Cloud Computing Environment and Security Challenges: A Review

Muhammad Faheem Mushtaq[1], Urooj Akram[1], Irfan Khan[2], Sundas Naqeeb Khan[1], Asim Shahzad[1], Arif Ullah[1]
[1]Faculty of Computer Science and Information Technology,
Universiti Tun Hussein Onn Malaysia (UTHM),
Johor, Malaysia
[2]Directorate of Information Technology (IT),
Govt. Sadiq College Women University,
Bahawalpur, Pakistan

***Abstract*—Cloud computing exhibits a remarkable potential to offer cost-effective and more flexible services on-demand to the customers over the network. It dynamically increases the capabilities of the organization without training new people, investment in new infrastructure or licensing new software. Cloud computing has grown dramatically in the last few years due to the scalability of resources and appear as a fast-growing segment of the IT industry. The dynamic and scalable nature of cloud computing creates security challenges in their management by examining policy failure or malicious activity. In this paper, we examine the detailed design of cloud computing architecture in which deployment models, service models, cloud components, and cloud security are explored. Furthermore, this study identifies the security challenges in cloud computing during the transfer of data into the cloud and provides a viable solution to address the potential threats. The task of Trusted Third Party (TTP) is introducing that ensure the sufficient security characteristics in the cloud computing. The security solution using the cryptography is specifically as the Public Key Infrastructure (PKI) that operates with Single-Sign-On (SSO) and Lightweight Directory Access Protocol (LDAP) which ensure the integrity, confidentiality, availability, and authenticity involved in communications and data.**

***Keywords*—Cloud computing; deployment models; service models; cloud security; trusted third party; cryptography**

I. INTRODUCTION

Cloud computing extends the information technology capabilities by increasing the capacity and adds abilities dynamically without investing on large and expensive infrastructure, licensing software, or training new personals. Among the several benefits, cloud computing provides a more flexible way to access the storage and computation resources on demand. In the last few years, different business companies are increasingly understanding that by tapping the cloud resources and gaining fast access, they are able to reduce their initial business cost by paying only the resources they used rather than the need of potentially large investment (owning and maintenance) on infrastructure. Rapid deployment, cost reduction, and minimal investment are the major factors to employ cloud services that drive many companies [1]-[3]. Cloud computing is explained by National Institute of Standard and Technology (NIST). It is a model to enable convenient, ubiquitous and on-demand network access that is the configurable computing resources to shared resources which can be delivered and provisioned rapidly with minimum managerial interaction [4].

The cloud is the collection of virtualized and inter-connected computers that consists of parallel and distributed systems which can be dynamically presented and provisioned the computing resources based on some Service Level Agreements (SLA) that is established by the settlement between the customers and service provider [5]. The advantages of using cloud computing are offering infinite computing resources, low cost, security controls, hypervisor protection, rapid elasticity, high scalability and fault tolerant services with high performance. Many companies like Microsoft, Google, Amazon, IBM, etc. developed the cloud computing systems and provide a large amount of customers by enhancing their services [6]. Moreover, there are significant barriers to adopting cloud computing like security issue regarding the privacy, compliance and legal matters because it is relatively new computing model having a great deal of the uncertainty regarding the security of all levels such as host, network, data levels, and application can be accomplished [7]. The management of data and services is an important concern when the databases and application software are moves the cloud to the large data centers. It may arise many security challenges regarding the use of cloud computing includes the privacy and control, virtualization and accessibility vulnerabilities, credential and identity management, confidentiality, authentication of the respondent device and integrity [8], [9]. The increment in the adoption of cloud computing and the market maturity is growing steadily because the service providers ensure the complex security level, compliance and regulatory. In part this growth, the cloud services will deliver the increased flexibility and cost savings [10].

Cloud computing is authorized through the virtualization technology in which the host system operates an application referred as a hypervisor that generates one or more Virtual Machines (VM) and it faithfully simulates the physical computers. These simulations can be able to operate any software from operating system to the end-user application [11]. The number of physical devices lies in hardware level that includes hard drives, processors and network devices which are placed in the data centers. It is independent of the

geographical location that is responsible for processing and storage as needed. The effective management of the servers is performed by the combination of the virtualization layer, software layer, and the management layer. Virtualization layer is utilized to provide the necessary cloud components of rapid elasticity, resource pooling, and location independent. Also, it is an essential element of cloud implementation. The ability to implement security rules and monitoring throughout the cloud is done by the management layer.

This research explains the overview of cloud computing architecture as: 1) cloud deployment models; 2) cloud service model; 3) cloud basic characteristics; 4) cloud security. Security concerns of different companies with the growing importance of cloud resources are taking into account when the data migrate to the modernize cloud systems, advances in business needs and the impact of services offered by the different organizations to increase the market. Moreover, this study focuses on to identifying the security issues and challenges in cloud computing that considers the threads, vulnerabilities, requirements, risks and discusses the security solutions and suggestion for the cloud computing. Also, discusses the Trusted Third Party (TTP) in the cloud computing environment by enabling the trust and cryptography that ensure the integrity, authenticity and confidentiality of data by addressing specific security vulnerabilities. The suggested solution to the horizontal level services which are available for the concerned entities that basically maintain trust to realize the security mesh. Public Key Infrastructure (PKI) operates with Single-Sign-On (SSO) and Lightweight Directory Access Protocol (LDAP) and is utilized to securely authenticate and identify the concerned entities.

The rest of the paper is organized as follows: Section 2 summarizes the detailed design of cloud computing architecture. Section 3 explains the security challenges of the Cloud computing. Section 4 describes the analysis and discussion based on the security challenges identified in the cloud computing environment. Section 5 presents the conclusions and future work of this research.

II. Cloud Computing Architecture

NIST is responsible for providing security in the cloud computing environment and developing standards and guidelines which shows a valuable contribution that offers a better understanding of cloud services and computing technologies [2], [12]. Cloud computing architecture summarize as the four deployment models: public cloud, private cloud, community cloud, and the hybrid cloud. The deployment models represent the way that the computing infrastructure delivers the cloud services can be employed. The three cloud service models or delivery models are available for the customer: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). There are different levels of security required for these service models in the cloud environment. The wide range of services considered in cloud basic characteristic layer that can be used all over the internet. The cloud service provider is corresponded to provide services, resource allocation management, and security. The architecture explains the five basic components which consist of services that are used in the cloud. The cloud security is the very important and complex task when the data transfer or shared resources to the cloud within the client-server architecture. The architecture of cloud computing is shown in Fig. 1 and details are discussed as follows:

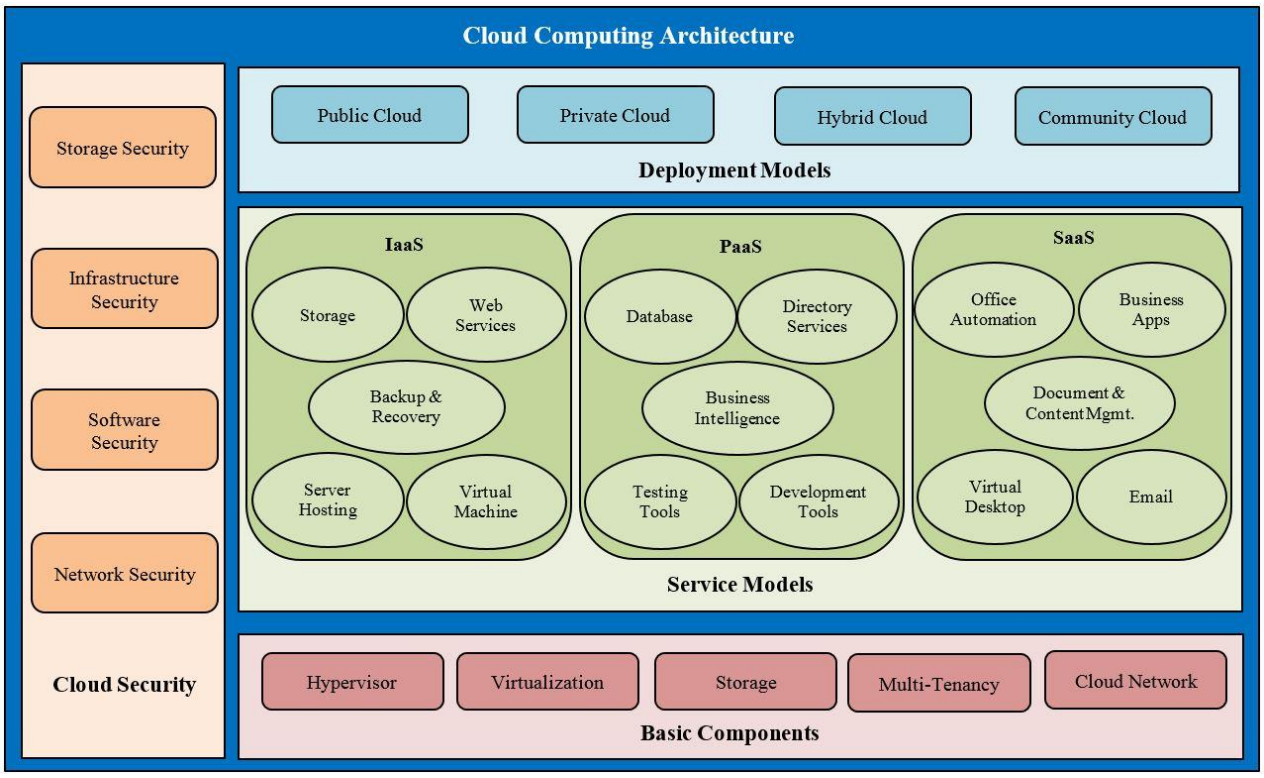

Fig. 1. Cloud computing architecture.

A. Cloud Deployment Models

The cloud computing model has three deployment models that can be particularly used to represent the cloud service models and it explains the nature and purpose of the cloud. The deployment models can be shown in Fig. 2 and classified as follows:

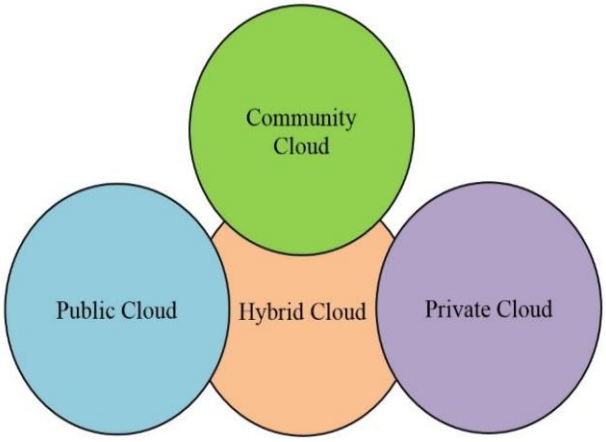

Fig. 2. Cloud deployment models.

1) Public Cloud: A public cloud represents the cloud hosting and owned by the service provider whereby the client and resource provider have service level agreement [4], [13]. Microsoft, Google, Amazon, VMware, IBM, Sun and Rackspace are some examples of cloud service provider. The plateform is designed in the form of generalized computing that holds the generic type of customer demand. The resources are made available to the public and easily accessible. Multiple entities are involved in operating public cloud and resource are public for the customers which makes them difficult to protect from malicious attacks. It contains some concerns over privacy, data access and security for customers because it is outside the firewall. It is less secure than the other deployment models and suited for a small and medium business that may not have to configure servers and purchase capital resources.

2) Private Cloud: The cloud infrastructure is managed and maintained by the single organization that compromises multiple customers. If any organization set up their own private cloud and recently create their own servers having physical hardware servers that put virtualization layer top on them then they would make resources available only internally. So, their application can deploy to their own physical control server, they don't need to go Microsoft or Amazon servers. They will set up their own infrastructure. It can ensure the physical security and more secure as compared to the public cloud because of its specific internal exposure. Private cloud is the only access to operate by the designated stakeholder and organization. However, the cost is significantly higher because expertise and training are needed for the server administrator, virtualization specialist, and network specialist. Virtual application and scalable resources provided by the cloud service provider are pooled together and it is available for customers to use and share. In private cloud, it is easier to address the relationship between the service provider and customer because the infrastructure operated and owned by the same organization [14]. It employs the capabilities of cloud management software to ensure reliable delivery service and integrity of the external resources.

3) Hybrid Cloud: Hybrid cloud is referred as the combination of two or more cloud deployment models that can be either public, private or community clouds which remains the unique entities but are bound together [15]. The importance of hybrid cloud usually offers extra resources when the high demand from the customer and for instance it is enabled to migrate some computation jobs from private to public cloud. It is well organized and allow different entities to access data over the internet because it offers more secure control of the applications and data. It provides a benefit over different deployment models and can be internally and externally hosted. Hybrid cloud gets more popularity and became a dominant model. The main reason is that it has the ability to take advantage of cost-saving, scalability in elasticity that public cloud may provide, allow control flexibility when it needed.

4) Community Cloud: Community cloud is referred as the organizations shared its cloud infrastructure among the customers having similar interest or concerns like a policy, the security requirements, mission and compliance consideration. We say that the several organizations or a third party are operated, controlled, shared and handled the resources of community cloud [16]. In case of the third party like Siemens have IT services and solutions that set up a media cloud for the media industry. It tends to be more rare and specialized. The cloud infrastructure of community cloud is shared and owned by different organizations such as research groups, together with work of companies and government organizations.

B. Cloud Service Models

Cloud computing architecture has a set of services which are used to access the configurable computing resources (applications, storage, servers, networks and services) on demand, dynamically scalable, virtualized and multi-tenant that offers a self-service over the internet. It provides the flexibility to handle the rapidly changing customer requirements and gives a reliable solution for customer demands. There are many service providers (Microsoft, Google, Amazon, Rackspace, etc.) that offer services to any of these models such as IaaS, PaaS and SaaS. The classification of cloud service models is important to figure out the particular service model that fulfills and accomplish its roles. The service model can be represented in Fig. 3 and the details are discussed as follows:

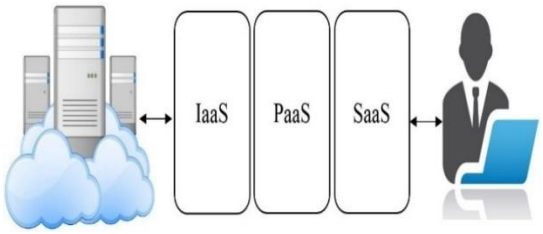

Fig. 3. Cloud service models.

1) Infrastructure as a Service (IaaS): IaaS offers the virtualized computing resources over the internet and deals with the hardware infrastructure such as servers, storage, processor, data center, network and various other infrastructure resources as a service where the user able to run and deploy arbitrary software. This infrastructure can significantly minimize initial cost of the companies to purchase computing hardware such as network devices, servers and processing power that allows the companies to major focus on core competencies instead of worrying regarding management and provisioning of infrastructure or own data centers [17]-[19]. The service providers for IaaS have hosted user applications and handle different jobs like resiliency planning and system maintenance backup. It has a major focus to improve the security in areas like VM monitor, intrusion detection, firewall and prevention (IPS/IDS). IasS model includes storage, web services, server hosting, VM, backup and recovery. The platform of IaaS provides the highly scalable resources which can be fixed on demand. It makes the plateform more suited for workloads having experimental, temporary or change unexpectedly. Furthermore, the characteristic includes the desktop virtualization, dynamic scaling, administrative tasks automation and policy-based services. The customer has control over deployed applications, storage, operating system and limited control are possible to select networking components like host firewall rather than the control or manage the cloud infrastructure. The well-known vendors for the IaaS are VMware, Hyper-V, Terremark, Amazon EC2, Dropbox, Sun Microsystems services and OpenStack to provide services to the customers and build their private or public cloud. Technically, the market of IaaS is relatively less movement of entry because it required a large investment to build the cloud infrastructure. The network services provided by public cloud in terms of Domain Name System (DNS) and load balancing. The DNS network service employs the domain name with IP addressing or hierarchical naming for the network identification and the load balancing offers a single access point to different servers that are working behind it. The load balancer used specific balancing techniques to distributes the network traffic between the multiple servers.

2) Platform as a service (PaaS): PaaS is the middleware of the service model and it provides the services in the form of programs, framework, integrated development environment, and development tools hosted on the server provider [20], [21]. It delivers a service to the developers that provides the software development lifecycle management (Planning, design, develop an application, deployment, testing and maintenance). The abilities offer to the customer or developers are deployed the developed applications onto the cloud infrastructure. The customer has only access to control the deployed applications and configurations of possible hosting environment instead of control the servers, storage, network and operating system. PaaS model worked similar to the IaaS but it offers the additional level of rented functionality and the customers using the services of PaaS model transfer more costs from hardware investment to the operational expense [22]. The vendor of PaaS offers some services for the application developers:

- The standards of the application based on developer's requirements.
- Logging, code instrumentation and reporting.
- Redundancy and security.
- A virtual development environment.
- The configuration of toolkits for the virtual development environment.
- Management interface and API.
- Multi-tenancy.
- Auto-provisioning and scalability of the underlying infrastructure.
- Built-in channel distribution for public application developer.

The well-known vendors for the PaaS model are: Microsoft Azure, Apprenda, Stackato, VMware, Google App Engine and NYSE Capital. PaaS model includes databases, directory services, business intelligence, testing and development tools. VM is employed in PaaS to act as a catalyst and it required to protect against the cloud malware attacks. It is important to include the valid authentication checks during the data transfer across the overall network channels and need to maintain the integrity of the applications. The security of PaaS can be compromised during the deployment of customer application or runtime of application and has challenges when underlying infrastructure security, lifecycle development and third-party relationship.

3) Software as a Service (SaaS): SaaS model is the collection of remotely hosted applications that are made available by the service provider for the customers on demand on the internet [4]. It has dominant cloud market as underlying technology that supports service oriented architecture and web services and still the market is growing rapidly. SaaS model offers the functionality of the business software to enterprise users at very low cost instead of providing facility to develop software or application. The vendors of SaaS models offer some core benefits are as follows:

- Easier administration.
- Universal accessibility.
- Easily collaboration.
- Software compatibility.
- Auto patch and updates management.

It allows the enterprises to get similar benefits of the internally operated commercially licensed software. However, still most of the enterprise users are not comfortable due to the deficiency in the visibility regarding their stored data in the cloud is secure or not [23]. Therefore, security concerns of enterprise addressing appear as the emerging challenge in the adoption of SaaS applications within the clouds. The security concerns about the application vulnerabilities, system availability and insider breaches that bring the loss of sensitive information or data. SaaS model includes virtual desktop, email, office automation, business apps, document and content management. The well-known vendors of SaaS service providers are the Salesforce and Google App that are the collection of remote computing services.

IaaS provides greater customer or tenant over the security than PaaS and SaaS. While the PaaS infrastructure provides better extensibility and customer control and the SaaS model is depending on integrated functionality with minimum customer control and extensibility. The security pressure of SaaS model varies on the cloud provider due to the degree of abstraction. Mostly large enterprise will like to create hybrid cloud environment with several private and public clouds having a possibility to mix community cloud into it. Some clouds will offer different enhancement in terms of security, performance, optimized pricing [24]. Furthermore, the optimized outcome is achieved by the enterprises through the deployment of an application with suitable cloud models. The well-known vendor used cloud service model with respective deployment models are shown in Table 1.

TABLE I. VENDER USED CLOUD DEPLOYMENT AND SERVICE MODELS

Service /Deployment Models	**Infrastructure as a Service (IaaS)**	**Platform as a Service (PaaS)**	**Software as a Service (SaaS)**
Public Cloud	Rackspace, Amazon EC2	VMware, Microsoft Azure, CloudFoundry.com, Google App Engine	Office 365, QuickBooks online, Salesforce.com
Private Cloud	OpenStack, Hyper-V, VMware, CloudStack	Stackato, Apprenda	Cisco WebEx
Hybrid Cloud	Rackspace, Custom	Cloud Foundry, Custom	Rackspace
Community Cloud	NYSE Capital	NYSE Capital	Salesforce

C. Cloud Basic Component

The cloud computing is deployed on the basic components and these components consist of wide range of services which can be used in the overall internet. In this study, some important components are considered as follows:

1) Hypervisor: The Hypervisor is referred to as Virtual Machine Monitor (VMM) or manager is computer hardware or firmware, software that allows to run and creates multiple virtual machines on single hardware host [25]. It is an important module of virtualization that monitors and manage the variety of Operating Systems (OS) which can share virtualized resources of hardware e.g. Windows, Linux and Mac OS that can run on the single physical system. The hypervisor can be classified into type 1 hypervisor and type 2 hypervisor. The type 1 hypervisor can directly operate in host system hardware such as Oracle VM server for x86, Microsoft Hyper-V and Xen. The type 2 hypervisor operates the guest operating from the host OS which offers virtualization service like memory management and I/O device support such as a Virtual box, VMware player, and VMware workstation. To determine the right selection of hypervisor that meets the need using the performance metrics such as guest memory, maximum host, a virtual processor supported and the CPU overhead. Moreover, to identify the hypervisor capabilities by verifying the guest OS on each hypervisor supports [25], [26].

2) Virtualization: Virtualization allows to share the physical instance resources by multiple customers or organizations. It helps to make one physical resource that is same as the multiple virtual resources [27]-[29]. Virtualization splits the services and resources from the underlying physical delivery environment. Virtualization is used to consolidate the resources (network resources, storage, processor and operating system) into a virtual environment that offers several benefits such as IT responsiveness and flexibility, reduce hardware cost by consolidation and workload optimization. However, it creates new challenges from attacker to secure the extra layer of VM due to more interconnection complexity and entry point increases using virtualization. It is important for the physical machine security because any problem may effect the other.

3) Storage: Customers use cloud storage over the network in which the data is backed up, managed and maintained remotely [9], [16]. The service provider major focus to improve the customer concerns regarding security capabilities such as authentication and encryption into their services. The vendors need to ensure that the data is secure, available and safe. Storage in cloud depends on the virtualized infrastructure with scalability, instant elasticity, metered resources, and accessible interfaces. The public cloud storage offers a multi-tenant environment of storage that is appropriate for the unstructured data. While the private cloud service offers dedicated storage environment that is protected behind customers or organization's firewall. The hybrid cloud service provides more data deployment options and business flexibility because it mix the private and public cloud services. The benefits of using cloud storage are information management, time deployment, and total cost of ownership.

4) Multi-tenancy: Multi-tenancy environment contain a single instance of application software that can serve the multiple users or customers. The customers can only share applications or resources rather than to observe or share each other data in the execution environment [30]. Each customer is

referred as the tenant and it may give the ability for customizing the application to some extent such as user interface color, but they are not authorized to customize the code of applications. SaaS service providers can run one part of the application with the corresponding database and offer web access or service to multiple tenants. The data of multiple tenants or customers is stored in the same database which effects the data leakage risk between this customer is high. The provider needs to ensure the security policies in which the data keep separate between the multiple tenants. The outcome of multi-tenancy is the optimal utilization of data storage and hardware mechanism. Multi-tenancy in cloud computing has broadened because it get advantages to romote access and virtualization for new service models.

5) Cloud Network: cloud networking is used to describe the access of network resources from the centralized service provider using the internet [31]. In this cloud, network and computing resources can be shared among the customers. The secure networking infrastructure is required for the efficiently manage and build the cloud storage. Cloud network needs an internet connection which is same with the virtual private network that allows the customer to securely access files, applications, printers, etc. The cloud network technology in the form of Software-Defined Networking (SDN) having a number of networking access devices and switches that can be deployed over the shared wide area.

D. Cloud Security

Cloud security is the set of control-based policies, compliance and technologies designed to deploy the protection of applications, data and infrastructure associated with the cloud. Cloud is used by more organizations and associated providers for operating data have become the priority to contract for proper security and potentially vulnerable areas. Cloud computing security is the major concerns when shared resources, access control, privacy and identity management needs [32]. Some of the concerns are discussed as follows:

- The data store in the cloud can be deliberately disclosed by the cloud providers, employees and its contractors.
- Cloud-based data may be incorrectly modified and vulnerable to delete (lost accidentally) by the service provider.
- In the public network, the data may be possibly accessible through the insecure APIs and protocols.
- The resources in the cloud are typically shared with different tenants that may be attacked.

Although, the security of data is in-fact challenging when data transfer to the cloud. This section briefly discusses the security concerns as follows:

1) Cloud Storage Security: The popularity and adoption of cloud storage is rising that produce many security challenges for the cloud providers as well as for the customers. IT experts to warn that every kind of technologies even virtual or physical, it contains inherent risks when using file-sharing applications and cloud storage. Customers store their data in the cloud have no longer owns the data because it will transfer through the third party that means the privacy setting of data is beyond the control of service provider or enterprises [33]. Customers need to ensure the quality of service and security of the data in the cloud. The security concerns about storage are data leakage, BYOD (Bring Your Own Data), snooping, cloud credentials and key management.

2) Cloud Infrastructure Security: Cloud computing enabling the distributed workforce and provides many benefits for the customers but it is essential to learn how to operate the cloud infrastructure that ensures and verify the secure deployment of services, storage of data, communication and safe operation through administration [21]. With the rapid adoption of cloud services, the concerns (privacy, security and reliability) have emerged as potential barriers. Information security professionals usually define the security guideline, rules and practice of cloud infrastructure of the organization at the application, host and network levels.

3) Software Security: The cloud provider required to protect their applications or software from internal and external thread throughout from design to production in their entire life cycle [34]. It is important to define the security process and policies about the software that enables the business instead of introducing other risk and it poses challenges for the customers and the cloud provider. Software security can be handled or defeat by implementing bugs, design flaws, buffer overflow, error handling agreements.

4) Cloud Network Security: A cloud service provider has the responsibility to allow the only valid network traffic and block all malicious traffic. Cloud providers are not shared the internal network infrastructure like the access routers and switches employ to connect cloud VMs to the provider network. The customer concerned on internal network attacks which include 1) leakage of confidential data; 2) unauthorized modification; and 3) denial of service or availability. Network security has concerns from both internal and external attacks because the attacker may legally authorize from another part of the network and attack can occur either physical or virtual network [34].

III. Security Challenges in Cloud Computing

The applications of cloud services are operating in the cloud computing infrastructures by using the internet or internal network. The concept of trust in the organization can be referred as the customers assure the capabilities of the organization that it provides the required services reliably and accurately. Trust in cloud computing environment based on the selected cloud deployment models in which the applications are delegated and outsourced to the control of the owner. Trust has required an efficient and effective security policy in the traditional architecture that addressed the functional constraints and flows between them [35], [36]. External systems access the constraints that attack the programs which effect the access or control on the customer data. In cloud deployment models, the community or public clouds assigned control to the organization that owned the cloud infrastructure. When the

public cloud-deployed, the control allows the owner of the infrastructure to strictly apply adequate security policy which ensures the appropriate security activities performed that reduces the threats and risks. Basically, the cloud security is associated to trust on computing and services employed by the infrastructure owner. The cloud infrastructure in private cloud is managed and operated within the premises of private organization in which no additional security challenges introduced, so the trust remained within the organization. It is believed that transfer of data or any association of organization or systems to the outside organization that opening a way to gain unauthorized access to the information resources [37].

Cloud computing allows the providers to run, deploy and develop applications that can be work rapidly (performance), scalability, maintainability and reliability without any concerns about the locations and properties of the underlying infrastructure. The consequences to avail these properties of the cloud when we store or transfer private data of different companies and get services from the cloud service providers by employing the internet that arises the privacy and security issues. For the purpose of securing cloud Information Systems (IS) which involve to identifying the challenges and threats that need to be addressed using the appropriate countermeasures implementation. Cloud computing infrastructure needs the assessment of risk in areas such as integrity, confidentiality, privacy, auditing, reliability and availability. Essentially, the security has major aspects of integrity, confidentiality and availability that are utilized in designing the adequate security system. These major security aspects are required to secure the data, hardware and software resources. Furthermore, discusses the Trusted Third Party (TTP) in the cloud computing environment through enabling trust and cryptography [38]. The cryptography is used to ensure the authenticity, confidentiality and integrity of data by trying to address the specific security vulnerabilities. Third parties or Cloud providers exhibit the trust of customers with specific quality, operational and ethical characteristics, and it comprises the minimal risk factor acknowledgment. TTP in the IS which is offering scalable end-to-end security services that depend on the standards and suitable in separate administrative domains, specialization sectors, and geographical areas. TTP in distributed cloud environment appears as the ideal security facilitator the customers or systems are belong to different domains without the knowledge or information of each other is needed to establish secure interactions. The security challenges of cloud computing infrastructure that can be considered in detail as follows:

A. Integrity

Data integrity in cloud computing is the preservation of data that is stored in cloud server to verify the data is not modified or lost by employing the services of the third party. Organizations can achieve more confidence to prevent system and data integrity from unauthorized access [39]. They provide such mechanisms having greater visibility to determine what or who may modify the system information or data that potentially affects their integrity. Authorization mechanism is utilized to determine the system what or which level of access to a specifically authorized customer should have to protected resources controlled through the system. Authorization is essential to ensure only the valid customers can access or interact with the data due to increasing the number of access points and customers in cloud computing environment.

The data integrity involves the three main entities: 1) a cloud storage provider to whom outsourced the data; 2) owner of data outsource his data; and 3) auditor who ensures the data integrity. The auditor may be the owner of data or he can assign responsibility to a third party [40]. The process of data integrity scheme defined as in two phases and is shown in Fig. 4. The preprocessing phase includes the preprocessed data and generated some additional metadata. After that outsources the data and metadata to the cloud storage provider. The verification phase includes the auditor send a challenge request to the cloud storage provider that generates possession proof with the data and metadata, and offers it to the auditor. The verification of proof done by the auditor that ensures the data integrity is intact.

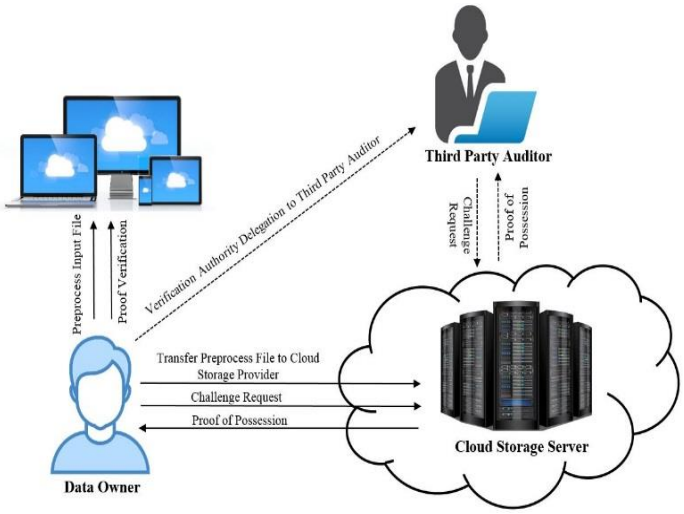

Fig. 4. Data integrity scheme.

The timely identification of any data deletion or corruption by using the data integrity scheme and takes necessary measures for the recovery of data. The data integrity scheme contains some design challenges in the cloud that are discussed as follows:

1) Computation eficiency: In data integrity scheme, the data can be preprocessed before outsource into the cloud storage server. The generation of metadata from original data similar to the cloud storage server. This processing creates overhead while performing may effect the computation efficiency. The preprocessing phase for small dataset does not matter the computation efficiency but it has a significant effect by using large datasets. In the server end, the computation cost of the proof of possession limits on how regularly the customer can verify or ensure the outsourced data integrity [41]. Data integrity scheme used primitives as metadata that also effects on the computation time.

2) Communication efficiency: The communication efficiency can be described three major aspects in the data integrity scheme: 1) data owner have challenge request for the proof of possession; 2) the challenge response from the cloud

storage server for the verification of possession; and 3) overhead occur during the initial transfer of data along the metadata. The communication overhead in dynamic data that comprises the updates verification. The metadata utilized the primitives have effects on the communication cost. Algebraic signatures offer the communication efficiency by using the low network bandwidth during response time and challenge request [41]. The size of response and challenge is usually small by using the Hill cipher and offering the efficient communication.

3) Reduced disk I/O: The overhead in metadata access and block access for the generation of proof on the cloud storage server have derived the efficiency of disk I/O in the data integrity scheme. For the purpose of generating proof to access all blocks that impact on the efficiency of the data integrity scheme and scheme become impractical for employing large datasets. The overall efficiency of disk I/O can influence on following parameters [42], [43].

- The size of the disk in data integrity scheme either employ variable length block size or fixed. The size of the block is small, then the larger the blocks in the file that will influence the preprocessing time in metadata tags generation for all blocks.
- Due to the variable length of data/metadata that cannot be accessed directly a particular block index. It will impact on the disk I/O to increases the process of verification, so the time increases of generating a proof.
- The parameter challenge in a number of blocks has an influence on both the I/O cost and computation cost. The large blocks in a challenge that leads in proof generating time increased.

4) Security: The concerns while designing the data integrity schemes because they are vulnerable to different attacks [44]-[46]. The possible attacks against the schemes are discussed as follows:

- The tag forgery attack is possible through malicious cloud storage provider that try to hide the data damage of customers and avoid the auditing challenge.
- In the data deletion attack, the cloud storage provider may proceed the challenge through generating a legal proof of possession with the tags in which the original data may have entirely deleted.
- In the replace attack, the cloud storage provider may replace the data blocks of deleted or corrupted pair and respectively tags using another valid pair as the response of challenge with that deceive the verifier.
- The pollution attack defines the correct data is employed by the dishonest server in the generation of response against a challenge but it offers corrupted or useless blocks in repair phase.
- In the data leak attack, the extraction of stored data by the attacker during the proofing protocol with wiretapping technique.

The data integrity schemes may find difficult or fail to identify the data corruption timely that consequences an unrecoverable damage. The cloud provider ensured to maintain data accuracy and integrity. The cloud computing models explain numerous threats containing the sophisticated insider attack on the data attributes. Software integrity protects the software from the unauthorized modification by intentionally or unintentionally. Cloud service providers implementing a set of APIs or software interfaces used to help the customers to interact and manage the cloud services. Moreover, the cloud services security based on the interface's security because the unauthorized customer may gain control of them and change or delete the customer data [47], [48]. Administrator or software's owner is responsible to protect the software integrity. Network and hardware integrity is required to address the cloud provider and protect the underlying hardware from fabrication, modification and theft. Cloud service models (IaaS, PaaS and SaaS) are the fundamental task to keep the data integrity and usually offer massive data procession ability. The challenges associated with the data storage in the cloud when the solid-state disks (tapes or hard disk drives) capacity are increased and unable to keep pace with the growth of data. So, the vendors need to scale up the storage by increasing the space of solid-space disk (hard drives or tapes) that may consequence the high possibility of either the data corruption, data loss, disk failure or the node failure. Furthermore, the capacity of the solid-state disk is increasing more and more, while it may not get much faster in terms of data access.

B. Confidentiality

Confidentiality refers to keeping the customer's data secret in the cloud computing system and only the authorized customers or systems can able to access the data [49]. Cloud computing provides (e.g. applications and its infrastructures) are basically in the public clouds have more threads on the systems or applications are exposed as compare the hosted in the private data centers. So, it is the fundamental requirement to keep the customer data secret ever the increasing number of applications, customers and devices involved. The vendors of cloud computing are extensively adopted the two basic approaches such as cryptography and physical isolation to achieve the confidentiality [50]. The cloud computing provides services and data that are transmitted through the public network and it cannot achieve physical isolation. While virtual LAN and middle boxes network such as packet filters and firewall should be deployed to accomplish virtual physical isolation. VPN cubed released by CohesiveFT to offers a security boundary for the IT infrastructure although it is inside the single, multiple or hybrid cloud data center ecosystems. Vertica offers VPN and firewall to secure its database and deploys on the Amazon EC2. When the Amazon EC2 has provisioned the Vertica database and offers customers to full root access that helps customers can secure the systems. They

create a VPN connection among the enterprise customers and Vertica to the cloud instance and firewall is set for the outside world. Confidentiality is also enhancing by encrypted the data before transfer into cloud storage and TC3 is successfully employed in this approach. Numerous concerns arises regarding the issues of application security and privacy, multi-tenancy, and data remanence [51].

1) Multi-Tenancy: Multi-tenancy refers to the characteristics of cloud resources that shared including the data, memory, networks and programs. Cloud computing is like the business model where the multiple customers can access same shared resources at the application level, host level, and network level. Multi-tenancy is similar to multi-tasking that shares some common processing resources like CPU and it present number of confidentiality and privacy threats.

2) Data Remanence: The data is represented in residual that can be unintentionally removed or erased due to the lack of hardware separation among different customers and virtual separation of the logical drives on a single cloud infrastructure, it may lead the unintentionally disclose the private data.

3) Application Security and Privacy: Data confidentiality is associated with the user authentication. To protect the customer's account from hackers is a large problem of controlling the access of the objects including software, devices and memory. The electronic authentication established the confidence of customer identities. If the customer used weak authentication to account can lead to an unauthorized access to the cloud. In the cloud computing environment, the customer needed to trust the applications offered by the organization that is handled and maintained the customer data in a secure manner. The possibilities of unauthorized access by the use of vulnerable applications or weak identification that create the issue of data privacy and confidentiality.

C. Availability

Availability in cloud computing including applications and its infrastructure is to ensure that the authorized customers can access the property of system at all time on demand. Cloud computing models (IaaS, PaaS and SaaS) allows its customers to access the services and applications from anyplace at any time. Vendors of cloud computing offers the cloud platform and infrastructure that is based on VM. The Amazon web services offer S3, EC2 that is based on VM called Skytap and Xen provides virtual lab management application depends on the hypervisor (Xen, VMware and Microsoft Hyper-V). For example, Xen virtual machine offered by Amazon is able to provide separated storage virtualization, memory virtualization, machine/CPU virtualization etc. where the large number of commodity PCs hosted. This is the reason the service providers can split resources (memory, capacity, storage, CPU cycle) on demand from Amazon based on usage expense in the form of each unit. Currently, the vendors of the cloud are offering platforms and infrastructures depend on the VM (Skytab, Amazon) provide the ability to filter and block the traffic based on port and IP address to secure systems but these services are not equal to the network security controls in mostly cloud enterprises.

Most cloud vendors (Google, Amazon) provide geographic redundancy in their cloud and hopefully allowing high availability on a single provider. The cloud system is capable to carry operations even in the security breaches possibilities or authorities misbehave [52]-[54]. Cloud service shows a heavy reliance on the network and infrastructure resources available at any time.

The information system design used to verify the identities of many systems that share mutual essential security requirements and determine the particular demands for information security and data protection. The multiple customer distributed environment suggests security challenges based on which level of user operates physical, virtual or application is shown in Table 2. The objectives of distributed system security are as follows:

- To ensure the data confidentiality among the participating systems.
- When add or remove resources on a physical level then maintain the exactly same security level.
- Make sure that there is no data leakage among different applications during the separation of processes and data in the cloud at the virtual level.
- To maintain or manage the integrity provided by the services such as correct operations and confidentiality.
- To provide the appropriate secure networks among the non- open systems world.
- To authenticate the different communicating customer's identities and if necessary the data delivery and origin for the purposes of banking to ensure the non-repudiation.
- To ensure the availability of data or systems communicated among the participating systems.
- The integrity of data or systems is maintained by preventing any modification or loss from unauthorized access between the participating systems communicated.

TABLE II. DISTRIBUTED SYSTEM SECURITY REQUIREMENT AND THREATS

Cloud Level	Physical Level	Virtual Level	Application Level
Cloud Services	Physical datacenter	IaaS, PaaS	SaaS
Users	Owner owns the cloud infrastructure that applies to the organization or customer	Developers deploy software on the infrastructure of the cloud that applies to the organization or customer	End user subscribes the services provides by cloud provider that applies to the organization or customer
Security Requirements	• Protection of network resources • Network protection • Legal use of cloud infrastructure • Security and reliability of hardware	• Virtual cloud Protection • Cloud control management security • Access control • Communication and application security • Security of data (transit/ rest/ remanence)	• Software security • Protection of data from exposure • Privacy in multi-tenant environment • Service availability • Communication protection • Access control
Security Threats	• Misuse of cloud infrastructure • Hardware modification or interruption or stealing • Network attacks • DDOS • Natural disasters • Connection flooding	• Network exposure • Session hijacking • Software interruption or modification • Connection flooding • Programming flaws • Impersonation • DDOS • Traffic flow analysis	• Privacy breach • Network exposure • Interception • Analysis of traffic flow • Data interruption • Session hijacking • Data modification at transit or rest • Impersonation

D. Trusted Third Party (TTP)

Trusted third party in cryptography helps to facilitate the interaction among the two parties and reviews all crucial operations among them. The cloud computing environment required the TTP services that exhibits to establish the essential trust level and offers an ideal solution to maintain the authenticity, integrity and confidentiality of communication and data. TTP can produce the trusted security domain with the specifically addresses the loss or missing of the traditional security boundary. It is an impartial organization which delivers the confidence of business by technical and commercial security features to electronic transactions [38]. TTP services are underwritten and offered along with the technical but also through the structural, financial and legal means. It is operationally linked with the chain of trust (certificate paths) for the purpose of providing a web trust that establishing the concept of Public Key Infrastructure (PKI). PKI offers legally acceptable and technically sound mean to implement data integrity, data confidentiality, authorization, strong authentication, and non-repudiation. In a distributed information system, PKI gets benefits from coupling through the directory that is a set of objects having same attributes that are organized in hierarchical and logical manner. Lightweight directory access protocol has become the vital protocol that supports to access PKI directory services for the Certificate Revocation List (CRL) and employed by web services for the authentication [55]. PKI is coupled with directory can be utilized to distribute: 1) certificate status information (CRL); 2) application certificate such as end-user certificate need to obtain using email before the transfer of encrypted message; and 3) private key, If the users do not use similar machine every day then the portability is needed in the environment. The directory contains the encrypted secret or private key are decrypted using the password given by customer at the remote workstation.

PKI are used with the Single-Sign-On (SSO) mechanism that can be ideal for cloud computing environment, where customers navigate among the abundance of the boundaries of cross-organization. In SSO environment, the user has not required to entering the password repeatedly to access multiple resources over the network. SSO is deployed with PKI that enhance the authentication and authorization process of the whole infrastructure between the evident technical issues due to it assured the sufficient level of the usability. The TTP can depend on following methods are defined as follows:

1) Client-Server Authentication: The certification authority needs to verify the entities or systems that are involved in interaction with the cloud computing environment which includes to certifying virtual servers, network devices, environment users, and physical infrastructure servers. The certification authority of PKI develops the required strong credentials for the virtual or physical entities that are involved in cloud and security domain are build with specific boundaries. The availability of strongest authentication process in distributed environments is the digital signature that is the combination of Ldap and SSO which ensure the user flexibility and mobility [56]. The authentication of customers is performed transparently and automatically to other devices or servers over the network by signing private key.

Cloud computing platform become enormous in which every service need secure authorization and authentication process. Among the conceptual boundaries of organization outsourced or own services become fuzzy, the adoption of required SSO solution is critical. Sibboleth is the middleware open source software that offers SSO within or across the organizational boundaries and trust on third party or cloud provider to share the information like user and named attributes [56]. Authorization process can be achieved after the successful authentication in which customer exchange his attribute without worried about the disclosure of personal information in the resource server.

2) Low or high-level confidentiality: Transmission of data across the network is a challenge due to its continuously rising

the threats of data interruption or modification. Due to the deficiency in traditional physical connection, the complexity increases in cloud computing environment that it required not only protection toward cloud traffic but additionally among the cloud hosts. PKI allows by implementing SSL or IPSec protocol for the secure communications. IPSec enables to send or receive the protected packets such as UDP, TCP, ICMP, etc. without any modification and offers authenticity and confidentiality based on the requirement [38], [57]. IPSec customer can authenticate themselves with the PKI certificate to enchance scalability due to the earlier transmitted of trusted CA certificate. SSL protocol enables the interface among applications with end-to-end encryption and TCP/IP protocols offer encrypted communication channel and authentication between the client-server. Communication is needed to protect hosts, customers and host-to-host due to the unique characteristics of cloud computing. In this regard, SSL and IPSec are chosen based on the security requirement and diverse needs.

3) Cryptographic data separation: The protection of sensitive data is essential in the cloud computing environment that established as a crucial factor in the successful SaaS model deployment. Cryptographic separating of the data, computations and processes are hidden or secret using the encryption technique that appears intangible for outsiders and maintains the confidentiality, integrity and privacy of data. Symmetric and asymmetric cryptographic techniques are combined (referred as hybrid cryptography) that can provide the efficiency and security of data [58], [59].

IV. Analysis and Discussion

In this section, discusses the suggested security solution of the challenges faced in the adoption of cloud computing environment that influence the customers to release security burden with trusting a third party. This study observed that the concerns of trust, security and privacy highlighted by many cloud providers and customers. The deployment of security strategies in the cloud environment to achieve integrity, confidentiality and availability of data or systems that adopts to change the relationship between the cloud provider and the customers. A trust-worthy access control infrastructure is needed to avoid any unauthorized access to the shared resources. Trust required operating in each layer of the cloud service models (IaaS, SaaS, PaaS) and it needs to ensure the security at the technical, legal, procedural and operational level to allow secure communication. Trust certificate establishes an entities credentials, identity and responsibilities and serves as the electronic authentication. The required trust is provided by TTP to ensure the identity of communicating parties or entities and examined to adhere the strict policies and requirements. The end user is needed to utilize electronic certificate for authentication with the cloud service and validating the access rights to avail the particular resources. The secure SSL connection is created by the combination of the personal digital certificate with the service provider certificate (IaaS or PaaS), so the cloud infrastructure guarantees or ensures the security of encrypting exchange data.

A number of services are hosted by the cloud infrastructure, so the several applications are transferred to the virtual server and each required their own certificate for the SSL communication. The application provider needs his own certificate for the encryption and decryption of application data and authentication for secure communications in the cloud. A digital certificate is used by the owner of hardware infrastructure to communicate security among the virtual servers and devices. Key management is the challenging issue in cloud infrastructure as the virtualization services are concealing the representation of the location of physical key storage and disable the traditional protection mechanism. In this case, the key protection by deploying the temper proof devices such as customer smart card that is coupled with hardware security module as a component of virtual deployment. The solution for this problem is addressed with cryptography by PKI that provides and ensures the integrity, confidentiality and authentication of the communication and data involved. In the cloud environment, TTP ensures the specific security characteristics. While it realizes a trust mesh among the entities involved forming cloud federations. The solution of the problem to the horizontal level services which are available for the concerned entities that basically maintain trust to realize the security mesh. This approach utilized the SSO technology, LDAP directories, and PKI cryptography to securely authenticate and identify the concerned entities. The TTP is based on the following methods: 1) client-server authentication; 2) low or high-level confidentiality; and 3) cryptography separation of data.

The ability of PKI is to effectively address the problems of security issues in key management. System and network performance is the important factor in the centralized system. Availability in cloud infrastructure will increase the network demand and quality of service offers the key issues during host-to-host communication, it required additional encryption process to handle the deficiency. The flexibility of using cloud infrastructure in the context of demand on CPU controls the systems from overhead and accelerates encryption and decryption technique.

V. Conclusion and Future Work

Cloud computing is the emerging technology that brings many benefits for its customers, organizations and companies. However, despite bringing several advantages, it raises many security challenges in the adoption of cloud. We explained the detail design of cloud computing architecture in which deployment models, service models, cloud components, and cloud security are explored. This research attempted to present many security challenges, threats, attacks and vulnerabilities in the systems or data during transfer to the cloud. The countermeasure of the security threats will assist the organizations to continue the cost-benefit analysis and to encourage them to transfer into the cloud. In this paper, we discussed the generic design principles of cloud computing environment that stem from the necessary control the relevant threads and vulnerabilities. Cloud computing security requires a fundamental point of view from where it is based on mitigating protection and trust to the TTP. Most of the identified threats can be address by the combination of SSO, LDAP and PKI in cloud computing that is dealing with the

authenticity, availability, integrity and confidentiality in communication or data. This research can be further analyzed in future to improve the quality and availability of services that brings the attraction of the customers toward the deployment of cloud computing and develop more customer's trust to the TTP. Also, developing a framework of complete security and privacy trust evaluation management system is a part of cloud computing services which satisfies the security demands.

REFERENCES

[1] M. Armbrust, I. Stoica, M. Zaharia, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, and A. Rabkin, "A review of cloud computing," Commun. ACM, vol. 53, no. 4, 2010.

[2] V. Chang, "A proposed framework for cloud computing adoption," Int. J. Organ. Collect. Intell., vol. 6, no. 3, pp. 1–17, 2016.

[3] R. B. Bohn, J. Messina, F. Liu, J. Tong, and J. Mao, "NIST cloud computing reference architecture," Proc. IEEE World Congr. Serv., pp. 594–596, 2011.

[4] P. Mell and T. Grance, "The NIST definition of cloud computing," NIST Spec. Publ. 800-145, vol. 145, p. 7, 2011.

[5] R. Buyya, C. S. Yeo, and S. Venugopal, "Market-oriented cloud computing: Vision, hype, and reality for delivering IT services as computing utilities," Proc. 10th IEEE Int. Conf. High Perform. Comput. Commun., pp. 5–13, 2008.

[6] M. Zhou, R. Zhang, W. Xie, W. Qian, and A. Zhou, "Security and privacy in cloud computing: A survey," Proc. 6th Int. Conf. Semant. Knowl. Grid, pp. 105–112, 2010.

[7] D. G. Rosado, R. Gomez, D. Mellado, and E. Fernández-Medina, "Security analysis in the migration to cloud environments," Futur. Internet, vol. 4, pp. 469–487, 2012.

[8] C. Wang, Q. Wang, K. Ren, and W. J. Lou, "Ensuring data storage security in cloud computing," 17th Int. Work. Qual. Serv., pp. 37–45, 2009.

[9] L. Wei, H. Zhu, Z. Cao, X. Dong, W. Jia, Y. Chen, and A. V. Vasilakos, "Security and privacy for storage and computation in cloud computing," Inf. Sci., vol. 258, pp. 371–386, 2014.

[10] P. Wilson, "Positive perspectives on cloud security," Inf. Secur. Tech. Rep., vol. 16, no. 3–4, pp. 97–101, 2011.

[11] L. Savu, "Cloud computing deployment models, delivery models, risks and research challanges," Proceeding IEEE Int. conf. comput. manag., 2011.

[12] F. Liu, J. Tong, J. Mao, R. Bohn, J. Messina, L. Badger, and D. Leaf, "NIST cloud computing reference architecture," NIST Spec. Publ. 500-292, pp. 1–28, 2011.

[13] C. Modi, D. Patel, B. Borisaniya, A. Patel, and M. Rajarajan, "A survey on security issues and solutions at different layers of Cloud computing," J. Supercomput., vol. 63, no. 2, pp. 561–592, 2013.

[14] A. paltform computing white Paper, Enterprise Cloud Computing: Transforming IT. 2009.

[15] S. Kaisler, W. H. Money, and S. J. Cohen, "A decision framework for cloud computing," Proceeding IEEE 45th Hawaii Int. Conf. Syst. Sci. A, pp. 1553–1562, 2012.

[16] M. Ali, S. U. Khan, and A. V. Vasilakos, "Security in cloud computing: opportunities and challenges," Inf. Sci. (Ny)., vol. 305, pp. 357–383, 2015.

[17] J. Brodkin, "Seven cloud-computing security risks.," InfoWorld from IDG, 2008.

[18] A. Macdermott, Q. Shi, M. Merabti, and K. Kifayat, "Detecting intrusions in the cloud environment detecting intrusions in the cloud environment," Proc. 14th Annu. Post- Grad. Symp. Converg. Telecommun. Netw. Broadcast., 2013.

[19] F. Lombardi and R. Di Pietro, "Secure virtualization for cloud computing," J. Netw. Comput. Appl., vol. 34, pp. 1113–1122, 2011.

[20] S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing," J. Netw. Comput. Appl., vol. 34, no. 1, pp. 1–11, 2011.

[21] D. Sun, G. Chang, L. Sun, and X. Wang, "Surveying and analyzing security, privacy and trust issues in cloud computing environments," Procedia Eng., vol. 15, pp. 2852–2856, 2011.

[22] Q. Zhang, L. Cheng, and R. Boutaba, "Cloud computing: state-of-the-art and research challenges," J. Internet Serv. Appl., vol. 1, no. 1, pp. 7–18, 2010.

[23] H. Fan, F. Khadeer, M. Younas, and O. Khadeer, "An integrated personalization framework for SaaS-based cloud services," Futur. Gener. Comput. Syst., vol. 53, pp. 157–173, 2015.

[24] L. F. B. Soares, D. A. B. Fernandes, J. V. Gomes, M. M. Freire, and P. R. M. Inacio, "Cloud security: state of the art," Secur., Priv. Trust Cloud Syst., pp. 3–44, 2013.

[25] K. Hashizume, D. Rosado, E. Fernández-Medina, and E. Fernandez, "An analysis of security issues for cloud computing," J. Internet Serv. Appl., vol. 4, no. 5, pp. 1–13, 2013.

[26] K. Hashizume, N. Yoshioka, and E. B. Fernandez, "Three misuse patterns for cloud computing," Secur. Eng. Cloud Comput. Approaches Tools, pp. 36–53, 2013.

[27] T. Garfinkel and M. Rosenblum, "When virtual is harder than real: security challenges in virtual machine based computing environments," Proc. 10th Conf. Hot Top. Oper. Syst., pp. 20–25, 2005.

[28] D. Owens, "Securing elasticity in the cloud," Commun. ACM, vol. 53, no. 6, p. 46, 2010.

[29] M. Al Morsy, J. Grundy, and I. Müller, "An analysis of the cloud computing security problem," Proc. APSEC Cloud Work. Sydney, Aust., pp. 1–6, 2010.

[30] A. Jasti, P. Shah, R. Nagaraj, and R. Pendse, "Security in multi-tenancy cloud," Proc. Int. Carnahan Conf. Secur. Technol., pp. 35–41, 2010.

[31] H. Aljahdali, A. Albatli, P. Garraghan, P. Townend, L. Lau, and J. Xu, "Multi-Tenancy in cloud computing," IEEE 8th Int. Symp. Serv. Oriented Syst. Eng., pp. 344–351, 2014.

[32] Z. Gou, S. Yamaguchi, and B. B. Gupta., "Analysis of various security issues and challenges in cloud computing environment: A survey," Handb. Res. Mod. Cryptogr. Solut. Comput. Cyber Secur. IGI Glob., pp. 393–419, 2016.

[33] T. C. Nguyen, W. Shen, Z. Luo, Z. Lei, and W. Xu, "Novel data integrity verification schemes in cloud storage," Comput. Inf. Sci., pp. 115–125, 2014.

[34] C. Eric, D. Chris, E. Mike, and G. Jonathan, "Security for cloud computing 10 Steps to ensure success," Cloud Stand. Cust. Counc., pp. 1–35, 2015.

[35] S. Paquette, P. T. Jaeger, and S. C. Wilson, "Identifying the security risks associated with governmental use of cloud computing," Gov. Inf. Q., vol. 27, no. 3, pp. 245–253, 2010.

[36] K. Karaoglanoglou and H. Karatza, "Resource discovery in a Grid system: Directing requests to trustworthy virtual organizations based on global trust values," J. Syst. Softw., vol. 84, no. 3, pp. 465–478, 2011.

[37] N. Iltaf, M. Hussain, and F. Kamran, "A mathematical approach towards trust based security in pervasive computing environment," Proceeding Int. Conf. Inf. Secur. Assur., pp. 702–711, 2009.

[38] S. Rizvi, K. Cover, and C. Gates, "A trusted third-party (TTP) based encryption scheme for ensuring data confidentiality in cloud environment," Procedia Comput. Sci., vol. 36, pp. 381–386, 2014.

[39] S. Aldossary and W. Allen, "Data security, privacy, availability and integrity in cloud computing: issues and current solutions," Int. J. Adv. Comput. Sci. Appl., vol. 7, no. 4, pp. 485–498, 2016.

[40] F. Zafar, A. Khan, S. U. R. Malik, M. Ahmed, A. Anjum, M. I. Khan, N. Javed, M. Alam, and F. Jamil, "A survey of cloud computing data integrity schemes: Design challenges, taxonomy and future trends," *Comput. Secur.*, vol. 65, pp. 29–49, 2017.

[41] L. Chen, "Using algebraic signatures to check data possession in cloud storage," *Futur. Gener. Comput. Syst.*, vol. 29, no. 7, pp. 1709–1715, 2013.

[42] E. Esiner, A. Kachkeev, S. Braunfeld, A. Kupcu, and O. Ozkasap, "FlexDPDP: Flexlist-based optimized dynamic provable data possession," *Cryptol. ePrint Arch. Rep. 2013/645*, pp. 1–40, 2013.

[43] G. Ateniese, R. Burns, and J. Herring, "Provable data possession at

untrusted stores," *Proc. 14th ACM Conf. Comput. Commun. Secur.*, pp. 598–610, 2007.

[44] Y. Yu, J. Ni, M. H. Au, H. Liu, H. Wang, and C. Xu, "Improved security of a dynamic remote data possession checking protocol for cloud storage," *Expert Syst. Appl.*, vol. 41, no. 17, pp. 7789–7796, 2014.

[45] K. Yang and X. Jia, "Data storage auditing service in cloud computing: Challenges, methods and opportunities," *World Wide Web*, vol. 15, no. 4, pp. 409–428, 2012.

[46] Y. Zhu, H. Hu, G.-J. Ahn, Y. Han, and S. Chen, "Collaborative integrity verification in hybrid clouds," *Proc. 7th Int. Conf. Collab. Comput. Networking, Appl. Work.*, pp. 191–200, 2011.

[47] S. K. P and R. Subramanian, "An efficient and secure protocol for ensuring data storage security in cloud computing," J. Comput. Sci., vol. 8, no. 6, pp. 261–275, 2011.

[48] Q. Wang, C. Wang, K. Ren, W. Lou, and J. Li, "Enabling public auditability and data dynamics for storage security in cloud computing," Parallel Distrib. Syst., vol. 22, no. 5, pp. 847–859, 2011.

[49] M. Armbrust, A. Fox, R. Griffith, A. Joseph, and RH, "Above the clouds: A berkeley view of cloud computing," Univ. California, Berkeley, Tech. Rep. UCB, pp. 7–13, 2009.

[50] M. F. Mushtaq, S. Jamel, and M. M. Deris, "Triangular coordinate extraction (TCE) for hybrid cubes," J. Eng. Appl. Sci., vol. 12, no. 8, pp. 2164–2169, 2017.

[51] Cloud Security Alliance, "Top threats to cloud computing," Cloud Secur. Alliance, pp. 1–14, 2010.

[52] F. S. Al-Anzi, A. A. Salman, N. K. Jacob, and J. Soni, "Towards robust, scalable and secure network storage in cloud computing," Proceeding 4th Int. Conf. Digit. Inf. Commun. Technol. Its Appl., pp. 51–55, 2014.

[53] K. D. Bowers, A. Juels, and A. Oprea, "HAIL: A high-availability and integrity layer for cloud storage," Proc. 16th ACM Conf. Comput. Commun. Secur. - CCS '09, vol. 489, p. 187, 2009.

[54] A. Bessani, M. Correia, B. Quaresma, F. André, and P. Sousa, "DEPSKY: Dependable and secure storage in a cloud-of-clouds," ACM Trans. Storage, vol. 9, no. 4, pp. 1–36, 2013.

[55] S. Boeyen and T. Moses, "Trust management in the public-key infrastructure," Entrust seucring Digit. identities Inf., no. January, pp. 1–36, 2003.

[56] A. Levi and M. U. Caglayan, "The problem of trusted third party in authentication and digital signature protocols," Proc. 12th Int'l Symp. Comput. Inf. Sci., 1997.

[57] M. S. E. H. Tebaa, "Secure Cloud Computing Through Homomorphic Encryption," Int. J. Adv. Comput. Technol., vol. 5, no. 16, pp. 29–38, 2013.

[58] M. F. Mushtaq, S. Jamel, K. M. Mohamad, S. Kamal, and A. Khalid, "Key generation technique based on triangular coordinate extraction for hybrid cubes," *J. Telecommun. Electron. Comput. Eng.*, 2017.

[59] A. Bhardwaj, G. V. B. Subrahmanyam, V. Avasthi, and H. Sastry, "Security algorithms for cloud computing," Procedia Comput. Sci., vol. 85, pp. 535–542, 2016.