_{CipherText}\|*BI_1+(2*BI_2)$	$2*(\|AT_{CipherText}\|+1)*BI_1+(2*BI_2)$
Decryption	dC_e+2dBI_2	$2*\|AT_{user}\|*C_e+(2*\|m\|+2)*BI_2$
Policy	Threshold	AND, OR, Threshold
User Accountability	Not Satisfied	Satisfied
User Revocation	Not Satisfied	Satisfied
Fine Grained Access Control	Not Satisfied	Satisfied

Some of the few notable disadvantages of CP-ABE are inefficiency, less flexibility in managing policy and attributes and increase in overhead of the algorithm with increasing user attributes. The comparision of ABE and CB-ABE in Table-2 **[18][19].**

5. CONCLUSION:

The cloud computing has gained a astonishing number of the clients as a cause of its reduced upfront investment, instant scalability, advanced data management, isolated virtual environments, shared hardware resources ,easy to understand interface and instant service subscription and cancellation. Although the cloud has a competitive advantage over the traditional computing yet the threats associated with cloud threatens some enterprises(including banking) and governmental organization from migrating to cloud environment. This pause from migration can be averted by improving the security services and formation of standard regulations to provide accountability. Having analyzed the viable recent security threats associated with cloud computing, this paper can be considered as a precursor for further in-depth research and analysis of cloud's security services.

REFERENCES:

[1] Ramachandra, Gururaj&Iftikhar, Mohsin& Khan, Farrukh. (2017). A Comprehensive Survey on Security in Cloud Computing. Procedia Computer Science. 110. 465-472. 10.1016/j.procs.2017.06.124.

[2] Hussain, Syed Asad, Mehwish Fatima, AtifSaeed, Imran Raza, and Raja KhurramShahzad. "Multilevel classification of security concerns in cloud

computing." *Applied Computing and Informatics* 13, no. 1 (2017): 57-65.

[3] John Viega, McAffee, Cloud Computing and the Common Man," published on the IEEE Journal ON Cloud Computing Security, pp. 106-108, August 2009.

[4] S. Jin, J. Seol, J. Huh, and S. Maeng, "Hardware-assisted secureresource accounting under a vulnerable hypervisor, ACMSIGPLAN Notices, vol.50, no.7,pp.201–213,2015.

[5] FarzadSabahi, M., IEEE, Secure Virtualization for Cloud Environment Using Hypervisor- based Technology.International Journal of Machine Learning and Computing, 2012.Vol. 2 (February 2012), pp.39-45.

[6] Chen, S. L. Z. L. X., Z. Corporation, and C. Shenzhen, Virtualization security for cloud computing service. International Conference on Cloud and Service Computing, 2011(2011 IEEE), pp.174-179

[7] Litchfield, Alan T. and AbidShahzad. "Virtualization Technology: Cross-VM Cache Side Channel Attacks make it Vulnerable." *ArXiv* abs/1606.01356 (2016).

[8] Gunasekaran, Jashwant Raj, Michael Cui, PrashanthThinakaran, Josh Simons, Mahmut T. Kandemir, and Chita R. Das. "Multiverse: Dynamic VM Provisioning for Virtualized High Performance Computing Clusters." In *2020 20th IEEE/ACM International Symposium on Cluster, Cloud and Internet Computing (CCGRID)*, pp. 131-141. IEEE, 2020.

[9] Barrowclough, John Patrick and RameezAsif. "Securing Cloud Hypervisors: A Survey of the Threats, Vulnerabilities, and Countermeasures." *Security and Communication Networks* 2018 (2018): 1681908:1-1681908:20.

[10] Duncan, Adrian, Sadie Creese, Michael Goldsmith, and Jamie S. Quinton."Cloud computing: Insider attacks on virtual machines during migration." In *2013 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications*, pp. 493-500. IEEE, 2013.

[11] Singh and S. K. Saroj, "A Secure Data Dynamics and Public Auditing Scheme for Cloud Storage," 2020 6th International Conference on Advanced Computing and Communication Systems (ICACCS), Coimbatore, India, 2020, pp. 695-700, doi: 10.1109/ICACCS48705.2020.9074337.

[12] Kumar, Sandeep& Gupta, ErPiyush.(2014). A Comparative Analysis of SHA and MD5 Algorithm.International Journal of Computer Science and Information Technologies.5.pp: 4492 - 4495.

[13] Katende, Nicholas & Wilson, Cheruiyot&Kibe, Ann. (2017). Enhancing Trust In Cloud Computing Using Md5 Hashing Algorithm And Rsa Encryption Standard. International Journal of Scientific & Engineering Research, Volume 8, Issue 3, March-2017. 8(3).pp.550-566.

[14] M. Ilaiyaraja, P. Balamurugan, R. Jayamala, 2014, Securing Cloud Data using Cryptography with Alert System, International Journal Of Engineering Research & Technology (IJERT) Volume 03, Issue 03 (March 2014): 98-101

[15] Mathur, Etti and Manish Sharma. "A Review of Attribute based Encryption Technique for Security in Cloud Computing." *International Journal of Computer Applications* 159 (2017): 43-45.

[16] Chaudhari, Nikhil &Saini, Mohit& Kumar, Ashwin&Govindaraj, Priya. (2016). A Review on Attribute Based Encryption. 380-385. 10.1109/CICN.2016.81.

[17] Xie, Xingxing, Hua Ma, Jin Li and Xiaofeng Chen. "An Efficient Ciphertext-Policy Attribute-Based Access Control towards Revocation in Cloud Computing." *J. UCS* 19 (2013): 2349-2367.

[18] Waters, Brent. "Ciphertext-policy attribute-based encryption: An expressive,

efficient, and provably secure realization." In *International Workshop on Public Key Cryptography*, pp. 53-70.Springer, Berlin, Heidelberg, 2011.

[19] J. Sun, "Privacy Protection and Data Security in Cloud Computing: A Survey, Challenges, and Solutions," in IEEE Access, vol. 7, pp. 147420-147452, 2019, doi: 10.1109/ACCESS.2019.2946185.

[20] Subramanian, Nalini ,Jeyaraj, Andrews. (2018). Recent security challenges in cloud computing. Computers & Electrical Engineering. 71. 28-42. 10.1016/j.compeleceng.2018.06.006.

[21] "10 Biggest Cloud Computing Challenges in 2020 for IT Service providers", https://www.mindinventory.com/blog/cloud-computing-challenges/

[22] T.S., Suganya& S, Murugavalli. (2019). A hybrid group search optimization: firefly algorithm-based big data framework for ancient script recognition. Soft Computing. 24. 1-9. 10.1007/s00500-019-04596-x.

[23] Nalini Subramanian, Andrews, J. Strong authentication framework using statistical approach for cloud environments. Concurrency ComputatPractExper. 2019; 31:e4870.

[24] T. A. Mohanaprakash and J. Andrews, "Novel privacy preserving system for Cloud Data security using Signature Hashing Algorithm," *2019 International Carnahan Conference on Security Technology (ICCST)*, CHENNAI, India, 2019, pp. 1-6, doi: 10.1109/CCST.2019.8888420.

[25] J. Chenni Kumaran; M. Aramudhan , "A survey on resource allocation strategies in cloud" International Journal of Reasoning-based Intelligent Systems (IJRIS), Vol. 10, No. 3/4, 2018.

[26] Senthilkumar.G, Chitra.M.P., "An ensemble dynamic optimization based inverse adaptive heuristic critic in IaaS cloud computing for resource allocation", Journal of Intelligent & Fuzzy Systems, vol. 39, no. 5, pp. 7521-7535, 2020.

[27] G.Senthil kumar, Dr.M.P.Chitra, "Finite horizon markov decision process based fuzzy optimization for resource allocation in sdn enabled virtual networks in iaas cloud environment" , Journal of Theoretical and Applied Information Technology 15th July 2020. Vol.98. No 13.