Computers and Electrical Engineering 71 (2018) 28–42

Contents lists available at ScienceDirect

Computers and Electrical Engineering

journal homepage: www.elsevier.com/locate/compeleceng

Recent security challenges in cloud computing☆

Nalini Subramanian Research Scholar*, Andrews Jeyaraj

School of Computing, Sathyabama Institute of Science and Technology, Chennai, India

ARTICLE INFO

Keyword:
Security challenges
Cloud computing
Crypto-cloud
Issues in cloud
Virtualization

ABSTRACT

Cloud computing is an archetype that enables access to a shared pool of computing resources for cloud users in an on-demand or pay-per-use, fashion. Cloud computing offers several benefits to users and organizations, in terms of capital expenditure and savings in operational expenditure. Despite the existence of such benefits, there are some obstacles that place restrictions on the usage of cloud computing. Security is a major issue that is always considered. The lack of this vital feature results in the negative impact of the computing archetype thus resulting in personal, ethical, and financial harm. This paper will focus and explore the security challenges that are faced by cloud entities. These entities include Cloud Service Provider, the Data Owner and Cloud User. Focusing on the crypto-cloud that constitutes of different Communication, Computation, and Service Level Agreement. Studying the causes and effects of various cyber attacks it will provide the necessary upgrades.

1. Introduction

Cloud computing creates a network-based environment vision to the users, which paves way for the sharing of calculations and resources regardless of location. The National Institute of Standards and Technology's (NIST) defines cloud computing [1] as, “A template for providing the suitable and when needed access to the internet, to a collective pool of programmable grids, storage, servers, software, and amenities that can be rapidly emancipated, with little communication and supervision from the provider”. The characteristics of the type of processing are exhibited in Fig. 1 as On-demand self-service, High-performance network access, Rapid Elasticity, Resource Pooling and Measured Service. It also depicts four deployment models namely Hybrid, Community, Private and Public clouds. This is then coupled with the three service models, which are, PAAS (Platform as a Service), IAAS (Infrastructure as a Service), and SAAS (Software as a Service). NIST's cloud computing definition provides the needed framework and common characteristics depicted such as Virtualization, Homogeneity, Geographic Distribution and Service Orientation among others.

With all the layers of the cloud service models depicted in Fig. 2, security issues need to be addressed. When the layers are to be compared the high dependence of the browser position's it at the top whereas, the bottom layers are more web services oriented. Overall, a decrease in investment and operational expenses is achieved this is also followed by an increase in efficiency and scalability through the layers

The service model deployed can be private, public, hybrid or community cloud as per the user requirements.

Organization: The next two sections that follow indicate the security challenges. Sections 4–7 address the security challenges in communication, computational, data level and Service Level Agreement (SLA) level. Finally, Section 8, provides the conclusion with a comparison of the author's survey with other pre-existing reviews

☆ Reviews processed and recommended for publication to the Editor-in-Chief by Associate Editor Dr. Hong Shen.

* Correspoding author.
E-mail addresses: mrgn.nalini@gmail.com (N. Subramanian), andrewspose@gmail.com (A. Jeyaraj).

https://doi.org/10.1016/j.compeleceng.2018.06.006
Received 8 July 2017; Received in revised form 13 June 2018; Accepted 29 June 2018

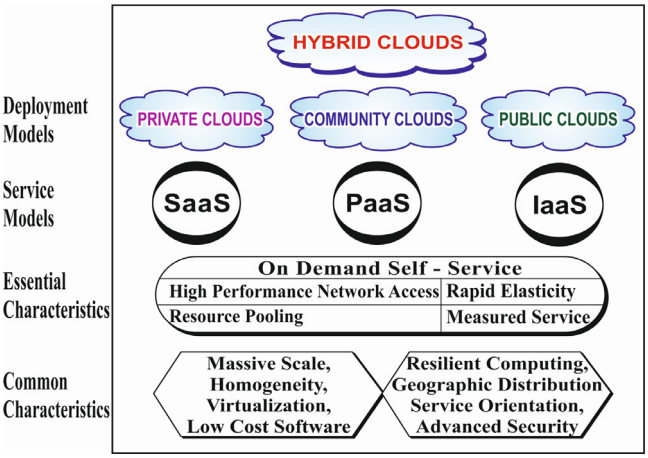

Fig. 1. NIST cloud definition framework.

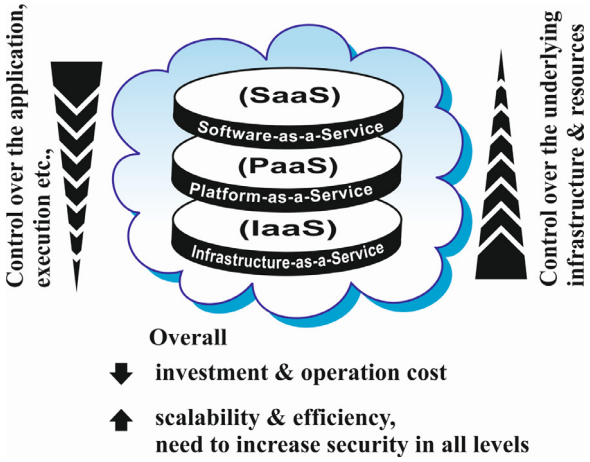

Fig. 2. Layers of cloud computing.

2. Security challenges

In cloud computing, the users are unaware of the exact location of their sensitive data, because the Cloud Service Providers(CSP's) maintain data centers in geographically distributed locations resulting in several security challenges and threats. The traditional security techniques such as firewalls, host-based antivirus software and intrusion detection systems do not offer adequate security in virtualized systems due to the rapid spread of the threats via virtualized environments.

2.1. Cloud computing threats and risks

On the other hand, Walker [2] identified that Cloud Security Alliance (CSA) has released the top 12 threats related to the cloud. These twelve threats are listed in Table 1. Among all these threats, data breaching is identified as the topmost security issue that needs addressing.

2.2. Security in crypto-cloud

Kamara [3], outlined the benefits of using a public cloud infrastructure. They also pointed out that the use of public clouds leads to several security risks. Confidentiality and integrity of the data are among the biggest risks causing grave concerns.

Fig. 3 clearly depicts the architecture of a crypto-cloud proposed by Kamara [3] in 2010. It consists of three basic entities, namely the Data Authority (the owner of the data), the consumer of the data, and the Cloud Storage Service Provider (CSSP). Data authority uploads the encrypted files, and the consumer or user of the cloud has authenticated access to the files. After these conditions are fulfilled then the requested file can be downloaded and decrypted using appropriate tokens and credentials. These entities face different security challenges in levels of communication, computation and Service Level Agreements (SLA's).

Table 1
CSA'S Top 12 threats.

Threat no.	Threat name
1	Data breaches
2	Compromised credentials and broken authentication
3	Hacked interface and Application Program Interfaces
4	Exploited system vulnerabilities
5	Account hijacking
6	Malicious insiders
7	The Advanced Persistent Threat(APT) parasite
8	Permanent data loss
9	Inadequate diligence
10	Cloud service abuses
11	Denial-of-Service(DoS) attacks
12	Shared technology, shared dangers

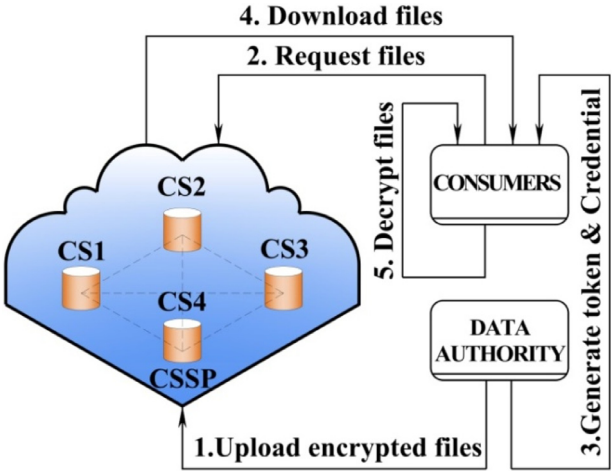

Fig. 3. Architecture of crypto-cloud.

3. Security challenges faced by the entities in cloud

Besides legal security requirements, it is necessary to address some basic security requirements like authentication, integrity, transparency, confidentiality, availability and audits as stated in Rebollo [4]. The security tree in Fig. 4 illustrates the importance of basic security requirements. The challenges specified at the root have to be addressed properly, just as the root secure the tree in the soil. When these basic requirements are met appropriately, the security tree ensures yields of benefits in terms of anything/everything as a Service (XaaS), metaphorically depicted as the fruits/leaves in a tree. The Protocols (TLS) and (SSL) which are Transport Layer Security and Secure Socket Layer respectively, are used for the secure transmission of data depicted with the trunk of the tree.

The security challenges specified in the security tree are classified on the basis of three basic entities as depicted in Fig. 3. The three levels namely are communication, computation and service level agreement as previously stated. The classification chart in Fig. 5 also outlines the three level of challenges to security. Security issues in each level are also clearly depicted with further classification. The security issues related to computational level address the data security and virtualization security.

The following Sections 4–7 deal with the security issues in the levels of communication, computation and SLA respectively.

4. Communication level

Communication level issues arise as a result of the sharing of common resources, infrastructure, etc., among the Virtual Machines (VM's) becoming the target of attack. Bhadauria [5] has classified this into network level, host level and application level. Attacks are identified on the basis of these three levels in communication.

4.1. Security in network level

The key features that should be addressed at the network level are confidentiality and integrity of data. The issues with respect to network level security are

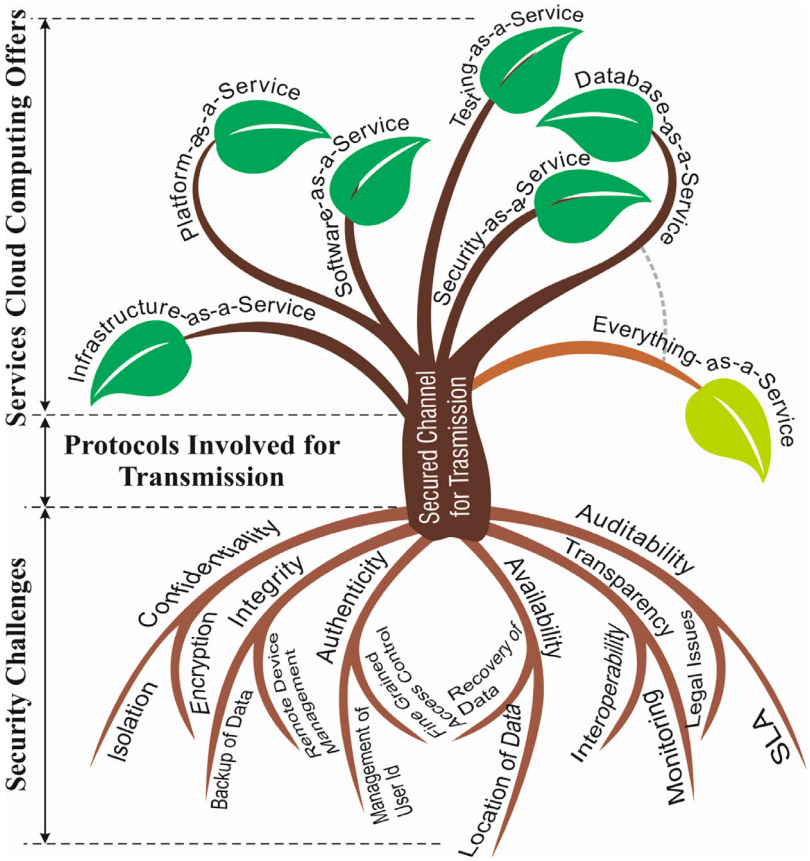

Fig. 4. Security tree.

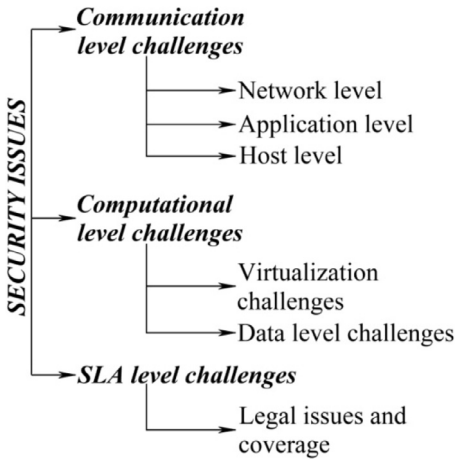

Fig. 5. Security issues classification.

- Domain Name Server Attacks;
- Prefix Hijacking in Border Gateway Protocol;
- Issue of Reused IP Addressing;
- Sniffer Attacks etc.

4.2. Security in application level

Applications need security to avoid providing opportunities for attackers to gain control over them with their attempt to change

their formats. The issues to be addressed at this level are:

- Cookie Poisoning;
- DDoS;
- Hidden Field Manipulation;
- Dictionary Attack;
- Google Hacking;
- CAPTCHA Breaking etc.

4.3. Security at host level

Host threats are addressed at the operating system level upon which applications work. The major host level threats are:

- Viruses, Trojan horses, and worms;
- Profiling;
- Password cracking;
- Footprinting;
- Denial of service;
- Unauthorized access.

5. Computational level

Implementation of the concept of virtualization in the cloud is one of the biggest computational level challenges.

5.1. Virtualization challenges

Abstraction of the physical resources is Virtualization. Some of the common classes of virtualization are *application virtualization, desktop virtualization, Network virtualization, Server and Machine virtualization.* Laniepce [6], 2013, classified the layers of virtualization as in Fig. 6.

The virtual layer consists of multiple instances of the Virtual Machines. It provides a picture of virtual and distributed environment running under the control of cloud provider on the top of the cloud infrastructure. The virtualization layer, enables deployment and running of different VMs simultaneously on a same physical host. It is performed by a specific component/ software called the hypervisor / Virtual Machine Monitor (VMM), which allocates resources among VM instances and maintains isolation between them. The virtual network permits communication of VMs through the virtual switch. The physical layer comprises hardware resources like memory, Central Processing Unit (CPU) and storage.

5.1.1. VM level (Virtual layer) security challenges

The VMs undergo their own life cycles through different states like creation, pending, prolong, running, suspended, resumed, power-off, shutdown, destroyed, etc.,

Fig. 7. Clearly categorizes the VM level security challenges cloud system.

1. ***VM cloning:*** Creation of a copy of an existing VM with the same identifier (ID), computer name, Internet Protocol (IP) address and Media Access Control (MAC) address is called VM cloning. The original VM called the parent shares the virtual resources with the cloned VM. Any changes made to the parent after cloning does not affect the cloned VM and vice-versa. If both the VM's run on the same network, security issues arises as the result of the duplication of IP address.

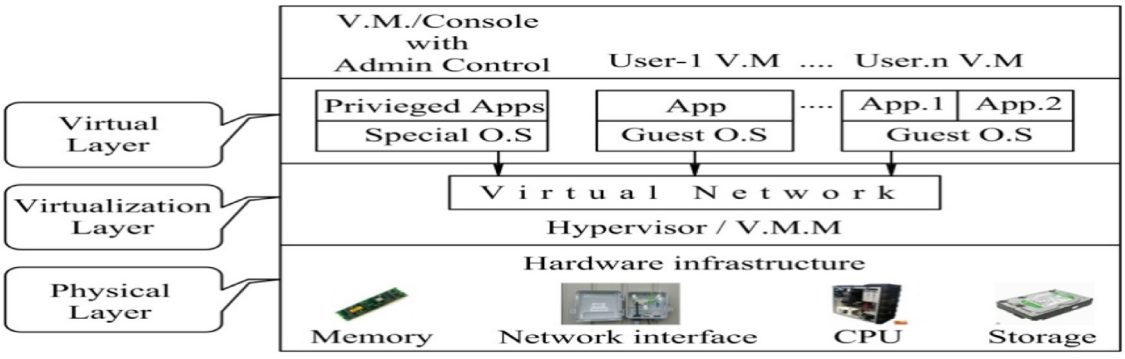

Fig. 6. Layers of virtualization.

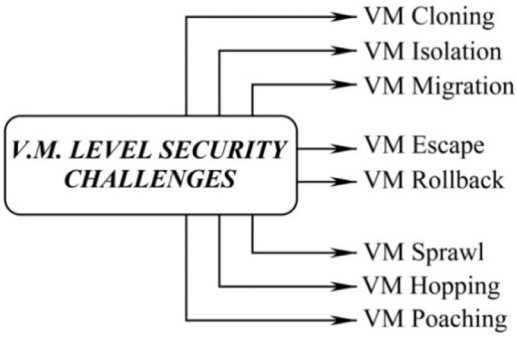

Fig. 7. VM level security challenges.

2. ***VM isolation:*** The VMs should be isolated to ensure safety and security. Isolation of VMs guarantees security for VM, even if another VM on the same physical host is compromised. But VM isolation is not the perfect solution when the hypervisor is compromised. The break in isolation due to reuse of IP addresses among the VM's leads to issues and need to be addressed. This may lead to the degradation of the entire system.
3. ***VM migration:*** VM's can be migrated from one server to another easily for improving the utilization of resources effectiveness. This process can be automated for achieving load balance and energy saving. This dynamic nature of the migration leads to security risks, not only to the migrated VM, but also for the new VM host. The modes of migrations are live and non-live VM migration. Achievement of live migration is a complex task when compared with non-live migration.
4. ***VM Escape:*** VMs usually run in isolated and self-contained environments in the host. Any attempt of the VM for direct interaction with the hypervisor through intervention in an isolated environment results in the escape of the VM. So this issue needs to be addressed properly for obviating any compromise of the entire virtual setup.
5. ***VM rollback:*** VM's can be cast backward to their former state. The revocation may be of the infected VM's to the pervious state with harmful virus/worms. So VM's, when roll backed, can be re-exposed to security vulnerabilities. Sabahi [7] used per-page encryption and hashing to protect memory snapshot. The memory contents were hashed using a Merkle hash tree depending on the granularity of pages. It is always preferred to maintain logs for all the operations, specifically suspend/resume and migration. A critical analysis reveals that VM rollback, if not handled in a secure manner, leads to activation of even harmful virus/worms.
6. ***VM sprawl*:** Uncontrolled deployment of virtual machines is known as a VM sprawl. Bose [8] has indicated, VM sprawling as a situation where there is a linear increase in the number of VMs, while a majority of them remain inactive. There are possibility of wastage of plenty of the host's resources. VM sprawl requires control to ensure achievement of effective resource management with minimal effort.
7. ***VM Hopping/VM Hyper jumps:*** VM hopping is gaining access to another VM, through the vulnerability of the hypervisor. This issue permits remote attacks and malware to compromise and attain control over the middleware packages on the underlying host by hopping from VM to VM. Often the most vulnerable VM's are identified as the launch point for further attacks on the system. This issue requires address in the future. The hypervisor vulnerability leads to a single-point-of failure.
8. ***VM poaching:*** The vulnerabilities present in the OS/apps lead to unexpected behavior of the entire system. They utilize the system resources, leading other VMs on the same host to starvation/failure. Patching the guest OS and regular application are suggested for successful mitigation of VM poaching.

Table 2 lists some articles addressing the VM security challenges

The over all analysis of Table 2, clearly lists the existing solutions to provide security to VMs. A comparative analysis of the various proposed techniques forbids any increase in the execution time and the number of the test systems. The recommendation is that packets at high rate should not be sent to VM's for maintaining the robustness of the system . And not to use the unrealistic assumption that would increase the complexity and not to neglect some identified assumptions/parameters. Advanced Cloud Protection System(ACPS), increases security and maintains integrity with minimal performance degradation. Wei [9] proposed a system that deploys many VM's on a shared network on the assumption of their belonging to a single organiztion. The authors have suggested the need for the provision of a secured system, irrespective of the VM of different organizations deployed on the same shared network.

5.1.2. Hypervisor level (Virtualization layer)

Qin [10], indicated the use of a hypervisor for monitoring the life cycle of VMs, which includes creation, suspension, resumption and migration. The Hypervisor/Virtual Machine Monitor (VMM) is just a low level code known for autonomous execution irrespective of an operating system. Hypervisor enables virtualization through resource pooling and multi-tenancy. The most common approaches to hypervisor-based virtualization are *para-virtualization. full-virtualization and hardware assisted virtualization.* Sabahi [7] stated that hypervisor-based virtualization suffers from ***Single-point-of-failure***. In Fig. 8 the challenges faced by the VMs in the

Table 2
Comparative analysis of V.M's security challenges.

S. No.	Author	Title of the security scheme	Work proposed	Strengths	Weakness
1	Schwarzkopf, 2012	Increasing virtual machine security in cloud enironments	Update checker: To identify outdated s/w packages (Dormant/Running) Online penetration suite: Performs pre-rollout scans of VMs.	Prevents execution of flawed VM's. Handles multiple software repositeries from different vendors.	Increase in runtime linearly with Increase in no. of test system. Network outages identification flaws in software component.
2	Bindra, 2012	Cloud Security: Analysis and Risk Management of VM Images.	Proposed a security analysis of the VM images.	Provides security on VM images.	……
3	Shea, 2013	Performance of Virtual Machines Under Networked Denial of Service Attacks: Experiments and Analysis	Enhancement of the robustness and security of modern virtualization.(DOS Attacks)	Implementation of SYN- proxies. Container-based virtualization is better to DOS attack	Problem arises when small packets are sent at a high rate.
4	Qin, 2012	State-of-the-art Virtualization Security in Cloud computing	Clearly categorized the issues according to virtualization security	Identifies techniques as inside and outside the V.Ms.	Identified performance factor is sometimes negelected. Some schemes are too complicated with unrealistic assumptions.
5	Lombardi, 2010	Secure Virtualization for cloud computing	Advanced Cloud Protection Systems(ACPS)	Increased security to cloud resources. Integrity of guest effectively monitored	Small performance penalty
6	Duncan, 2013	Cloud Computing: Insider Attacks on Virtual Machines During Migration	To detect insider attacks using digital forensics and system admin. techniques.	Detection of Packet Sniffing via ethernet tap	Detection of packet sniffing via passive tap is difficult.
7	Wu, 2010	Network Security for Virtual Machine in Cloud Computing	Proposed a novel virtual network framework to control communication among VM's.	Increase security through routing layer, firewall and shared network layer. Overcomes sniffing and spoofing attacks.	Restrict VMs of a single organization to be in the same shared network.

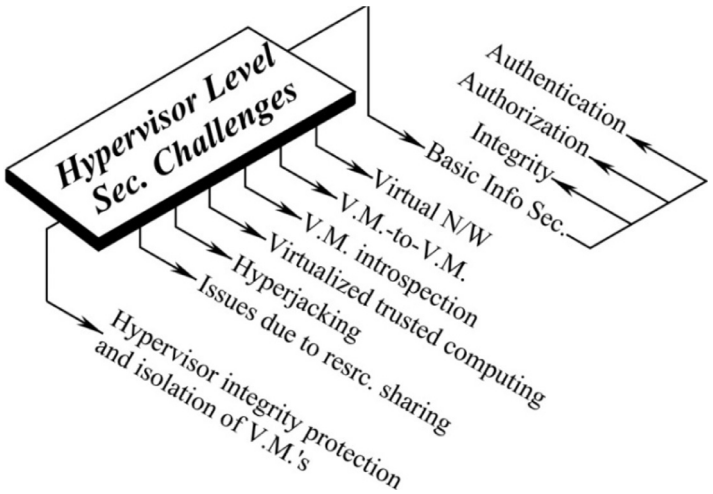

Fig. 8. Hypervisor level security challenges.

hypervisor level are clearly classified.

The following are the issues depicted in the Fig. 8.

1. ***Basic information security:*** Hypervisor level security challenges may lead to vulnerability of authentication, authorization and integrity.
2. ***Threats in virtual networking:*** The design of a virtual network should ensure secure connections between all the entities of the cloud. Brohi [11], have emphasized on the imperative need to implement hypervisor-resident VFs(Virtual Firewall) on the VMM for ensuring protection to the VM's. Laniepce [6], have listed threats like traffic snooping (network traffic interception), address spoofing (IP address forging), Virtual Local Area Network (VLAN) hopping (traffic segregation breaking), etc., thereby, identifying the threats in a virtual network need to be addressed with ease in the future.
3. ***VM-to-VM attack:*** A malicious intruder can gain the control of a VM through another VM that exists on the same physical host, by utilizing the loopholes in the hypervisor and also launch a side channel attack to corrupt the targeted VM, Laniepce [6]. A framework has been proposed by Zhang [12] for systematic detection and analysis of a number of inter-VM attacks which are easy to launch but difficult to detect. There is, therefore, a need to address this issue.
4. ***Security issue with VM introspection:*** A technique that helps monitoring the state of VM's running on a physical server is VM Introspection. More [13], focused on the Virtual Machine Introspection (VMI) tools and implemented in the hypervisor. Illegal look inside of VM's leads to unwanted access to their data and process. Therefore, they need advanced security measures for preventing unwanted access.
5. ***Issues due to virtualized trusted computing (VTC):*** The next logical step in virtualization is trusted computing, whose failure can break the security policy. Laniepce [6], Trusted Platform Module (TPM) outlined that each VM and hypervisor needs its own TPM. But in general, there is only one physical TPM managed by the hypervisor, which leads to security issues. Dongxi L [14] have referred to Virtual TPM (vTPM) and its management with keys and certificates. Software implementation of TPM increases the issues in Trusted Computing Base (TCB) and leads to vulnerabilities which should be taken care of.
6. ***Hyperjacking / hypervisor subversion:*** A malicious intruder gaining control over the hypervisor through a malicious VM with attempt to take over the control of the virtualization layer is known as hyperjacking. Miller [15], have outlined the attacks on dropbox, linkedIn, etc., due to hyperjacking. Microsoft's recent article on Hyperjacking states “viruses installed on the hardware/ BIOS can't be detected by the O.S”. Issues of this kind result in single-point-of-failures, which requires attention.
7. ***Issue due to resource sharing:*** A malicious VM leads to resource starvation to the intended VMs as a result of sharing common resources. Wueest [16], have stated that resource sharing leads to information leakage and 75% of security challenges occur due to this resource sharing. Resource sharing is one of the essential characteristics of cloud computing paradigm. Hence, there is great need to address issues related to resource sharing.
8. ***Threats in hypervisor integrity protection and isolation of VM's:*** In a virtualized environment, hypervisor manages the isolation among its guests. In the absence of protection to the integrity of the hypervisor, there is the chance of the secret of the guests being released. So, enhanced access control mechanisms in the hypervisor are required.

Table 3 presents the existing remedial techniques for hypervisor security. The listed techniques achieve hypervisor security in various ways. A comparative analysis leads to a recommendation for the use of multi-factor authentication for improving the security of the hypervisor. Virtualized Cloud Computing Infrastructures(VCCI) are secured from software related vulnerabilities by securing

Table 3
Some of the articles addressing the Hypervisor Security Challenges.

S. no.	Author	Title of the security scheme	Work proposed	Strengths	Weakness
1	Romney, 2013	The Aigility, Flexibility and Efficiency of Hypervisors in Engineering Education	Developed a NU program for Master of Science in Cyber Security and Information Assurance(MS-CSIA) with Agility- Decreases time to deploy servers, Flexibility- Cloning is easy, Efficiency- Student accessing current technology.	Use of multi-factor authentication increases security. Increase in bandwidth from 50mbps to 100mbps.	Memory is a critical factor when VM increases from 200 to 770
2	Sabahi, 2012	Secure Virtualization for Cloud Enivronment Using Hypervisor-based Technology	Proposed a new security architecture in hypervisor-based virtualization.	Improved security. Detects an overflow attack. Strengthen virtualization.	Security performance depends on VSEM and VREM.
3	Turnbull, 2013	Breakpoints: An Analysis of Potential Hypervisor Attack Vectors	Identified and analyzed four potential attacks in ESXi5.0 hypervisor	Reduced the risk of cloud computing by identifying hooking system calls and rerouting data	
4	Brohi, 2013	Identifying and Analyzing Security Threats to Virtualized Cloud Computing Infrastructures(VCCI)	Technique for virtualizing CCI type of attacks on VCCI includes the VMM.	Secured VCCI, through identifying attacks from outsiders and insiders	
5	Laniepce, 2013	Engineering Intrusion Prevention Services for Iaas Clouds: The Way of the Hypervisor	Proposed a hypervisor-based monitoring approach.	Most promising, improves user VM security.	Depends on the trust of cloud provider
6	Nimgaonkar, 2012	Ctrust: A framework for Secure and Trustworthy application execution in Cloud computing	Proposed attack model and prototype implementation of the Ctrust framework	Provides root of trust and security to users Scalable	Embedding hardware architecture.

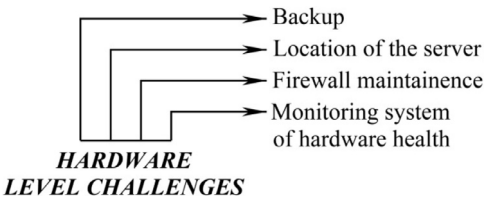

Fig. 9. Hardware level security challenges.

the Virtual Machine Monitor(VMM)/Hypervisor form both inside and outside attackers. Hypervisor-based monitoring always increases VM security and detects the overflow attack. Overall securing the hypervisor eliminates Single-point-of-failure(SPoF). The use of the concept of No hypervisor, requires the upgradation of the Operating Systems(OS) with all the features of hypervisors. However, this aggravates the complexity of the underlying OS. There is, therefore, the need for the hypervisor for achieving virtualization. Virtualization is the heart of cloud computing. The processes like Virtual Machine(VM) creation, suspension, resume, activation and allocation of the resources are available through the VMM. SPoF degrades the performance of cloud computing paradigm, so it should be secured.

5.1.3. Hardware level (Physical layer)

The hardware layer consists of resources like CPU, memory, networking and storage, etc., which is distributed over the cloud, and shared among the VMs by the virtualization layer. There is the danger of isolated protection getting breached, if through the vulnerability of the hypervisor, a guest manages to overcome the DAC(Discretionary Access Control) and MAC(Mandatory Access Control). Zissis [17] has pointed out to the security and vulnerability needs of the hardware. Threats like Distributed Denial of Service (DDOS), H/w interruption, H/w theft, H/w modification, misuse of infrastructure, etc. are possible in the absence of security to hardware. Mathisen [18], classified the issues in physical layer as in Fig. 9, like backup, location of the server, firewall maintenance and monitoring system for hardware health.

In addition to the above mentioned issues, ***hardware, health monitoring*** is required as mentioned by Turnbull [19], for finding the functionality of the hardware components and providing the information to the kernel and virtualization manager about the status of the component. The system should use a strong authentication mechanism in the virtual layer itself for mitigating the problems seen in te physical layer itself. So, that the issues related with hyperjacking can also be decreased.

6. Data level challenges

Data is the heart and the source of the entities of any crypto-cloud system. Data breach was identified as the most serious threat by CSA in Table 1. Prior to moving on to the new computing technology, there is an imperative need to have a knowledge of the number of levels of security that the technology provides to the data envisaged by this author, considering hacking capabilities are also well versed. The storage of data in some remote place (out-of-our-control) and achieving multi-tenancy gives rise to an issue called ***Data Leakage***. Chen [20] proposed the life cycle of the data, as ***Generation*** => ***Transfer*** => ***Use*** => ***Share*** => ***Storage*** => ***Archival*** => ***Destruction***, needs protection in all the stages.

Data level security on the whole can be classified as data-in-transit and data-in-rest. Data-in-transit does not lead to additional security risks when compared with data-in-rest, because, the transmission of data is done by default through TLS which provides a secured way of data transfer. From the hacker's view point data-in-rest is more attractive. Fig. 10 provides the classification of the threats related to the data level.

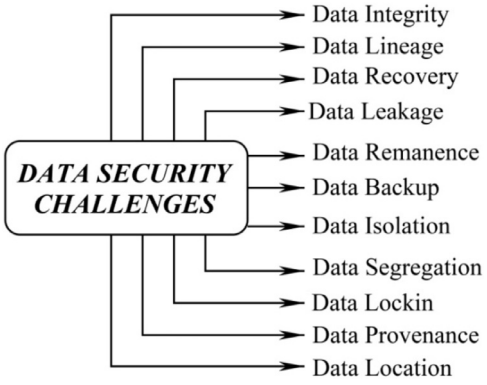

Fig. 10. Classification of data related challenges.

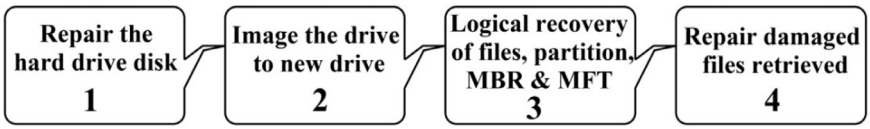

Fig. 11. Phases of data recovery.

6.1. Data in-transit

Data in-transit takes place among the entities in the crypto-cloud. The communication among the entities with a secured communication channel like Transport Layer Security, may give rise to the following issues taking place.

1. ***Data Lineage:*** Data lineage is related to the origin of the data and where it moves over a time period. Bhadauria and Sanyal [5], have proposed tracing the path of the data as data lineage. It helps in auditing. It is one of the challenging and tedious issues involved in tracing due to the non-linear nature of the cloud environment.
2. ***Data Leakage:*** Once the data is accessed by multi-tenant, the issue of data leakage arises. Sabahi [7], identified data leakage as one of the important security issues. As early as in March 2009, Chen [20], pointed out to the presence of a serious leakage of a user's private data, due to inherent security vulnerabilities in Google Docs. The danger of data leakage is substantial, requiring careful handling. Some of the challenges related to data leakage are, *Instance Messaging, Email, Web Mail, Blogs / Wikis, Malicious Web Pages, File Transfer Protocol (FTP) and Universal Serial Bus(USB)/ Mass storage device.*

6.2. Data- in-rest

Vyas [21], proposed an approach to secure storage of data in the cloud and performance integrity check on the stored data when accessing the data. Storing Encrypted file, hash file and meta-data in cloud improves the security of stored data in the cloud. Chatterjee [22] has presented review methods to ensure data security in the cloud, with the use of cryptographic measures to achieve privacy.

1. ***Data Recovery:*** The process of accessing data which is corrupted/damaged from the storage media is known as data recovery. The four phases of data recovery are depicted in Fig. 11.
   On deletion of a file, only the metadata is removed but the actual data remains on the disk. It can be recovered using file carving. Some commonly used Carving schemes are Bifragment gap carving, Smart Carving and Carving memory dumps. Common challenges to data recovery are OS failure, drive-level failure and deletion of file from a storage medium. These challenges have to be met.
2. ***Data Remanence/Sanitization/Removal:*** Data must be erased securely at the end of its life cycle. Overwriting is one of the traditional solutions for sanitizing data. According to Chen [20], the physical characteristics enable restore/recovery of deleted data, leading to disclosure of sensitive data. With proper skills and equipment, it is possible to recover data from failed devices. The remanence of the data after deletion require attention.
3. ***Data Backup:*** Frequent updating of data results in data loss. Data backup in cloud storage or external server is required for handling loss of data. Bhargav Vora [23] have specified a 3-2-1 rule, involving 3 copies of important files: 1-primary and 2-backups. They maintain the copies in 2 different storage media to defend against different types of attacks. Store 1 copy off-site. Maintenance of replication leads to security issues.
4. ***Data isolation:*** There should be a perfect separation between non-sensitive and sensitive data. Data should be isolated from unauthorized users through use of access control and encryption schemes. Fine-grained access control can be achieved through a user's identity, some of them are attribute-based, time- based etc. Isolation is a special kind of privacy. Lack of care in handling leads to VM to VM attack, there-by losing the confidentiality of the users.
5. ***Data segregation:*** Segregation of data refers to full separation between the cloud users in a virtualized environment. Negi [24], have suggested that data segregation is an issue that is raised due to multi-tenancy. Cloud providers should use highly secured protocols and encryption algorithms to achieve data segregation. Data Segregation vulnerabilities araise due to data validation, insecure storage and SQL injection flaws. Meeting the specified uses in a multi-tenant environment, is of great help in mitigating the problem of data segregation challenge.
6. ***Data Lock-in:*** Data Lock-in is the main obstacle to achievement of portability and interoperability. Sax [25], say that, in an industry insight, clearly outlined, the risk of cloud provider lock-in prevent the movement of data into, around and out of the cloud. The lock-in nature makes integration of data from different locations a difficult job. Consumers of the cloud should not get affected through this issue with a specific vendor.
7. ***Data Location:*** Storage as a service is highly dependent on the location of the data. Since the location of the data is not known to the users, users hesitate to store their sensitive data in the cloud. It is one of the common issues faced by organizations. The unknown location of data leads to questions of security, legal and requirements of regulatory compliance. This is one of the challenging issues due to untrusted cloud service providers.

Table 4
The existing remedial techniques for Data Level Challenges.

S. no.	Author	Title of the security scheme	Work proposed	Strengths	Weakness
1	Chen, 2012	Data Security and Privacy Protection Issues in Cloud Computing	*Survey:* Analyzed the data secuity and protection of data in various life cycle.	Presented the future research work related with data security and privacy protection.	
2	Wang, 2012	Toward Secure and Dependable Storage Services in Cloud Computing	A flexible distributed storage integrity mechanism, using the homomorphic token and distributed erasure-coded data.	Auditing cloud storage with less communication and computation cost. Fast data error localization. Efficient dynamic operations.	Maintains extra data structure information on the user side locally.
3	Liu, 2013	Mona: Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud	A scheme MONA for dynamic groups in the cloud.	Secured Efficient Storage and computation cost are indepent to revoked users.	
4	Wei, 2014	Security and privacy for storage and computation in cloud computing	Discouragement to privacy cheating and encouragement to secure computation auditing protocol	First protocol that bridges secure storage and computation auditing. Minimum cost It is effective and efficient	SecCloud slightly increase in time than original protocol.
5	Dong, 2014	Achieving an effective, scalable and privacy-preserving data sharing service in cloud computing.	A policy which combines CP-ABE and IBE techniques	Effective, scalable and flexible privacy-preserving data policy. Secured and provides fine-grained access control.	
6	Dong, 2015	SECO: Secure and scalable data collaboration services in cloud computing	A multi-level hierarchical identity based encryption against untrusted cloud.	Secure cloud data collaboration Provides fine-grained access control Efficient Low overhead on computation, communication and storage	Synchronization of data and privacy issues yet to be addressed.
7	Khalid, 2013	Cloud based Secure and Privacy Enhanced Authentication and Authorization protocol	An authentication and authorization protocol that outlines anonymous communication.	Easy to integrate Compatible	
8	Sun, 2013	A property-based testing framework for encryption programs	A property-based approach proposed for testing encryption programs	Effective. Fault detection capability is high.	Mimicked faults shows big difference with real-time faults. Limitation in number of Metomorphic relations(MRs).
9	Liu, 2014	Time-based proxy re-encryption scheme for secure data sharing in a cloud environment	A TimePRE to automatically expires the access rights of users	Achieves fine-grained access control and effective. Secure and practical Re-encryption cost is low	No. of keys issued to user will grow linearly. No fine-grained time accuracy.
10	Koo, 2013	Secure and efficient data retrieval over encrypted data using attribute-based encryption in cloud storage.	An efficient data retrieval scheme using ABE	Suited for Massive storage systems Access control and fast search	
11	Puthal, 2017	A dynamic prime number based efficient security mechanism for big sensing data streams	Dynamic Prime Number Based Security Verification (DPBSV) scheme for big data streams	Reduces communication overhead. Improves efficiency of verification process. Reduces time Utilize small buffer size.	
12	Shaikh, 2015	Data Classification for achieving Security in cloud computing	A data classificaton scheme and analyzed with sample datasets.	Improves security and strength substantially.	

6.3. Issues common to both data in-transit and data-in-rest

1. ***Data Integrity:*** Integrity refers to data accessed or modified by authorized entities alone. Integrity checks can be performed with/without third party audit. Kaur [26] on the other hand, proposed a data correctness scheme which involved a third party audit and ensured the safety of data. Regardless of data, both static and dynamic data should be protected from unauthorized observation, modification, or interference.
2. ***Data Provenance:*** Provenance includes the integrity of the data as well as their computational accuracy. (**integrity + computational accuracy = provenance**). However, Muhammad Rizwan Asghar[27], outlined that the description of how data is produced is provenance, therefore making it important for post-incident investigations. Martin[28], presented a risk-based approach to provenance. Some of the challenges that arose from the data provenance included computational overhead, storage overhead, platform independence and application independence among others.

Cloud data is the most important basic entity that needs to be secured. Data in transmission and data at rest both face security threats in their individual ways and also need to be addressed. Table 4, summarizes the various security challenges faced without incurring any extra storage cost, communication cost and computation cost. The SecCloud technique is an example and it results in a slight increase in time compared to the existing protocol, which is more vulnerable. Bringing down vulnerability even in the event of an escalation of cost regarded as an issue. The achievement of an effective, scalable, flexible, secured, and fine-grained access control combination of encryption techniques is possible(like Ciphertext-PolicyAttribute-Based Encryption-CPABE,& Identity Based Encryption- IBE). Future research can takeup techniques that provide more security with minimal management effort.

A system, which is strongly secured, even with the minimal increase in storage, communication, and computational cost is the need of the hour. The system should be effective, scalable and secure. However, security should not be an additional requirement, it should exist as a basic feature of the system at all levels(Computational, Communicational and Service Level Agreement).

7. Service level agreements (SLA's)

Services are to be offered by providers, to consumers with proper SLAs. Basic entities of crypto-cloud have the responsibility of maintaining the SLAs. Resource provisioning at any time depends on the bandwidth required, CPU, memory and key management amongst others. Different levels of SLA's exist and they are customer-based, service-based and multi-level SLA. There should not be any over/underestimation in the provision of the required resources.

The non-pervasive nature of SLA relates to confidentiality while integrity leads to the proposal of service level standards, Hoehl [29]. The inclusion of security metrics in SLA is necessary for mitigating risks and for effective transfer of responsibility between parties. There is no unique standard for SLA that applies to all security management needs. But some standards like European Commission SPECS(Secure Provisioning of Cloud Services) and ENISA(European Network and Information Security Agency) provide security through the maintenance of SLAs. The use of SLA helps to get a Quality of Service (QoS) upto an acceptable level. SLA includes contract definition, negotiation, monitoring and enforcement. Contract definition and negotiation, identifies the benefits and responsibilities of each party. Monitoring and enforcement build a trust between the consumer and the provider.

Dash [30], also pointed out that SLA with the scope of guaranteed availability of services. The ability of the provider, the performance of the users and availability of the services depend on the type of SLA. One should be aware of the following components in order to reduce the risk factors. Bandwidth and operation loss, the continuity of the business, the location of the data, appropriation of the data and the integrity as well as the reliability of the data among others. Only with proper SLA's the pay-as-use model can survive.

8. Conclusion

The various security issues in communication, computational and Service Level Agreement are explored. In the computational level, both virtualization and data related security issues are considered to be the most vulnerable entity. Virtualization is a basic element of cloud computing and increases the value of it. The challenges related to it in all the three layers, Virtual layer, Virtualization Layer, and Physical layer are addressed. Data related security issues are classified as issues on data at rest and issues on data in transmission. Both the issues are explored and there is great need to address issues related to them. Today, security challenges are numerous thus providing several opportunities for hackers to break the crypto-system. Though a lot of research and survey papers are in line with the survey suggested by this author. Cloud computing, still seems to be incomplete when it comes to security issues.

A comparison of our survey with other survey papers on the basis of the three basic levels is depicted in Table 5. The table shows that only a few articles have made a survey on the root cause and the effect of issues at the computational level specifically Virtual Machine level, Hypervisor level and Hardware level. There is an imperative need for a larger and intensive exploration on Service Level Agreement level as works for the future. This paper can be considered as the forerunner for a more intensive research in cloud computing through unexplored paths.

Table 5
Comparison of our survey from the perspective of three basic levels with existing surveys.

S. no.	Author	Communication level		Computational/Functional level				SLA level
		Network level	Application level	Virutalization			Data security	
				V.M. level	Hypervisor level	Hardware level		
1	Ali, 2015	X		X	X		X	X
2	Rong, 2013						X	X
3	Zissis, 2012		X	X		X	X	
4	Sun, 2011	X	X				X	
5	Shahzad, 2014	X					X	X
6	Rao, 2015	X					X	
7	Soofi, 2014	X	X				X	
8	Warhade, 2014	X	X				X	
9	Padhy, 2011	X	X	X			X	X
10	Denz, 2013			X	X	X		
11	Ouedraogo, 2015			X	X		X	X
12	Rawat, 2014					X	X	
13	Our survey	X	X	X	X	X	X	X

In general, cloud service providers should consider security as a necessity and not an afterthought.

References

[1] Mell P, Grance T. Version 15 The NIST definition of cloud computing October 7. National Institute of Standards and Technology; 2009http://csrc.nist.gov/groups/SNS/cloud-computing.
[2] Walker K. Cloud security alliance(CSA). The treacherous 12: cloud computing top threats in 2016. 2016. Feb. 29 https://cloudsecurityalliance.org/media/news/cloud-security-alliance-releases-the-treacherous-twelve-cloud-computing-top-threats-in-2016/.
[3] Kamara S, Lauter K. Cryptographic cloud storage. Microsoft Research Cryptography Group; January 2010http://research.microsoft.com/pubs/112576/crypto-cloud.pdf.
[4] Rebollo O, Mellado D, Fernandez-Medina E, Mouratidis H. Empirical evaluation of a cloud computing information security governance framework. Inf Software Technol 2015;58:44–57www.elsevier.com/locate/infsof.
[5] Bhadauria R, Sanyal S. Survey on security issues in Cloud Computing and Associated Mitigation Techniques. Int J Comput Appl (0975-888) June 2012;47(18).
[6] Laniepce S, Lacoste M, Kassi-Lahlou M, Bignon F, Lazri K, Wailly A. Engineering intrusion prevention services for iaas clouds: the way of the hypervisor, 2013 IEEE seventh international symposium on service-oriented system engineering.
[7] Sabahi F. Secure virtualization for cloud environment using hypervisor-based technology. Int J Mach Learn Comput February 2012;2(1).
[8] Bose R, Sarddar D. A SecureHypervisor-based technology create a secure cloud enivronment. Int J Emerg Res Manage Technol February 2015;4(2). ISSN: 2278-9359.
[9] Wei L, Zhu H, Cao Z, Dong X, Jia W, Chen Y, Vasilakos AV. Security and privacy for storage and computation in cloud computing. Inf Sci 2014;258:371–86www.elsevier.com/locate/ins.
[10] Qin Z, Zhang Q, Wan C, Di Y. State-of-the-art virtualization security in cloud computing. J Inf Comput Sci 2012;9(6):1487–97http://www.joics.com.
[11] Nawaz Brohi S, Adib Bamiah M, Nawaz Brohi M, Kamran R. Identifying and analyzing security threats to virtualized cloud computing infrastructures, In Proceedings of 2012 international of cloud computing, technologies, applications and management.
[12] Zhang S. Deep-diving into an easily- overlooked threat: inter-VM attacks. http://people.cis.ksu.edu/~zhangs84/papers/cloudTR.pdf; 2012.
[13] More A, Tapaswi S. Virtual machine introspection: towards bridging the semantic gap. J Cloud Comput Dec 2014.
[14] Dongxi L. A cloud architecture of virtual trusted platform module, Embedded and Ubiquitous Computing (EUC). IEEE/IFIP 8th International conference on. vol. 2010. p. 804–11.
[15] Miller CD. Associate in AMI- partners. Secuirty in the cloud: concern/excitement?, on July 10th. 2012http://www.ami-partners.com/blog.
[16] Wueest C, Barcena MB, O'Brien L. Mistakes in the Iaas cloud could put your data at risk. http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/mistakes-in-the-iaas-cloud-could-put-your-data-at-risk.pdf; May 2015.
[17] Zissis D, Lekkas D. Addressing cloud computing security issues. Future Gener Comput Syst 2012;28:583–92www.elsevier.com/locate/fgcs.
[18] Mathisen E. Security challenges and solutions in cloud computing. On 5th IEEE International conference on digital ecosystems and technologies (IEEE DEST 2011). 2011.
[19] Turnbull L, Shropshire J. Breakpoints: an analysis of potential hypervisor attack vectors. IEEE; 2013.
[20] Chen D, Zhao H. Data security and privacy protection issues in cloud computing, International conference on computer science and electronics engineering 2012.
[21] Vyas J. Prof: Prashant modi,``providing confidentiality and integrity on data stored in cloud storage by hash and meta-data approach. Int J Adv Res Eng, Sci. Technol. May 2017;4(5). e-ISSN: 2393-9877, p-ISSN: 2394-2444.
[22] Chatterjee R, Roy S. Cryptography in cloud computing: a basic approach to ensure security in cloud. IJESC 2017;7(5).
[23] Bhargav Vora S, Anandache JG. Data Backup on: cloud computing Techniques in digital libraries perspective. J Global Res Comput Sci May 2015http://www.rroij.com/open-access/data-backup-on-cloud-computing-technology-in-digital-libraries-perspective.php?aid=52577.
[24] Negi T, Chaudhary S, Rautela S. Data security in cloud computing. Int J Adv Res Comput Sci Software Eng May 2015;5(5) ISSN: 2277 128X, Available online at www.ijarcsse.com.
[25] Sax R, Reeher J. How to avoid lock-in and ensure data portability in the cloud, Feb 13, 2014.
[26] Kaur S, Khurmi DS. A review on security issues in cloud computing. Int J Comput Sci Technol March 2016.
[27] Asghar MR, Ion M, Russello G. Bruno Crispo2. Securing data provenance in the cloud, conference paper. January 2011https://www.researchgate.net/publication/220865656.
[28] Martin A, Lyle J, Namilkuo C. Provenance as a security control. https://www.usenix.org/system/files/conference/tapp12/tapp12-final17.pdf; 2012.
[29] Hoehl M. Security SLA for cloud proposal for standard cloud computing security SLAs – key metrics for safeguarding confidential data in the cloud. SANS institute 2015https://www.sans.org/reading-room/whitepapers/cloud/proposal-standard-cloud-computing-security-slas-key-metrics-safeguarding-confidential-dat-35872.
[30] Dash S, Saini H, Panda T, Mishra A. Service level agreement assurance in cloud computing: a trust issue. (IJCSIT) Int J Comput Sci Inf Technol 2014;Vol. 5(3):2899–906. ISSN:0975-9646.

Ms. Nalini Subramanian is a Research Scholar in Sathyabama Institute of Science and Technology. She received her M.E degree in Computer Science & Engineering from Sathyabama University, Chennai, India in 2006. She has 15 years of teaching experience. She is currently working in Jeppiaar Maamallan Engineering College, India. Her area of research interest includes cloud computing, network security and machine learning.

Dr. Andrews Jeyaraj received Ph.D degree in 2014 from Sathyabama University in the area of code optimization. He has published more than 40 research papers in referred international and national journals. His research interest includes machine learning, compiler design, operating system and Deep learning networks. He works currently as a Professor in the Department of School of Computing at Sathyabama Institute of Science and Technology, Chennai and has more than 15 years of teaching experience.