I.J. Modern Education and Computer Science, **2015, 8, 38-47**
Published Online August 2015 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijmecs.2015.08.05

Data Protection Techniques for Building Trust in Cloud Computing

Muhammad Yousaf Saeed, M.N.A. Khan
Shaheed Zulfikar Ali Bhutto Institute of Science and Technology, Islamabad, Pakistan
Email: yousafsaeed13@live.com, mnak2010@gmail.com

Abstract—Cloud computing has played much important role in comparison to other fields of IT, in providing Data storage, Data security, Quality of Services (QoS) etc. In the last few years, it had emerged and evolved so quickly due to its number of facilities and advantages to the organizations and end users. Many data security factors have also increased due to this fast evolution of cloud in the IT industry. Therefore several security models and trust establishing techniques have been deployed and are been in execution for providing more security to the data, especially the sensitive data. Despite of that much security, many of the models/techniques lacks in one or more security threat measures. In this paper a new model have been designed and proposed which introduces Security Aware Cloud. First the trust of the user or organization is established successfully on cloud than the security to the data is granted through privacy and encryption module. Level of quality of service and security are achieved under the Contract Trust layer while the Authentication and Key Management are covered under Internal Trust layer. For critical data privacy and encryption, Homomorphism mechanism is used. By the use of proposed trust and security model, we can enhance Return on Investment factor in the cloud for the data security and service provided by it.

Index Terms—Cloud Computing, Cloud Data Security, Cloud Trust Platform, Security Aware Cloud, Trusted Platform Module.

I. Introduction

Cloud computing is an Internet centered service which offers a new technique to use huge amount of shared resources available on the Internet. It is a potent and a flexible service spreading its wings on IT industry at a very fast pace. It enables services to be consumed easily as and when needed. This archetype has developed substantial interest in the corporate sector and the academia world, and is changing the way to do business. The services of cloud computing are provided across the entire computing spectrum. Organizations with big infrastructures are moving and extending their business towards cloud computing to lesser their price & to have clear vision & focus of best technology managers for creating strategic differentiation, they are to be freed. In this cloud, the ultimate consumers who use the services of cloud do not need anything to connect or equip themselves and their hardware with anything and they can have access to their data just through the Internet connectivity. There is a cloud service provider who facilitates services and manages those services in the cloud. The cloud provider facilitates all the services over the Internet and as a return the end users use services according to their business needs and pay the service provider accordingly. The services provided by the cloud vendors are basically based on the different number of implementations. There can be three main types of cloud computing services which the provider facilitates with.

These are Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). In SaaS, also known for software on demand service, the related data and its software is spread on the cloud by the service provider and the user can access and use it through any web browser he/she works with. In platform as a service, the service provider facilitates the user with set of software. Also PaaS is popular for providing solution stack over the platform. In infrastructure the cloud service provider facilitates the users with virtual machines, servers and storage to enhance their business capabilities. Like types of cloud services there are cloud types also which are private, public and a hybrid cloud. A private cloud is a cloud in which only the authorized users can use and access the services provided by the provider. In pubic cloud anybody can use the cloud services whereas the hybrid cloud contains the concept of both public and private clouds. Though cloud computing can save an organization's time and money but trusting the system is very much important because the real asset of any organization is the data which they share in the cloud to use the needed services either by putting it directly in the relational database, or eventually in a relational database through an application.

Cloud computing brings a number of attributes that require special attention when it comes to trusting the system. The trust of the entire system depends on the data protection and prevention techniques used in it. Numerous different tools and techniques have been tested and introduced by the researchers for data protection and prevention to gain and remove the hurdle of trust but there are still gaps which needs attention and are required to be lined up by making these techniques much better and effective.

Cloud computing is rising with a very high pace because of its countless benefits like reduction of the cost

of the IT infrastructure, high availability, excellent performance, etc. Organizations are moving towards the adoption of the cloud computing services with keen interest. In the cloud computing the end users don't need to install the software's or applications in their computers and they can access their data or files remotely from any computer through the internet. There is a cloud provider who manages the cloud and will provide the cloud services to its users. The cloud provider operates the cloud data center and manages its resources. In the cloud computing, all the storage and processing is done at the cloud data center. By a payment of a certain amount, you can achieve and get every solution on the internet in form of a service. You can use the service for minutes, hours, days or months according to your needs on a utility basis.

The services that are provided by the cloud providers are of three types which are: software as a service, infrastructure as a service and platform as a service. In the software as a service a user can access different software's and applications from the cloud provider by using a web browser. A user don't need to install the software, he'll get an instance of the software running in the cloud data center on his machine. In the infrastructure as a service a user can get the hardware as a service from the cloud data center. The hardware can be memory, disk space, processing power, etc. The user will use the hardware for as much duration as he wants and will pay for it. The demanded hardware will be allocated to the user in the cloud data center. In the platform as a service, the user will be provided with the set of software's, development tools or a platform. And by using that platform a user can develop or create different applications and products. A user can use different API's available at the cloud provider's end.

The fast speed Internet and different virtualization technologies have given emerge to the concept of cloud computing. The cloud can be a public, private or hybrid. In a public cloud anyone can by the services of a cloud through the internet. The private cloud offers services to a limited number of users. While the cloud the mixes the features of both public and private cloud is known to be hybrid cloud. Privacy & security are the main factors and problem of the quickly growing cloud. Reducing cost is mandatory but the information and data of the organizations are users are the backbone of the organizations and no one will ever want to give it in the custody of others without the proper proofs. The users will need to authenticate themselves for accessing the cloud resources and the identity of the user is critical to the success of the cloud computing.

II. Security Problems of Cloud Data

Cloud implements three major types of services SaaS, PaaS and IaaS to the end-user. In these service models different levels of security are provided in cloud computing environment. Efficient security technology in cloud computing is required to have proper secured cloud computing and to speedup cloud implementation. The security element in SaaS service model such data security, data integrity, identity management, data location, data availability, etc., are to be considered for better data security in cloud computing.

a) Data Security and Data Protection

Guarantee should be provided to the data that has been hosted by the consumer or the client of the cloud that it is safe from the unauthorized access and use and only authorized users are limited to it**.** There are many other risk and hazards posing potential to the data in cloud such as an authorized & unfortunate access to the sensitive and private data of the cloud client or customer.

b) Data/Information Reliability

Security provided to the cloud customer's data by the cloud vendors or CSPs should provide implementation that would have the methods, tools and procedures for ensuring data reliability and methods for explaining the cause that created threat to the data at a certain time and point. Strict and careful records are necessary for what type of the data has been positioned and located in the public cloud. The existence of such type of requirement for data reliability, the maintenance for the protection and basis of data or information is necessary in accordance to prevent damage or disclosure of data away from the agreed zones.

c) Data Locality and Repositioning

Highest degree of flexibility is being offered in cloud computing. The location and position of the data in cloud is not always been known to the consumers and users of cloud. The position and location of the data is to be known to the enterprises and organization when it is the case of sensitive data because organizations need the information of their private sensitive data that where it is stored, what are the methods used for its security etc. For such type of mechanism a predetermined or contractual pact or contract is being signed between the client and CSP that ensures that the data will be residing and placed at a specific known data server. Movement of data is done from one location to another in the sense to provide more security to the data in cloud. Service Level Agreement (SLA) is a type of agreement or a contract between the cloud providers through which they use the resources of each other.

d) Data Accessibility

The data of the client or customer stored in cloud are mostly in the form of pieces known as chunks that reside on different servers located at different locations. Whole establishment becomes comparatively hard and challenging in the case where data accessibility is the real major issue. Therefore, providing correct and appropriate data availability and accessibility to cloud authenticated user becomes more important for the CSP.

e) Identity Management

The cloud provider should provide an identity management system for providing authentication and authorization. This is an important issue for both provider

as well as user in a cloud computing environment. While providing authentication and authorization, an independent IdM stack, credential synchronization, federated IdM has implemented.

III. Literature Review

The cloud computing platform facilitates huge amount of shared resources to various organizations all over the world on the Internet. Shen *et al.* [1] analyzed requirement of security services in cloud computing. The authors proposed a solution for cloud services and build a model of cloud on trust based platform. This model integrate the cloud services for trusted computing platform TCP and trusted platform support services TSS whose basis is on trust component/module. In the last few years, it had emerged and evolved so quickly due to its number of facilities and advantages to the organizations and end users. Many data security factors have also increased due to this fast evolution of cloud in the IT industry. Therefore several security models and trust establishing techniques have been deployed and are been in execution for providing more & more security to the data, especially the sensitive & private one. Despite of that much security, many of the models/techniques lacks in one or more security threat measures. Neisse *et al.* [2] have focused on a system of cloud computing that permits review and requirement focused reliability dimensions and distant vital points of attestation for cloud organizations. They build a system that should be applied for Ven platform of cloud computing and also guaranteed trusted technologies that provides security. This system analysis the various related scenarios of different attacks to evaluate that computing in cloud is created on trust. The infrastructures of cloud normally necessitate that stake holders transfers data into cloud based on trust. The frame work that the authors presented in this research has various benefits. According to the scalability and economic point of view, this model provides extra services for cloud computing on trust base. The model is based on various layers. These are cloud computing model, design, security performance and implementation. Xen platform is used for cloud model. The design of this framework shows the working functionalities of physical hosting service on narrow level and shows history for storage.

In this implemented model the author has used some techniques which include integrity management engine, attestation configuration, tamper detection and trusted boot. This model is fully secured and trusted. This model guarantees the security of all kinds of data in form of folder, reports and fields. System should not be overloaded when DoS command attack occur. In this research, the authors present a solution for malicious problems for cloud customers. He also monitors integrity of files and data on Xen cloud platform.

Data's safety, privacy and trust in cloud environment is the main point for its broader adoption. Yeluri*et al.* [4]have focused on cloud services according to the security point of view and explore the major challenges of security in cloud at deploying the services. In this research, the authors discussed software vendor and hardware related security issues to enhance the control on cloud services. The authors used a case study of Intel TXT hardware platform for the verification of secure and trusted cloud computing services. They proposed a solution for cloud computing security and for hardware root of trusted computing chain. The methodology that is used for cloud secure is based on the main general three services of the cloud. Authors elaborated following key points and drivers for cloud security, which are identity management, data recovery and management, security in cloud confidentiality, trust, visibility, and assurance and application architecture. They used trusted computing chain that protects cloud data from un-trusted software. Also prevented from unsafe virtual machines, the propose solution for hardware used trusted computer pools and remote attestation. The model proposed by the authors in ensure the security of cloud computing and its services to build a trust.

Behl [5] focused on main security encounters in cloud architecture and environment and had discussed methodologies to cover drawbacks of security problems in cloud architecture and environment. Overall picture of grid computing has been changed by cloud computing. Distribution of data is a new way of cloud computing. In this research, the author proposed a solution for cloud security, complex distributed computing, security strategy, security concerns, and drawback of security challenges. The challenges discussed by the author are insider threats, data loss, service disruption, outside malicious attacks and multi-tenancy issues. There are various challenges for cloud security, but the author proposed a solution for protecting these issues for cloud computing. This research develops comprehensive strategy to face the challenges in cloud security.

Chen *et al.* [6] has focused on analysis of confidentiality and data sensitivity & security problems in cloud architecture and environment covering all the stages of life cycle of data. In this study, the authors elaborated privacy protection, data security, data segregation, cloud security and cloud computing. They have analyzed these issues and also provided a solution for resolving these issues. These issues are primarily at SPI (SaaS, PaaS, IaaS) level and the major challenge is data sharing. After the analysis of data security and privacy the comprehensive solution is to meet the need of identification and isolation of data is primary task ate design level of cloud based applications.

Cloud computing [7] provide us a podium to use a wide range of services that are based on the internet to deal with our industry procedures & various services of Information technology. But besides its all advantages it also increase the threat for security when a TTP (Trusted Third Party) is involved. By involving a TTP (Trusted Third Party) there is still a chance of heterogeneity of Users which effects security on a cloud. In this research, the authors propose a TTP (Trusted Third Party) independent approach for IDM (Identity Management) with the capability of using unique data on unreliable

clouds. Using predicate data over the encoded data and using multi organization calculation and computing and active bundle scheme are the approaches used here. In this scheme the bundle has self-reliability checking procedure, it include PII, protection mechanism, privacy policies and virtual machine for policy enforcement of these policies. The resolution lets the use of IDM solicitation on unreliable clouds.

Cloud computing is very effective security service that is based on conceptual technology. Data retrieval and safety of the security of data is the main issue in cloud architecture and environment. Kulkarni *et al.* [8] have focused on secured cloud services and protection of data by using encryption and decryption techniques at services level. In this research, the authors have highlighted the security threats for cloud computing and also explained techniques to avoid from these threats. In the last few years, it had emerged and evolved so quickly due to its number of facilities and advantages to the organizations and end users. Many data security factors have also increased due to this fast evolution of cloud in the IT industry. Therefore several security models and trust establishing techniques have been deployed and are been in execution for providing more & more security to the data, especially the sensitive & private one. Despite of that much security, many of the models/techniques lacks in one or more security threat measures. In this paper a new model have been designed & proposed which introduces "Security Aware Cloud". First the trust of the user or organization is established successfully on cloud than the security to the data is granted through privacy and encryption module. Level of quality of service and security are achieved under the Contract Trust layer while the Authentication and Key Management are covered under Internal Trust layer. For critical data privacy and encryption, Homomorphism mechanism is used. Cloud data runs on a network and due to the fact it creates a chance to attack on it. To avoid cloud data from threats the authors proposed the following protection mechanism. Access management and identity features should be authorized, protect server and networks, data storage security, security as a service, security of browser, authentication of users and lock in and data leaking.

Shuanglin [9] have focused on management policy for data security in cloud computing. The authors elaborated management policy and ensure that the internal data needs strong authentication and sensitive information must be filtered. Cloud is an internet bases service and all the data is on networks. In this research, the authors design a policy for data protection of cloud clients. When data is on public cloud then protection of data is complex issue. The policy that the authors design based on following methods. These are: Authentication technology, Visualization of Sensitive data, and technical support sections, filtration of sensitive data, establish safe management system, cloud computing gateway and classification of data evaluation.

Squicciarini [10] has focused on problems disclosure and damage to the sensitivity of data's privacy in cloud computing. Cloud computing provides a highly sensitive services on internet to individuals or large organizations. User worry about the leakage of data and loss of privacy in cloud service. In this research, the authors proposed a three tier solution to prevent from data leakage and privacy loss. These tiers are: lower protection, medium protection and strong protection. According to the researcher the strong protection tier prevents sensitive data of user profile from service provider. Medium level tier prevents from indexing effectiveness. The last protection tier forces user to obey the policy of cloud data. The authors proposed a new technique for the prevention of data leakage and loss of privacy and this technique is helping toward the seven tier protection techniques.

Cloud computing provides a new business services that is based on demand. The cloud networks have been built through dynamic virtualization of hardware, software and datasets. Hwang and Li [11] focused on trust in cloud computing on the basis of secure services. The authors explained the protection procedures to build trust in cloud computing. They discussed about cloud platforms, cloud service provider and security features for these services. They proposed a reputation management trust model that defined the different areas which were based on the different phases of cloud computing. Data coloring mechanism and secure data access mechanism is discussed by the authors in this paper and used the same mechanism for their framework. Cloud security infrastructure and the trust reputation management play a vital role to upgrading the cloud services. Iqbal et al. [13, 14] proposed performance metrics for software design and software project management. Process improvement methodologies are elaborated in [15, 16] and Khan et al. [17] carried out quality assurance assessment. Amir et al. [18] discussed agile software development processes. Khan et al. [19] and Khan et al. [20] analyzed issues pertaining to database query optimization and requirement engineering processes respectively. Umar and Khan [21, 22] analyzed non-functional requirements for software maintainability. Khan et al. [23, 24] proposed a machine learning approaches for post-event timeline reconstruction. Khan [25] suggests that Bayesian techniques are more promising than other conventional machine learning techniques for timeline reconstruction. Rafique and Khan [26] explored various methods, practices and tools being used for static and live digital forensics. In [27], Bashir and Khan discuss triaging methodologies being used for live digital forensic analysis. References [28-44] reviewed different techniques in different domains and reported their critical evaluations along with a workable framework where necessary.

IV. HOMOMORPHISM

Securing the data in the databases, whether they are in traditional environment or cloud environment, has remained the major concern and issue in the field of IT. In this regard Encryption approaches and schemes have played a very effective and efficient role. These

encryption schemes and approaches have been helpful in Cloud environment where we didn't need to involve the 3rd party in the transaction and interaction b/w the client/user & cloud server. One of encryption known as the Homomorphic Encryption is the best in this regard because without knowing or having the knowledge of the private key, this encryption can perform operation and computation on the encrypted data. This encrypted data or the result of the encrypted data, which is also in the encrypted form, is decrypted with the secret reserved key which authenticated user/client have. When the results of this encrypted data are decrypted and matched with the original results, they appeared to be same. This states that through Homomorphic encryption we can store and retrieve the data in the encrypted form in the cloud and also can perform computation on it, which will be useless for the unauthorized user because all the work to be done is in the encrypted form, in fact the results the user gets is also in the encrypted form. The main flavor of the Homomorphic encryption is that the user has the access to deal with the encrypted cipher data directly without the intervention of any kind of 3rd party or any administrator authority body. The user can also assure the security of the data whereas anyone who didn't know the secret private key can't access the data or can decrypt it.

Moreover the Homomorphic encryption is further divided in two categories according to its behavior, i.e. Partial Homomorphic Encryption (PHE) and Full Homomorphic Encryption (FHE). However PHE have been somehow implemented and been practical used in the cloud computing but the FHE has not been implemented or been used practically due to its huge number of processing and computations which involves large and heavy resources to carry out this operation. In PHE the encryption method or operation used in any single one, i.e. whether it will perform additive Homomorphic encryption or multiplicative Homomorphic encryption. Whereas in the FHE the operation to be performed are single or the combination of more, i.e. it can be multiplicative or additive or combination of both such as NAND or XOR. But FHE, no doubt, is more powerful in security aspect as compared to PHE but because of requiring a much lot or computation processing it has not been implemented. As of FHE it has been theoretically, mathematically and empirically been proven to be more secure and threat proof than other encryption schemes been in use.

The idea and the concept of Homomorphic Encryption was first introduced and suggested in 1978 by the three scientists named as Ronald Rivest, Leonard Adleman and Michael Dertouzos. Since the introduction of the Homomorphic encryption, scientists began to work on the encryption schemes to reach the level of Homomorphism in their encryption schemes. Most of the encryption schemes had also reached in providing maximum level of security and privacy. These encryption schemes were either Additive Homomorphic or Multiplicative Homomorphic but neither the combination of both. The problem of being PHE or a single type of Homomorphic is that it can only perform one type of operation on the encrypted data, i.e. additive or multiplicative. If the combined operation of both were needed then these encryption were little useless or helpless. Additive Homomorphic encryptions are the Pailler and the Goldwasser-Micalli encryptions whereas the Multiplicative Homomorphic encryptions are RSA and ElGamal encryptions. For the first time in 2009 the idea and the concept of Full Homomorphic Encryptions (FHE) was proposed and introduced by Craig Gentry who used Ideal Lattices for this purpose. The advantage and merit of Fully Homomorphic Encryption is that it can perform computations and operations (number of Additions & Multiplications) on encrypted data. The main flavor of FHE lies in the fact that the results and the calculations of the sensitive and private data can be outsourced while the secret key is kept safe with the authorized user/client.

However PHE have been somehow implemented and been practical used in the cloud computing but the FHE has not been implemented or been used practically due to its huge number of processing and computations which involves large and heavy resources to carry out this operation. In PHE the encryption method or operation used in any single one, i.e. whether it will perform additive Homomorphic encryption or multiplicative Homomorphic encryption. Whereas in the FHE the operation to be performed are single or the combination of more, i.e. it can be multiplicative or additive or combination of both such as NAND or XOR. But FHE, no doubt, is more powerful in security aspect as compared to PHE but because of requiring a much lot or computation processing it has not been implemented. As of FHE it has been theoretically, mathematically and empirically been proven to be more secure and threat proof than other encryption schemes been in use. The problem of being PHE or a single type of Homomorphic is that it can only perform one type of operation on the encrypted data, i.e. additive or multiplicative. If the combined operation of both were needed then these encryption were little useless or helpless. Additive Homomorphic encryptions are the Pailler and the Goldwasser-Micalli encryptions whereas the Multiplicative Homomorphic encryptions are RSA and ElGamal encryptions. For the first time in 2009 the idea and the concept of Full Homomorphic Encryptions (FHE) was proposed and introduced by Craig Gentry who used Ideal Lattices for this purpose. The advantage and merit of Fully Homomorphic Encryption is that it can perform computations and operations (number of Additions & Multiplications) on encrypted data. The main flavor of FHE lies in the fact that the results and the calculations of the sensitive and private data can be outsourced while the secret key is kept safe with the authorized user/client.

The services that are provided by the cloud providers are of three types which are: software as a service, infrastructure as a service and platform as a service. In the software as a service a user can access different software's and applications from the cloud provider by using a web browser. A user don't need to install the software, he'll get an instance of the software running in the cloud data center on his machine. In the infrastructure

as a service a user can get the hardware as a service from the cloud data center. The hardware can be memory, disk space, processing power, etc. The user will use the hardware for as much duration as he wants and will pay for it. The demanded hardware will be allocated to the user in the cloud data center. In the platform as a service, the user will be provided with the set of software's, development tools or a platform. And by using that platform a user can develop or create different applications and products.

In the last few years, it had emerged and evolved so quickly due to its number of facilities and advantages to the organizations and end users. Many data security factors have also increased due to this fast evolution of cloud in the IT industry. Therefore several security models and trust establishing techniques have been deployed and are been in execution for providing more & more security to the data, especially the sensitive & private one. Despite of that much security, many of the models/techniques lacks in one or more security threat measures. In this paper a new model have been designed & proposed which introduces "Security Aware Cloud". First the trust of the user or organization is established successfully on cloud than the security to the data is granted through privacy and encryption module. Level of quality of service and security are achieved under the Contract Trust layer while the Authentication and Key Management are covered under Internal Trust layer. For critical data privacy and encryption, Homomorphism mechanism is used.

V. Proposed Model and Framework

This section proposes a cloud trust model for the security of data in the cloud. The proposed trust and security model is a combination of several component and modules which will be discussed in detail below. Moreover we have developed a Security Aware Cloud which will be residing in the general cloud. All the Service providers and Service integrators that will come under the proposed model will be residing under this Security Aware private Cloud. The interest on the basis of which trust would be establishing will be relying and based on the internal trust in this private type cloud. Moreover the root of trust for measurement in the proposed model will be put on the hardware rather than the software. Although level of security and Service's quality is also controlled by the Contracted trust.

A. Security Aware Cloud

This is a type of private cloud which is not the same to the present current clouds in many ways. It differs from the general cloud services due to following trust layers:

a) Internal Trust Layer

Internal trust layer is defined as the platform which guarantees that the administration/operation in this layer is under usual internal control of an organization or user. This layer corresponds to Trusted Platform Module in the systems of the physical hardware components and devices. All the processes and the data that are to be monitored and cared by the company itself are resided and located in this layer. This layer only works correctly when it has been placed in an in-house competence. Key management is operated in this trust layer. By putting key management into internal trust, an assumption can be made by the company or the organization to controlling of data or processes when allowed to place the trust in this internal layer. Although all the data that are to be processed and computed in a more secure and safe way then these are to be done in the trusted platform module of internal layer. However, this can involve critical and sensitivity data that could cause harm to the user if got in wrong hands.

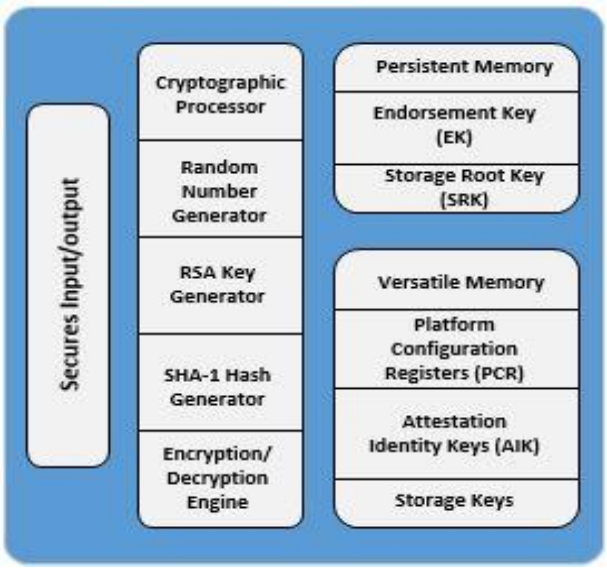

Fig.1. Trusted Platform Module

b) Contracted Trust Layer

This layer is the second point that the security aware cloud assumes and differs from the general cloud. Cloud services and their level are the main things that an industry or a company should have to be conscious of when talking about cloud. While all the contentions & statements given by a company or a user could be trusted or believed at a certain level. All the decisions could be made by the company or an individual user in the selection of a CSP for the representation of their services contingent to the CSPs service's quality with the contract through the evaluation of these services. A company or an individual could have the trust of a CSP to a limit which is included in the definition of an agreement or contract that had been signed. Furthermore, a cloud service provider could have it position in the circle of a trust of a user or an organization through the agreement of a service/practice policy or statement. A CSP could be invited to enter in the circle of a trust when a company come to an agreement on the basis of service/practice policy or statement. All the objects and unit that had not been defined in the service/practice policy or statement are not included in the circle of trust. Therefore cloud providers must be under the contracted layer.

c) Hard and Soft Trust

The security aware cloud in the proposed model also differ from the rest of the other general clouds in the way that it combines the hybrid trust approach, i.e. hard trust and soft trust. Hard trust is based on the strong validation while soft trust is based on the confirmation about past behavior. Hard trust is also defined as the trust that is derived from concrete security mechanisms such as validation of properties through certificates. Usually these certificates are characterized by certainty. Whereas on the hand soft trust is defined as trust that is derived from the past experiences and behavior associated with an entity. Soft trust mechanisms consider one's own direct experience with the other party in the past, recommendations from other or a combination of both. However trust saturation is a common problem with soft trust based approach. While hard trust may not be aware of dynamic changes. In this sense hard trust approaches are rigid, as they are usually based on single time check which when bypassed put the service platform in a vulnerable state. Combination of both hard and soft trust mechanisms in a hybrid model overcomes the limitations of these mechanisms used separately. Hence, a hybrid trust model is a good option to evaluate the overall trust on cloud service platforms as well as on service providers.

d) Handle & Caring of Data Criticality

Conservatively, due to imprecise and the lack of anxiety in the cloud security, cloud does not handle and control the criticality and operation of data. Private cloud can be one of the answer and solution to such type of problem. These type of clouds are usually created inside of a company or an organization. All the complete and total control is in the hand of the organization as this solution of private cloud covers one organization at a time. Enhancing the security of a publicly cloud could be a good solution as the creation and establishment of a private cloud could cost more to the organizations of a middle size. There is a strong a strict requirement that is needed by the supply of certain services to control and handle the operation of the criticality of data. All of these services could be achieved through a server which acts as an agreement or contract in between the company or an individual user and the CSP in a public cloud. Whereas, the services at the security and privacy levels could be delivered by the CSP. However, a company or an organization can shift or transfer the controls to its data to the cloud through the agreement of these level of services with which they are able to have optimization in the cost of handling the data.

e) Attestation Module

The procedure in which the accurateness of information is promised is known as Attestation. Platform's reliability is proved after the confirmation and verification to the extents of that platform. The register for the configuration of the platform that rely inside the trusted platform module can be used for the extension of the extents, and the key for the attesting of identification is used for the digital signature for theses registers inside of trusted platform module. Module of trusted platform is a type of cryptography processor for security and is the main and important component and part of trusted computing. All the data or information that is of less or more sensitivity is secured in the module of trusted platform, for example the keys for the crypto processes are been kept in the protected and isolated localities whose access is only granted by certain private and restricted commands which are known to authorized body.

One strategy goal of Attestation Agent module in our proposed cloud trust and security model is to provide the user or the client with the proof that they have full control over their requirements of cloud up to the satisfaction, and also the nominated trustworthy atmosphere run their dealings and trade successfully. For every individual client, the position and condition of all the corporal platforms and ASPs are been calculated and computed by this attesting agent whose basis basically is the methods of trustworthy computing. To provide isolation and limpidity to the clouds is another main aim and objection of this agent. The factors that doesn't affect the cloud provider or their influence on them is almost negligible are; configuration of physical platform, Virtual machine's version, etc. However, this type of informative knowledge could enhance the isolation of the cloud provider and clients could obtain this knowledge/information openly. Verification of such isolation and transparency can be done by this modular agent.

Applications and other software could be verified by this module that would be of excessive help to the clients of cloud. However there may be some software and applications such as the software for monitor, software for the measurement, etc. that may be greatly affecting the self-reliance and trust of the cloud's client. To resolve these type of problems, the development of such software should be made through the 3rd party and their accreditation should also be done through 3rd party experts. On the same lines as described above, clients are satisfied by this attesting module about the attestation for succession of the software.

DRTM: This module is an important component in TPM of our proposed model. Through the exclusion of some factors or components like, Bootloader or bios, benefits could be achieved in the reduction of trusted computing base. Trusted atmosphere could be achieved anytime through this module deprived of resetting the platform. Some other small concepts that have been utilized in our trust and security model of Cloud are as under.

Contract: The services provided and offered by the CSP are used and utilized by the organization or company based on the definition of service/policy statement. Moreover, CSP could have trust on the company when the organization offers its agreement on its statement.

Practice/Service Statement & Policy/Service Statement (SP/SPS): The services that are provided by the CSP are defined in this component. The range of security of services can be trusted by the company or

organization that has been defined is this component.

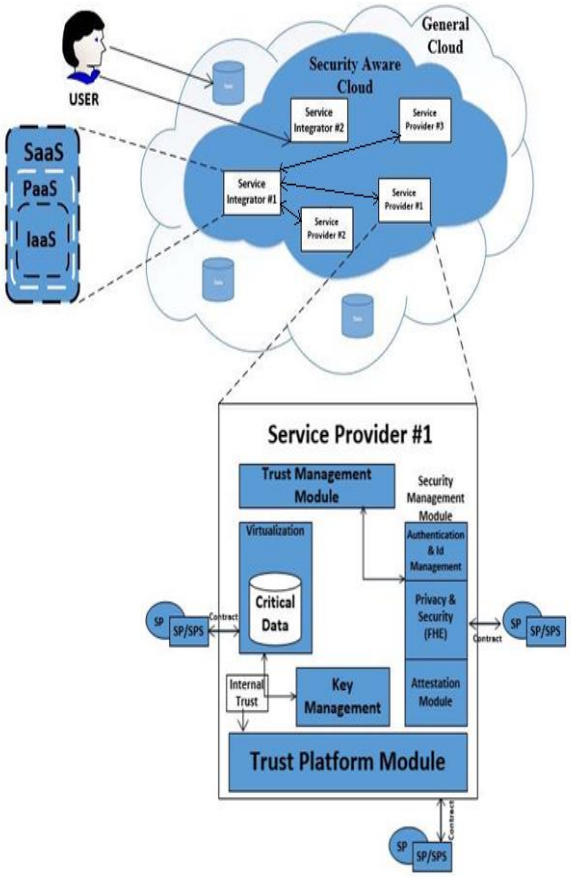

Fig.2. Cloud trust & Security Proposed Model

VI. VALIDATION

The proposed model was evaluated by first describing the security parameters and factors on the basis of which the trust is evaluated. Then weight was assigned to each and every security parameter described previously. These weights are further utilized in the calculation of trust of each security parameter. The average trust of these parameters is calculated to have an overall trust of a Service Provider. This overall trust of a Service provider is collected and integrated by the Service Integrator. The user interacts with the Service integrator which enlists the overall Trust percentage, based or calculated from the security parameters, of all the Service providers residing within the Security Aware Cloud. On the basis of the trust percentage shown to user by the Service integrator, the user then selects the Service provider according to their need and requirements.

Note that the overall Trust percentage is been calculated on the basis of weightage of security parameters provided by the Service provider. We validated our model by giving weights to the security parameters of some Service providers and in result of that we obtained different Trust percentages of every Service provider. Following are the three tables; one showing the weights to security parameter of each service provider given by us, the other describing the factors of each parameter on the basis of which percentage is calculated and the last showing the percentage of trust provided by each provider that have been calculated on the basis of first table.

$$\text{Trust \%age}\ (\text{SP}) = \frac{\text{parameter1}(\text{weight}) + \ \ldots\ . + \ \text{parameter1}(\text{weight})}{\text{Total Sum Weight of Security Parameters}}$$

Table 1. Weighting of Security Parameters

	Security Parameters					
	Software-level Security	Database Security	Network base Security	Encryption Algorithm	Physical & Personnel Security	Authentication & Identification
	25	**35**	**15**	**45**	**15**	**25**
SP#1	20	23	13	35	11	15
SP#2	11	30	07	43	09	23
SP#3	23	25	10	29	10	20

Table 2. Factors of Security Parameters

Software-level Security	Password Protection, Session Timeouts, Permission & Access,, etc.
Database Security	Integrity controls, Rows/Columns log monitoring, Auditing, etc.
Network base Security	Firewall, Hacking attempt rate, Switch & Intrusion Detection etc.
Encryption Algorithm	RSA, RC4, 3DES, AES(128/256), MD5, etc.
Physical & Personnel Security	Vulnerability matrix, Patrol logs, Motion detection, Alarms, etc.
Authentication & Identification	Kerberos, RADIUS, SSL, etc.

Table 3. Trust Percentage Evaluation

	TRUST PERCENTAGE						Total Avg. %age
	Software level Security	Database Security	Network base Security	Encryption Algorithm	Physical & Personnel Security	Authentication & Identification	
SP#1	80	65.71	86.66	77.77	73.33	60	73.91%
SP#2	44	86	46.66	95.55	60	92	70.70%
SP#3	92	71.43	66.66	64.44	66.66	80	73.53%

VII. Conclusion And Future Work

In evaluating trustworthiness of cloud service provider, validation of their claimed trust properties and consumer's satisfaction on the validation processes play a critical role. But cloud computing is still in its infancy and although trust and security issues are delaying its adoption. It is growing quickly and we need to provide trust and security mechanisms to ensure that cloud computing benefits are fully realized. To achieve all this, first it was analyzed that why we feel insecure against clouds. After analyzing, proposed model have been designed and presented which successfully establishes trust between the CSP and user/organization and then provide security to the data. A private cloud within the General cloud was established named "Security Aware Cloud" which compromises of different trust, authorization and security components. The connection between the user and security aware cloud is on contract bases while the connections among the components are Internal TPM hardware based.

The future work for the proposed model will be to make it more enhance, efficient and robust that it could also be manageable & provide trustworthy and security proof mechanism against the malicious and other vulnerable attack advancing in IT industry. Several researches on the concept of model proposed in this paper are in plan, such as the performance analysis and trust verification method on customers' side.

References

[1] Z. Shen, Li Li, Fei Yan, and Xiaoping Wu, "Cloud Computing System based on Trusted Computing Platform", International Conference on Intelligent Computation Technology and Automation (ICICTA), 2010.

[2] R. Neisse, Dominik Holling, and Alexander Pretschner, "Implementing Trust in Cloud Infrastructures", 11th IEEE/ACM International Symposium on Cloud and Grid Computing (CCGrid), 2011.

[3] Meiko Jensen, JorgSchwenk, Nils Gruschka, and Luigi Lo Iacono, "On Technical Security Issues in Cloud Computing", IEEE International Conference on Cloud Computing, 2009.

[4] Raghu Yeluri, Enrique Castro-Leon, Robert R. Harmon, and James Greene, "Building Trust and Compliance in the Cloud for Services", Annual SRII Global Conference (SRII), 2012.

[5] AkhilBehl, "Emerging Security Challenges in Cloud Computing", World Congress on Information and Communication Technologies (WICT), 2011.

[6] Deyan Chen, and Hong Zhao, "Data Security and Privacy Protection Issues in Cloud Computing", International Conference on Computer Science and Electronics Engineering (ICCSEE), 2012.

[7] RohitRanchal, Bharat Bhargava, Lotfi Ben Othmane, LeszekLilien, Anya Kim, Myong Kang, and Mark Linderman, "Protection of Identity Information in Cloud Computing without Trusted Third Party", 29th IEEE Symposium on Reliable Distributed Systems, 2010.

[8] Gurudatt Kulkarni, JayantGambhir, TejswiniPatil, and AmrutaDongare, "A Security Aspects in Cloud Computing", IEEE 3rd International Conference on Software Engineering and Service Science (ICSESS), 2012.

[9] R. Shuanglin, "Data Security Policy in the Cloud Computing", 7th International Conference on Computer Science and Education (ICCSE), 2012.

[10] Anna Squicciarini, SmithaSundareswaran, and Dan Lin, "Preventing Information Leakage from Indexing in the Cloud ", IEEE 3rd International Conference on Cloud Computing (Cloud), 2010.

[11] Kai Hwang, and Deyi Li, "Trusted Cloud Computing with Secure Resources and Data Coloring", IEEE Internet Computing, 2010.

[12] Ranjita Mishra, Sanjit Kumar Dash, Debi Parsad Mishra, and AnimeshTripathy, "A Privacy Preserving Repository for Securing Data across the Cloud", 3rd International Conference on Electronics Computer Technology (ICECT), 2011.

[13] Iqbal S., Khalid M., Khan, M N A. A Distinctive Suite of Performance Metrics for Software Design. International Journal of Software Engineering & Its Applications, 7(5), (2013).

[14] Iqbal S., Khan M.N.A., Yet another Set of Requirement Metrics for Software Projects. International Journal of Software Engineering & Its Applications, 6(1), (2012).

[15] Faizan M., Ulhaq S., Khan M N A., Defect Prevention and Process Improvement Methodology for Outsourced Software Projects. Middle-East Journal of Scientific Research, 19(5), 674-682, (2014).

[16] Faizan M., Khan M NA., Ulhaq S., Contemporary Trends in Defect Prevention: A Survey Report. International Journal of Modern Education & Computer Science, 4(3), (2012).

[17] Khan K., Khan A., Aamir M., Khan M N A., Quality Assurance Assessment in Global Software Development. World Applied Sciences Journal, 24(11), (2013).

[18] Amir M., Khan K., Khan A., Khan M N A., An Appraisal of Agile Software Development Process. International Journal of Advanced Science & Technology, 58, (2013).

[19] Khan, M., & Khan, M. N. A. Exploring Query Optimization Techniques in Relational Databases. International Journal of Database Theory & Application, 6(3). (2013).
[20] Khan, MNA., Khalid M., ulHaq S., Review of Requirements Management Issues in Software Development. International Journal of Modern Education & Computer Science, 5(1),(2013).
[21] Umar M., Khan, M N A., A Framework to Separate NonFunctional Requirements for System Maintainability. Kuwait Journal of Science & Engineering, 39(1 B), 211-231,(2012).
[22] Umar M., Khan, M. N. A, Analyzing Non-Functional Requirements (NFRs) for software development. In IEEE 2nd International Conference on Software Engineering and Service Science (ICSESS), 2011 pp. 675-678), (2011).
[23] Khan, M. N. A., Chatwin, C. R., & Young, R. C. (2007). A framework for post-event timeline reconstruction using neural networks. digital investigation, 4(3), 146-157.
[24] Khan, M. N. A., Chatwin, C. R., & Young, R. C. (2007). Extracting Evidence from Filesystem Activity using Bayesian Networks. International journal of Forensic computer science, 1, 50-63.
[25] Khan, M. N. A. (2012). Performance analysis of Bayesian networks and neural networks in classification of file system activities. Computers & Security, 31(4), 391-401.
[26] Rafique, M., & Khan, M. N. A. (2013). Exploring Static and Live Digital Forensics: Methods, Practices and Tools. International Journal of Scientific & Engineering Research 4(10): 1048-1056.
[27] Bashir, M. S., & Khan, M. N. A. (2013). Triage in Live Digital Forensic Analysis. International journal of Forensic Computer Science 1, 35-44.
[28] Sarwar, A., & Khan, M. N. (2013). A Review of Trust Aspects in Cloud Computing Security. International Journal of Cloud Computing and Services Science (IJCLOSER), 2(2), 116-122.
[29] Gondal, A. H., & Khan, M. N. A. (2013). A review of fully automated techniques for brain tumor detection from MR images. International Journal of Modern Education and Computer Science (IJMECS), 5(2), 55.
[30] Zia, A., & Khan, M. N. A. (2012). Identifying key challenges in performance issues in cloud computing. International Journal of Modern Education and Computer Science (IJMECS), 4(10), 59.
[31] Ur Rehman, K., & Khan, M. N. A. (2013). The Foremost Guidelines for Achieving Higher Ranking in Search Results through Search Engine Optimization. International Journal of Advanced Science and Technology, 52, 101-110.
[32] Khan, M., & Khan, M. N. A. (2013). Exploring query optimization techniques in relational databases. International Journal of Database Theory & Application,6(3).
[33] Shehzad, R., KHAN, M. N., & Naeem, M. (2013). Integrating knowledge management with business intelligence processes for enhanced organizational learning. International Journal of Software Engineering and Its Applications, 7(2), 83-91.
[34] Ul Haq, S., Raza, M., Zia, A., & Khan, M. N. A. (2011). Issues in global software development: A critical review. An Appraisal of Off-line Signature Verification Techniques 75 Copyright © 2015 MECS I.J. Modern Education and Computer Science, 2015, 4, 67-75 Journal of Software Engineering and Applications, 4(10), 590.
[35] Zia, A., & Khan, M. N. A. (2013). A Scheme to Reduce Response Time in Cloud Computing Environment. International Journal of Modern Education and Computer Science (IJMECS), 5(6), 56.
[36] Tariq, M. & Khan, M.N.A., (2011). The Context of Global Software Development: Challenges, Best Practices and Benefits. Information Management & Business Review, 3(4).
[37] Shahzad, A., Hussain, M., & Khan, M. N. A. (2013). Protecting from Zero-Day Malware Attacks. Middle-East Journal of Scientific Research, 17(4), 455-464.
[38] Khan, A. A., & Khan, M. (2011). Internet content regulation framework. International Journal of U-& EService, Science & Technology, 4(3).
[39] Kaleem Ullah, K. U., & MNA Khan, M. K. (2014). Security and Privacy Issues in Cloud Computing Environment: A Survey Paper. International Journal of Grid and Distributed Computing, 7(2), 89-98.
[40] Abbasi, A. A., Khan, M. N. A., & Khan, S. A. (2013). A Critical Survey of Iris Based Recognition Systems. Middle-East Journal of Scientific Research, 15(5), 663-668.
[41] Khan, M. N. A., Qureshi, S. A., & Riaz, N. (2013). Gender classification with decision trees. Int. J. Signal Process. Image Process. Patt. Recog, 6, 165-176.
[42] Ali, S. S., & Khan, M. N. A. (2013). ICT Infrastructure Framework for Microfinance Institutions and Banks in Pakistan: An Optimized Approach. International Journal of Online Marketing (IJOM), 3(2), 75-86.
[43] Mahmood, A., Ibrahim, M., & Khan, M. N. A. (2013). Service Composition in the Context of Service Oriented Architecture. Middle East Journal of Scientific Research, 15(11).
[44] Masood, M. A., & Khan, M. N. A. (2015). Clustering Techniques in Bioinformatics. I.J. Modern Education and Computer Science, 2015, 1, 38-46.

Authors' Profiles

Muhammad Yousaf Saeed obtained MS degree in Computer Science from SZABIST, Islamabad, Pakistan. He has over five years of experience in the IT Industry. His research interests are in the fields of cloud computing and Software Engineering.

M.N.A. Khan obtained D.Phil. degree in Computer System Engineering from the University of Sussex, Brighton, England. His research interests are in the fields of software engineering, cyber administration, digital forensic analysis and machine learning techniques.