DOI: http://dx.doi.org/10.26483/ijarcs.v9i2.5861

ISSN No. 0976-5697

Volume 9, No. 2, March-April 2018

International Journal of Advanced Research in Computer Science

REVIEW ARTICLE

Available Online at www.ijarcs.info

CLOUD COMPUTING: MAJOR CHALLENGES AND COUNTER ACTS

Arjmand Ashraf
Department of Information Technology
Central University of Kashmir
Srinagar, India

M Abdul Jawad
Department of Information Technology
Central University of Kashmir
Srinagar, India

Abstract: Although Cloud Computing has remarkably provided us easy accessible, manageable and maintainable resources at effective costs, but due to the fact that all or multiple users are allocated with the similar resources present security threats to the cloud subscribers. It is well known fact that in cloud paradigm, the data and applications are always under the control of third party, which give rise to serious concerns among the cloud subscribers. Cloud computing attracts the attention of research community due to its potential to provide tremendous benefits to the industry and cloud subscribers, but it lingers because of the security, privacy, and trust issues with Cloud subscribers. If Cloud Service Provider's (CSP's) are being able to provide efficient security tools, the utilization of services will rise exponentially and it will soon become globally accepted computing. This paper provides state of the art of major security challenges in the cloud paradigm and the countermeasures to counteract with the security breaches.

Keywords: Cloud security, Cloud service provider (CSP), Cloud Subscriber, Cloud Paradigm, Cloud Administrator

I. INTRODUCTION

Cloud computing is a representation for enabling pervasive, expedient, on-request network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be expeditiously provisioned and released with minimal management effort or service provider interaction [NIST]. As per the NIST definition, Cloud computing is the threefold service model consisting of Essential Characters, Service models, Deployment models as shown in fig 1. The essential characteristics are On demand self-service, Broad network access, Resource pooling, Rapid elasticity, Measured service, and Multitenancy. These features provide convenience of larger resources at economic costs. This makes Cloud Service Provider and Cloud Subscriber to avoid purchasing of large capital outlays, thereby avoiding the management and maintenance overhead. The service model include Infrastructure as a service (Iaas), Platform as a service (Paas), Software as a service (Saas), Data storage as a service (Daas), Security as a service (S_{ec}aas), anything as a service (Xaas) [2]. By "Anything as a service" we mean that Cloud is being able to offer almost everything to its users. Among all the services being offered by the Cloud Service Provider, Iaas (infrastructure as a service) is the most basic service offered to the Cloud users, Paas (platform as service) and Saas (software as service) are higher level of services. Apart from these services, Multitenancy is one of the corner stones offered by CSP, initially started by Saas vendors and later adopted by others [3]. The NIST definition is implemented over the Cloud architecture that is being run by Cloud service Providers. Cloud service providers are entities like Salesforce.com, Google apps, Google Apps Engine, Microsoft Azure, Amazon Web Services that provide services to the tenants.

Since 1900, outsourcing has been a normal way out to conduct business, and a common question in every Cloud Subscribers mind is that whether the offering of Cloud Platform are secure than the traditional on premise implementations. Most of these questions are being raised because of the multitenancy feature of cloud computing [3]. Even if CSP infrastructure and management capabilities are more secure and trustworthy than those of personal computing devices, still this platform is hindered with internal and external threats in the form of media failure, software bugs, malware, admin errors, security breaches [4]. There are certain examples which serve as proof to the security breaches in Cloud Paradigm like: Apple's iPad subscriber privacy leak, Amazon S3's recent downtime, and Gmail's mass email deletions, [2]. In 2007, criminals targeted the prominent cloud service provider (CSP) Salesforce.com, and succeeded in stealing customer emails and addresses using a phishing attack [5]. The user doesn't have access to the Cloud's internal operational details and the data they have stored on the platform so, Cloud Service Provider might also peep into the data and do manipulations as they want. The fundamental insecurity is due to the sheared architecture among multiple tenants i.e. Multitenancy [7].

Multitenancy is the practice of placing multiple tenants/users/Cloud Subscribers over the same underlying physical architecture to reduce costs, therefore providing economics of scale. Almost all of the Cloud Service Providers offer the feature of Multitenancy. The competitive nature of Cloud Computing is such that the CSP's have to minimize the total cost of ownership so as to survive in the market, and that is made possible only because of the feature of multitenancy. Multitenancy is analogous to a multiple families living in the same condomium, where each family have their own confined space, however there is always a

risk that one family may have access to another family's confidential information. Similarly the feature of multitenancy in the Cloud Paradigm introduces a unique set of security risks towards the co resident tenants which are yet to be acknowledged [7].

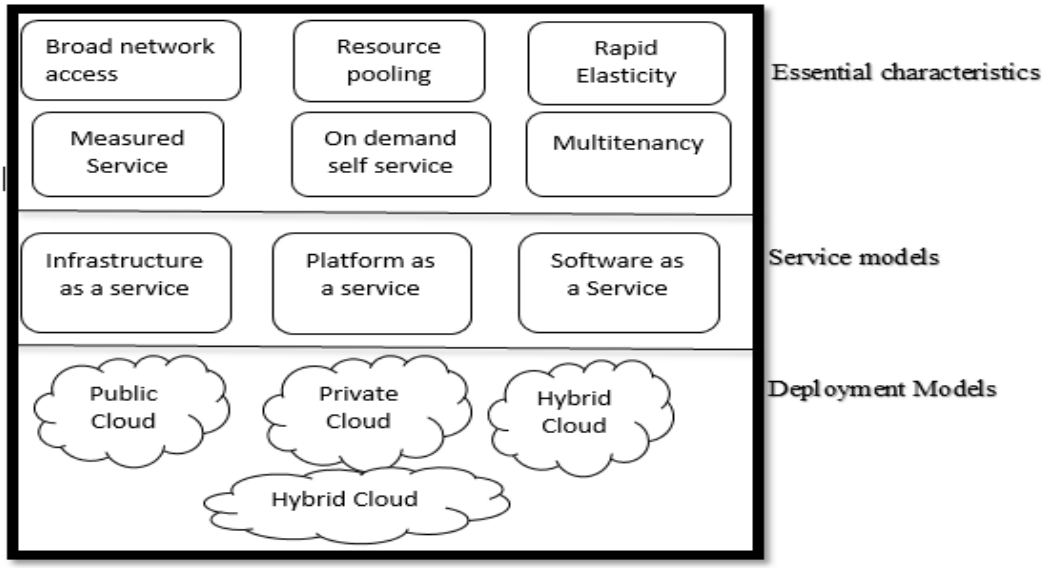

Figure 1: NIST definition of Cloud Computing

A. Basic Threats in Cloud Paradigm

The Cloud paradigm is being characterized by two main stakeholders the Cloud service provider and the Cloud Subscriber. The Cloud service provider (CSP) consist of cloud system administrators (CSA), tenant administrators (or operators) who actually manage the tenant virtual machines, and Tenants who provide services to end users, running over the virtual machines, while Cloud subscriber is the end user, who actually utilizes the services [6]. The given architecture consists of multiple tenants (T_1, T_2… T_N) which are being hosted by N number of virtual machines over the same physical underlying architecture. Since multiple tenants are being served by similar underlying architecture, there are many chances that this architecture will result in the security breach of tenants. Although the security provided by cloud paradigm is more than that of present in our homes, still the cloud users live with the threat that their data might get compromised. Some of the basic threats which can be there in the whole Cloud architecture are shown in Fig 2, reproduced from [6]. Although there is proper isolation between the tenants working on same or different virtual machines, but due to the fact that underlying physical architecture is same, makes the cloud paradigm vulnerable to threats.

1) Threats from the end user: The End user is the one who actually exercises the benefits of Cloud architecture by subscribing to the desired services. There is always a threat from the user side. If the user is malicious, there are chances that it will compromise with confidential data of other users belonging to the same or different tenants, therefore making a compromise with confidentiality of data. These tenants may further belong to same or different virtual machines, but using the same underlying architecture. The malicious

2) user may result in Denial of Service attacks, by keeping the server busy and preventing other legitimate users to enjoy the services. Furthermore, if the malicious user is being able to manipulate the contents of documents, will breach the integrity of data [6].

3) Threats from the tenant: A tenant is a group of users (it may be a single user as well) who share a common access with specific privileges to the software/hardware instance. It acts as a mediator between Cloud Service Provider and Cloud Subscriber. There can be attacks from the tenant users on the tenant virtual machines, even though there may be host based security system at place [6]. Furthermore, there is a chance of attacks from the malicious tenant administrator against the virtual machines serving other tenants, by exploiting the vulnerabilities for malicious purpose [6]. Hence the need of the hour is to have a proper isolation among the various tenants being served by either the similar or dissimilar virtual machines.

4) Threats from the Cloud administrator: The Cloud Administrator may be a person or software as well, managing and maintaining everything in the Cloud Paradigm .Cloud administrator has two primary roles; configuration of Cloud management services and monitoring the services [LINK]. The Cloud administrator is having every information regarding the users and the virtual machines, so if cloud administrator is malicious, it can become a bottleneck for the Cloud paradigm. For example, the Dom0 administrators of XEN can obtain all the required information from Memory allocated to the tenant when it is in unencrypted form [6]. This information is then used by the Cloud admin in an illegitimate way.

II. LITERATURE SURVEY

M. Ali Samee, U. Khan, and Athanasios V. Vasilakos [1] in year 2015 presented a survey paper which highlighted the

arguments which arise because of the sheared, virtualized, and public nature of cloud architecture. They have presented a summary on cloud security challenges be it challenges at communication level or architectural level, or be it challenges at contractual and legal aspects. Apart from discussing the issues the appropriate countermeasures are being presented. Some of them are Intrusion Detection System, Intrusion Prevention system, Advanced Cloud protection system, virtualization, and some security tools. They have mentioned in their paper that the traditional security issues are becoming more critical and challenging in the cloud paradigm as there is absence of user control over the data he stores on the cloud architecture. They have mainly focused on the challenges because of the colocation of data of multiple users on the similar underlying physical architecture.

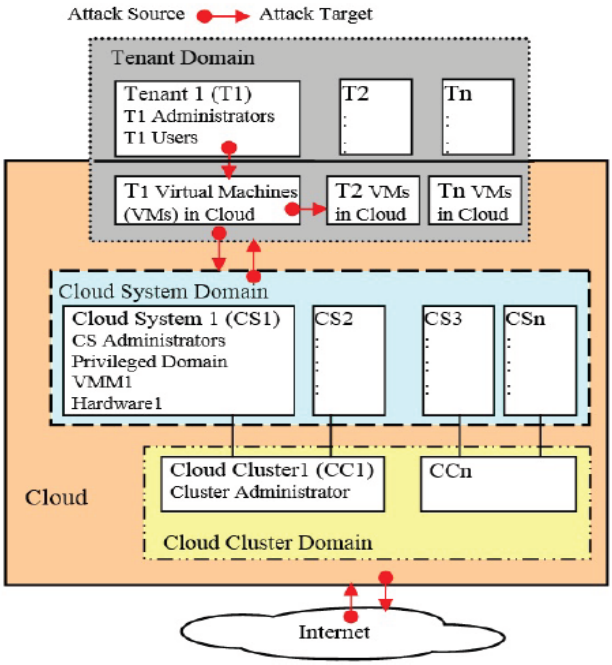

Figure 2: Some basic threats in Cloud Computing [6]

In a survey by Diogo A.B. Fernandes, Liliana F. B. Soares, João V. Gomes, Mário M. Freire, Pedro R. M. Inácio [2] emphasized towards the fact that, flexibility of combined features like on demand self-service along with pay per usage model has greatly influenced the computing world thereby shifting the traditional on premise computing to the Third party control. They have put forward a survey of number of works on concerns like security issues, vulnerabilities, threats, and attacks. Moreover they have introduced a taxonomy for their classification. So, to attain the motivation of providing a secure and trusted cloud architecture, identifying and then rectifying the security issues should be at top priority.

A study by Paul G Dorey [3] intensified the most important feature of Cloud Computing: Multitenancy, and the security risks associated with it. As per the findings the risk profile has been evaluated on the basis of CIA triad and the underlying architecture. The security objectives have been described and their impact on the Cloud subscriber upon the violation of these objectives. The author has formulated certain questions regarding the CIA and Multitenant Architecture that a subscriber should use as a framework to evaluate any CSP-MT (Cloud Service Provider-Multitenant) maturity. Based upon the response of these questions a subscriber should decide whether he should go for data outsourcing or any other service provided by the CSP. Furthermore, the author has proposed some Risk mitigation factors in order to provide a secure Multitenant architecture to the Cloud Subscribers.

In another study by Kui Ren et al. [4] in year 2012 outlined several threats in the Public Cloud paradigm which are being presented as the challenge in the mass adoption of Cloud Computing. As per the study Security and Privacy as the two most important and primary obstacles in Cloud architecture. They have addressed Data outsourcing, Computation outsourcing, Lack of user control and Multitenancy as the main causes for security and privacy issues. As such there is not any proposed architecture in this paper yet they have presented possible counter measures to the aforementioned factors and motivated further investigation in this field so that a threat free Public Cloud is introduced to the users.

Siani Pearson and Azzedine Benameur [5] executed their work on the Privacy, Security, and Trust issues thereby highlighting the major threats in Cloud Paradigm. They have put forward various issues; lack of user control, dynamic provisioning, lack of standardization, multitenancy etc. which actually lead to compromise of the cloud architecture. Besides they have put forward a number of mechanisms which will assure the threat free Cloud services like; data security mitigation, standardization, accountability etc. Depending upon the sensitivity of the user's data, the solutions need to be tailored as per the security context, which is again an overhead to implement.

In year 2014 Vijay Varadharajan and U.Tupakula [6] put in writing a monograph on the security services which a cloud service provider can offer to its clients apart from the other services. In their work they have put forward a security architecture where the baseline security will be provided to every user and tenant to protect all the stakeholders of cloud paradigm and underlying architecture as well. This baseline security will be provided to the users of Cloud without any extra cost. In order to secure the Cloud architecture they have suggested another service to be provided by CSP: "Security as a Service". Depending upon the sensitivity of the user data, if a user will subscribe to this service, he shall be charged as per the charges mentioned in SLA's. Also they have mentioned about the different domains in the cloud architecture from where the attacks are possible and some counter measures to the mentioned attacks. The issue with this security architecture is that the security mechanisms and tools offered by CSP gather more information about the tenant or user and hence there is privacy at stake.

W.J.Brown Vince Anderson, Qing Tan [7] mentioned the security risks which lead to trust issues among the Cloud users, and the proper counter measures which if properly implemented will lead to secure multitenant cloud

architecture. They have mainly focused on the Separation of duties, Auditing and control, and Trusted Computing. Trusted computing actually consists of two concepts: Transitive trust and Platform Attestation, which is based on the fact that initialization of a computing device will follow a trusted pathway through a bootstrap process, where one level will initialize keeping in consideration that previous level is a secure microkernel. Besides all of the counter measures presented in this paper we cannot fully secure the multitenant architecture, as it has mentioned some encryption schemes which make the processing very slow, thereby compromising with the availability.

A recent paper by Xiao-Fang Liu et al. [8] aiming at minimization of active physical servers and placement of virtual machines on the active servers. They have utilized the Ant Colony System along with the Order exchange and Migration system for minimizing the active number of servers and placement of virtual machines. Although it effectively decreases the active number of servers thereby minimizing the energy utilization at the cloud servers or Data Centers but it will lead to the security and privacy concerns, because lesser the number of active servers, more will be the number of virtual machines assigned to them. In this case the isolation may not be properly done, hence malicious tenants would be able to compromise with Confidentiality, Integrity, and Availability of other tenants. Hence, there is a tradeoff between the Energy optimization and security modules.

There is an another monograph aiming at translating the existing algorithms so as to conduct fully Homomorphic data on cloud paradigm by Ayantika Chatterjee and Indranil Sengupta [9]. Regardless of the fact, Cloud provides services which are easily accessible that make it a convenient paradigm, it is being challenged by the security of sensitive data. The primary solution to protect the confidential data is to encrypt the data, but then the processing and response time becomes a challenge. It takes more time to decrypt the data then processing and then again encryption of data. Moreover, the data has to be downloaded by the user, decrypt it, process it, encrypt it, and then upload it again on the Cloud. This will defeat the very purpose of Cloud for its resource utilization. While the encrypted data is made pass through the insecure channel, hence there are chances that it might be attacked by advisory. It would be profitable if direct processing is performed on the encrypted data, without downloading and decrypting it at client side. This is supported by Homomorphic Encryption schemes. However complete Homomorphic encryption schemes permit random operations directly on the cipher text. The authors have come up with the techniques to translate basic logic operations which are used for algorithmic implementation in any high level language. They have also addressed the decision making, loop handling, and termination conditions in an algorithm.

In a paper by Karim Zkik et al. [10] emphasized on safeguarding the user privacy by presenting a novel approach of Homomorphic encryption. The work aims to be focused on S_{ec}aas (Security as a service) model of Cloud Computing wherein any user will choose the level of security by subscribing to this service. The S_{ec}aas is made possible by two sub services: Authentication as a service (Aaas), and Encryption as a service (Eaas). The genuine encryption method to use is Homomorphic encryption, where any kind of processing takes place on the encrypted data. But its high response time permits its global use in cloud Computing. Therefore, this paper has proposed a novel security model by evading the negative factors in Homomorphic Encryption, by the name "Authentication and Homomorphic Encryption as a service" (A-HEaas).

III. MAJOR ISSUES IN CLOUD COMPUTING

Cloud Computing is a promising innovation, but the security issues prevent it from being the next generation technology [9]. The widely adopted framework to access the basic security profile of any IT system security is CIA (Confidentiality, Integrity, and Availability) triad. Besides CIA other factors in Cloud paradigm may be used to evaluate the system reliability like Multitenant Architecture, Access control, and Trust parameter. The sharing of resources is one of the key characteristics by which multiple tenants access the similar resources, and pave a way for the security breach. The data in the cloud is much more vulnerable to risks rather than in traditional on premise computing. The foremost issues in Cloud architecture are discussed below:

A. Confidentiality issues

Confidentiality is a set of rules which limit access to information. It can also be defined as "preserving authorized restrictions on information access and disclosure, including means for protecting personal and proprietary information" [3]. Hence we can say that confidentiality means when our data is safe from all unauthorized access. There are many features in cloud that lead confidentiality issues, these are Data proliferation, Transborder data flow, unauthorized data usage. In all of the aforementioned issues the data is replicated and made available to multiple parties, even without the consent of user [5]. This unauthorized disclosure of data to other parties could adversely affect the proper functioning of individual or business organization.

B. Integrity issues

Integrity involves maintaining the consistency, accuracy, and trustworthiness of data over its entire life cycle. In other words it may also be explained as "guarding against improper modification, addition, and deletion and ensuring non repudiation of data" [3]. As data is available to all, any malicious user can change the authentic contents to the malicious contents, and may even delete the data, thereby compromising with the integrity constraint.

C. Availability issues

Availability stands for "ensuring timely and reliable access to the resources" [3]. It may also be defined as "providing adequate communication bandwidth and preventing occurrence of bottlenecks". Availability is best ensured when we have presence of network, which is the basic criteria to access cloud services. As one fact is always there, "no available network means no cloud". So, to ensure availability of every other service, network availability is important.

For fast and adaptive disaster recovery, data replication is performed so as to prevent interruption to the users and ensure availability. These backup copies are stored in geographically isolated areas, which could be fireproof and waterproof, but these replicated copies may also be responsible for security issues. When the Cloud subscriber wants to lock-out or windup his business form the CSP, at that instant he can't be sure whether CSP has deleted all its replicas. Availability is commonly exploited by the DDOS attacks (distributed denial of service attacks).

D. Architectural issues

A Cloud Service Provider aims at providing robust architecture to stand with business goals of Cloud Subscriber so as to meet the three aforesaid objectives [3]. The CSP architecture is best known for virtualization, which gives illusion to all of its users that underlying architecture belongs to them. Virtualization allows multiple users to access the services of cloud simultaneously. In turn Virtualization is made possible by a software popularly known as Virtual machine monitor (VMM) or Hypervisor. The VMM allows installation of multiple Virtual machines (VM's) or guest operating systems on the similar underlying architecture. This feature fosters many complications in the Cloud paradigm such as VM image shearing, VM isolation, VM escape, VM migration, VM rollback [1].

E. Lack of user control over data

Although Cloud ensures security to the user data, but it does not let user to have full control over it [1]. There is always a risk that the data may be accessed by some unauthorized user [5]. Also the CSP may breach the security, by using the user data for advertisement purposes. In case of multitenancy, where the data may be used by multiple users, and if user wants to dispose of the data he may not be able to do it, as it may be used by other users. All these factors arise because user is not solely controlling his data.

F. Trust issues

"Trust is a psychological state comprising the intention to accept vulnerability based upon positive expectations of the intentions or behavior of another" [5]. Trust issues arise because the CSP's are not able to completely secure their data. Even though most of the individuals or organizational business is being run by the Cloud paradigm, still most of people are preferring the on premise traditional computing. Therefore, when it is clear to the customer that his data might not be fully secure, it leads to a chain of suspension and distrust.

IV. COUNTERACTS TO THE INSECURE CLOUD PARADIGM

In the aforesaid sections various kinds of risks and threats have been mentioned. In order to prevent the Cloud computing model from the security risks, and to deliver risk free services to the cloud subscribers, various methodologies discussed in many works can be implemented. In this section some of the countermeasures are entailed, but in IT industry it is impossible to develop a clear countermeasure to overcome any risk [7].

A. Separation of duties

Separation of duties (SOD) refers to fact of system's ability to distribute a task into subtasks, and assign them to different computing or processing units. The purpose is to eliminate the conflicts among various computing units based upon their roles and to assure that a single users doesn't enjoy all the privileges. Till now there is no standardization of roles in the cloud paradigm, as the emerging roles and methodologies are not clearly defined yet. For the current situation there is not that much of support being provided for SOD, as the security is being provided for single domain. So, one step towards secure cloud architecture is to implement Separation of duties [6].

B. Auditing and client control

Till now there is no such auditing method present at the Cloud architecture, but if implemented it will result in a much secure and trusted computing platform. There is great need to implement internal auditing as well as external auditing, so that there will be a complete shift from traditional computing to cloud computing hence, make it widely acceptable computing model [5]. The auditing can be performed based upon below mentioned views.

1) *From architectural point of view [3]:*
   - How does the CSP achieve Multitenancy for different Cloud subscribers and services?
   - How are guest operating systems (VM's) deployed and secured?
   - In future, is the CSP going to add some feature that would contrast to our likes?
2) *From confidentiality point of view [3]:*
   - Is there any way that CSP admin can illegitimately access our confidential data?
   - Is there any way that other tenants can peep into our data?
   - To what extent is the data going to remain secure and confidential from third party?
3) *From integrity point of view [3]:*
   - How to be aware that CSP is doing the computations correctly?
   - How to believe that CSP is going to store our data without any modification?
   - How monitoring and service repairing is done at architectural level?
4) *From availability point of view [3]:*
   - Will critical systems go down, if CSP is attacked by some malicious user for Denial of service?
   - Will data be replicated without my consent?
   - How quickly can the CSP recover?

C. Proper Sanitization

Sanitization in context of security can be defined as the process of cleaning the confidential data from the Cloud resource when the same data is under threat that it will become public to others. It is one among the serious concerns which is hindering the complete switch from traditional computing to cloud computing. Now a days monitoring and tracking mechanisms have become so common in tracing out the information related to any cloud subscriber, and it can be minimized if the data is properly disposed of. Google is having some data sanitization mechanisms where they physically destroy the hard disks in order to avoid data leakage, but if the data sanitization problems are not so

effective, it will result in an unbearable data loss. The multitenancy along with the resource pooling and elastic features of cloud enable the resources to be shared among multiple tenants, hence it signifies one resource allocated to one tenant shall be assigned to other at other instant of time. This paves a way for the malicious users to breach the Confidentiality and integrity of data. Moreover the process of data recycling should minimized, and data repatriation be done in an efficient way, so that the cloud subscriber will completely trust the platform [2].

D. Encryption Protocols

From the layman's point of view, if he is asked for data security at cloud, he will suggest for encryption of the data. To a greater extent the security issues will be minimized if the data is being encrypted but, the issue with this methodology is that the computation speed will greatly be decreased and the purpose of cloud will no longer remain stand. Even though the encryption process is an effective step in terms of attaining the security, so the encryption should be performed only on confidential data, rest should be kept unencrypted. The mostly used encryption protocols are AES and Blowfish [7], [5]. The following two encryption methods can be performed:

1) Predicate encryption: In this method the master keys are distributed with the tenants, and each owner is having a very precise access to the encrypted data, so that only desired information is made accessible to a user [7].

2) Homomorphic encryption: This method is most efficacious, the encrypted data is being processed without decrypting it. Therefore, the computation time is decreased and hence the response time gets marginally reduced, without wasting any time on the encryption decryption cycle [7]. This method allows a limited number of operations to be performed on cipher data.

3) Attribute Based Encryption: Attribute Based Encryption (ABE) is another approach to deal with the confidentiality of data, based on the Public Key Encryption and Identity based encryption (IBE).It allows the public key to be any arbitrary string of the user, containing number of attributes related to the user itself. For example the attributes can be name, email id, contact number of the user. It works on the fact that only the legitimate person who would be knowing all the attributes of the user shall be able to decrypt the cipher text, thereby enhancing the data confidentiality.

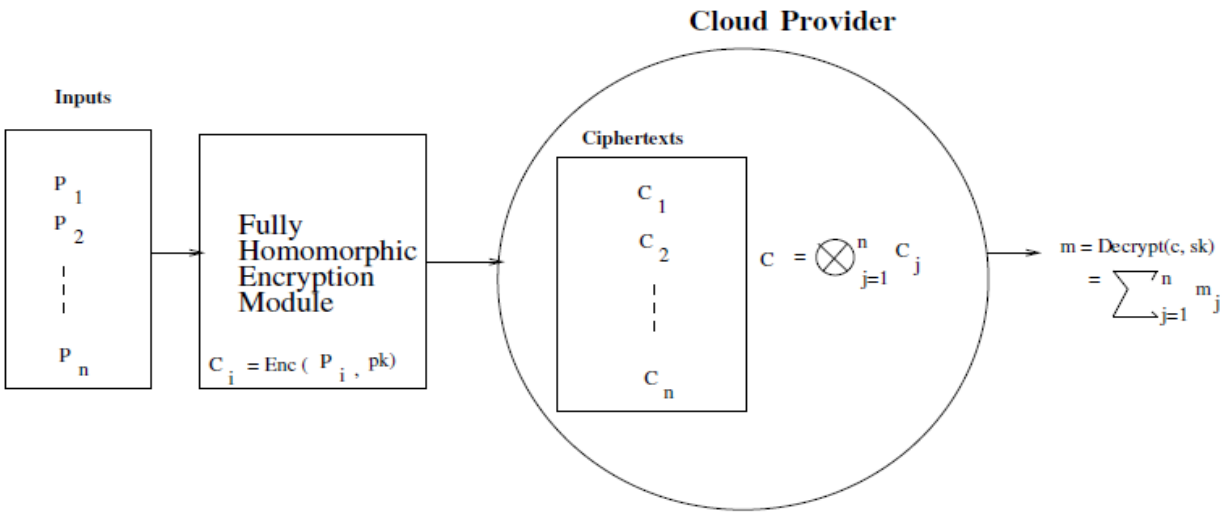

Figure 3: FHE processing on Cloud [9].

E. Fully Homomorphic Encryption

In order to overcome the shortcomings of Homomorphic encryption Fully Homomorphic Encryption method was developed. FHE is able to perform random operations on Cipher data, hence leading the Homomorphic Encryption. The cipher data is being processed on the Cloud architecture as per the user request without decrypting it. Consequently the data doesn't get revealed to the advisory. It processes the data without any approach to the secret key and without learning results. Therefore, preserving the very purpose of Cloud Computing and user data as well. However, till now the concept of Homomorphism is a theoretical concept [9].

In spite of the fact, Homomorphism seem to be very advantageous, but implementation of this concept is quite difficult, because in practice it requires compilation of complex circuitry for the given algorithm. FHE schemes are circuit based i.e. the changes in the algorithms need to be implemented at the circuitry level. Moreover the algorithms need to be translated so that they can process data in encrypted domain as well [9]. Figure 3 reproduced from [9] illustrates the FHE encryption on the Cloud architecture.

F. Trusted computing

Trusted computing refers to the techniques and methods to overcome the security issues and to develop a threat free computing paradigm, implemented though enhancements either in hardware or software, or both. The trusted computing consists of two basic concepts as shown in the figure 3 reproduced from [7].

*1) Transitive trust:*Transitive trust refers to a computing system, which can boot from a CRTM (Core Root of Trust Measurement), which may be a microcode, a hardware chip, ROM module, encrypted firmware but signed by a certified authority. So, the initialization will follow a pathway

through the bootstrap, where one level of initialization can implicitly trust that previous level is a secure microkernel [7].

E.g. CRTM→ BIOS→ OS loader→ OS→ Application.

2) Platform attestation: In case of platform attestation a computing platform proves to a third party that it is a trusted platform. Although it seems a genuine technique to check the trustworthiness of any computing platform, yet it suffers from some challenging tasks. The most challenging task is

to formulate a framework of sensible and quantifiable metrics that can be used to decide whether a computing platform is trusted [7].

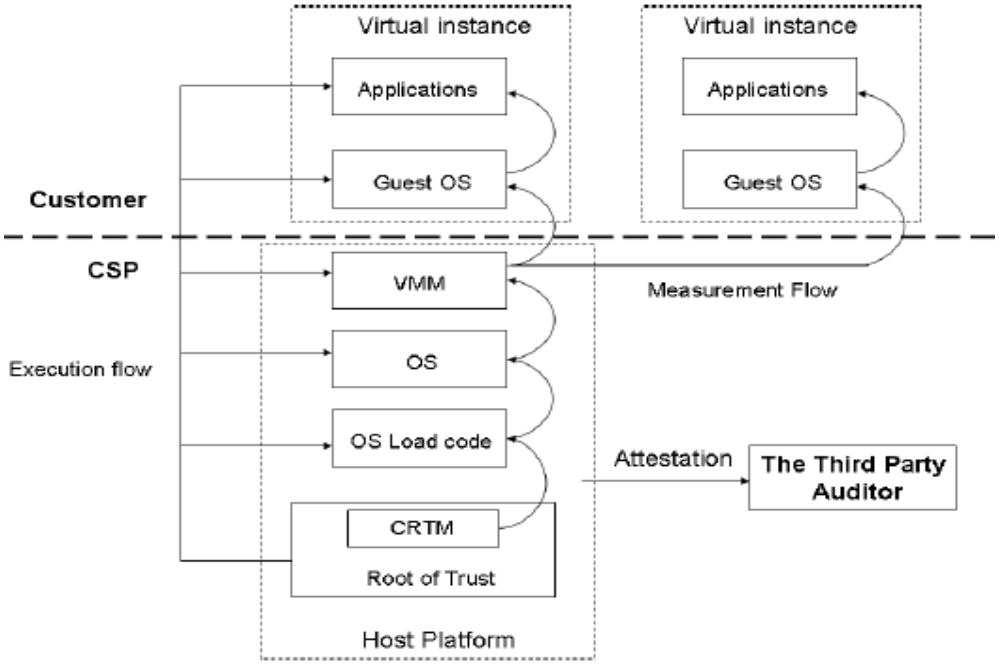

Figure 4: multi-tenant trusted computing environment model (mtcem) [7].

V. CONCLUSION

Cloud computing is no doubt serving the IT industry beyond expectations by giving almost "Everything as a service", but its exponential hype is being hindered by the security, privacy and trust issues. Despite of the advancements in virtualization of resources, availability of services, CSP's are lagging in the responsible management of confidential data and auditing of Cloud Service Provider. Besides the fact that if CSP would provide security to the end user and tenant, the security tools will gather more information about them, therefore privacy is at stake. Hence we can say there is tradeoff between the security and privacy issues. While subscribing to the services provided by CSP, a cloud subscriber must know about the security and privacy policies of the CSP, so that they can decide whether they should opt for the concerned CSP. Identifying the security issues and implementing appropriate counter measures will assist business organizations to pave the way for a trusted computing, and will encourage more subscribers. Hence if there is amendment in the architectural and security policies of Cloud paradigm in the form of proper isolation, auditing then this computing paradigm would gain extreme attention by of shifting every business from on premise to of premise.

VI. ACKNOWLEDGEMENT

Firstly, I would like to express my sincere gratitude to my advisor Dr Assif Assad for continuous support in writing this manuscript and related work. I could not have imagined having a better mentor than him. I would also like to thank my guide M Abdul Jawad for his patience and immense knowledge which motivated me to do this work. Last but not the least I would like to specially thank to my parents who are always there for me like a strong pillar.

VII. REFERENCES

[1] M. Ali Samee, U. Khan, and Athanasios V. Vasilakos "Security in Cloud computing: opportunities and challenges", Information Sciences, vol 305, pp 357-383, 7 Feb 2015.

[2] Diogo A.B. Fernandes, Liliana F. B. Soares, João V. Gomes, Mário M. Freire, Pedro R. M. Inácio "Security issues in Cloud computing: A Survey", Information security, vol 13, pp 113-170, 2017.

[3] Paul.G.Dorey. "Multitenancy security risks" 2014.

[4] K.Ren Cong Wang, and Qian Wang "Security challenges for Public Cloud", IEEE Computer Security, vol 12, pp 69-73.

[5] S. Pearson, A. Benameur. "Privacy, Security, and Trust Issues arising from Cloud computing", 2nd IEEE International Conference on Cloud Computing Technology and Science, pp 693-702, 2010.

[6] V.Varadharajan, U.Tupakula. "Security as a service model for Cloud environment", IEEE transactions on network and service management, vol. 11, pp 60-75, march 2014.

[7] W.J.Brown Vince Anderson, Qing Tan "Multitenancy security risks and countermeasures".

[8] Xiao-Fang Liu et al. "An energy efficient Ant Colony system for virtual machine placement in Cloud computing", IEEE transactions on evolutionary computation, vol. 22, no. 1, pp 113-128, February 2018.

[9] Ayantika Chatterjee and Indranil Sengupta." Translating algorithms to handle fully Homomorphic encrypted data on the Cloud", IEEE Transactions on Cloud Computing, 2015.

[10] Karim Zkik et al. "A new authentication and Homomorphic Encryption as a service model for preserving privacy in Clouds", Journal of Computer Science, vol 13 (12), pp702-717, 2017.