10-31-2013

Security and Privacy in Cloud Computing: A Survey

Shilpashree Srinivasamurthy
Indiana University - Purdue University Fort Wayne, srin01@students.ipfw.edu

David Q. Liu
Indiana University - Purdue University Fort Wayne, liud@ipfw.edu

Athanasios V. Vasilakos
University of Western Macedonia, Greece, vasilako@ath.forthnet.gr

Naixue Xiong
Colorado Technical University - Colorado Springs, nxiong@coloradotech.edu

Security and Privacy in Cloud Computing: A Survey

[1]Shilpashree Srinivasamurthy; [2] David Q. Liu; [3]Athanasios V. Vasilakos ; Naixue Xiong*

[1]Department of Computer Science Indiana Univ. – Purdue Univ. Fort Wayne Fort Wayne, IN 46805, USA
[2]Department of Computer Science Indiana Univ. – Purdue Univ. Fort Wayne Fort Wayne, IN 46805, USA
[3]Department of Computer Engineering University of Western Macedonia 56100 Kozani, Greece

*School of Computer Science Colorado Technical University Colorado Spring, CO 80907, USA

[1]srins01@students.ipfw.edu; [2]liud@ipfw.edu; [3]vasilako@ath.forthnet.gr; *nxiong@coloradotech.edu

Abstract- **Cloud computing can be defined as management and provision of different resources, such as, software, applications and information as services over the cloud (internet) on demand. Cloud computing is based on the assumption that the information can be quickly and easily accessed via the net. With its ability to provide dynamically scalable access for users, and the ability to share resources over the Internet, cloud computing has recently emerged as a promising hosting platform that performs an intelligent usage of a collection of services, applications, information and infrastructure comprised of pools of computers, networks, information and storage resources. Cloud computing is a multi-tenant resource sharing platform, which allows different service providers to deliver software as services in an economical way. Cloud computing is the latest technology revolution in terms of usage and management of IT resources and services driven largely by marketing and service offerings from the largest IT vendors including Google [26], IBM [19], Microsoft, and HP along with Amazon [17, 20, 24] and VMWare. However along with these advantages, storing a large amount of data including critical information on the cloud motivates highly skilled hackers, thus creating a need for the security is considered as one of the top issues while considering Cloud Computing. In this paper, we first explain the security model of cloud computing, and then analyze the feasibility, threats, and security in cloud computing in terms of extensive existing methods to control them along with their pros and cons. After that, the related open research problems and challenges are explored to promote the development of cloud computing.**

Keywords- Cloud Computing; Fault Tolerance; Security And Privacy; Services

I. INTRODUCTION

Cloud computing is the collection of virtualized and scalable resources, the capability of hosting application and providing required services to the users with the "pay only for use" strategy, where the users pay only for the number of service units they consume. Cloud computing can be defined as the provision of computing services via the Internet such as [7]: Applications (software-as-a-service, or SaaS), Platforms, Infrastructure (IaaS), and Process orchestration and integration.

Cloud computing refers to the delivery of computing and storage capacity [42] as a service to a heterogeneous community of end-recipients. The name comes from the use of clouds as an abstraction for the complex infrastructure it contains in system diagrams. Cloud computing entrusts services with a user's data, software and computation over a network [41]. It has considerable overlap with software as a service (SaaS) [1-5, 30].

This next subsection explains the five essential characteristics defined by NIST (National Institute of Standards and Technology) [30].

On-demand self-service: The on-demand self-service is defined as the service provided by cloud computing vendors that enables the provision of cloud resources on demand whenever they are required [1].

Broad network access [2]: The cloud computing provides the access to the various resources in the world via broad network access [40], including both wired, fiber and wireless networks [46].

Resource pooling [3]: It is generally considered as a pool of resources such as assets, equipment, personnel, effort, etc., for the purposes of maximizing advantage and/or minimizing risk to the users.

Rapid elasticity [4]: It is defined as the rapid ability to scale resources both up and down as needed. To the consumer, the cloud appears to be infinite, and the consumer can purchase as much or as little computing power as they need [44]. Defined by the National Institute of Standards and Technology (NIST) as one of the five essential characteristics of cloud computing.

Measured service [5]: Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service.

The main contributions of this paper are as follows: we first introduce the user to the concept of cloud computing by discussing the various essential characteristics, and then the architecture of cloud computing is described. After that, we discuss the various advantages and threats [32], the various security aspects [43], and the various security architecture of cloud computing. Finally, the open challenges of cloud computing [22] are explored. This paper focus on exploring and analyzing new findings, which include new technological developments as well as new understandings in the field of cloud computing.

The rest of this paper is organized as follows: Section 2 explains the security architecture of cloud computing. In Section 3, we first describe the feasibility of cloud computing wherein the various advantages of cloud computing are weighed against the obstacles and threats,

and then the various cloud computing threats and the various security aspects are identified from various scholarly articles. Section 4 explains the various solutions that are proposed for existing threats, the solution architecture and pros and cons of each solution. In Section 5, the paper explains the open research problems and challenges of Cloud Computing. Finally, we conclude our work.

II. SECURITY ARCHITECTURE OF CLOUD COMPUTING

Security is an important issue concerning the cloud computing. Obviously It is no secret that cloud computing is becoming more and more popular today and is ever increasing in popularity with large companies as they share valuable resources in a cost effective way, and there is an ever growing threat of security becoming a major issue [38]. This paper shall look at ways in which security threats can be a danger to cloud computing and how they can be avoided [34]. Chen et al. [35] had examined contemporary and historical perspectives, and argued that few cloud computing security issues are fundamentally new or fundamentally intractable as well as that two facets are to some degree new and fundamental to cloud computing: the complexities of multi-party trust considerations, and the ensuing need for mutual auditability.

Figure 1 shows the open secure architecture of cloud computing. The Open Security Architecture cloud-computing pattern [23, 33] is a proposed to illustrate core cloud functions, the key roles for oversight and risk mitigation, and collaboration across various internal organizations, and the controls that require additional emphasis. The various controls in this architecture are as follows.

- SA-1/4/5 System and Services Acquisition: ensure that acquisition of services is managed correctly.
- CP-1 (Contingency Planning): ensure a clear understanding of how to respond in the event of interruptions to service delivery.
- Risk Assessments controls: helps to understand the risks associated with services in a business context [25].

The pattern also provides a view into activities that are shared by security architects, security managers, and business managers. They should

• Agree on the control baseline applicable to this cloud sourcing activity/service.

• Confirm how this translates into the control framework of the cloud provider.

• Decide on additional risk mitigating controls.

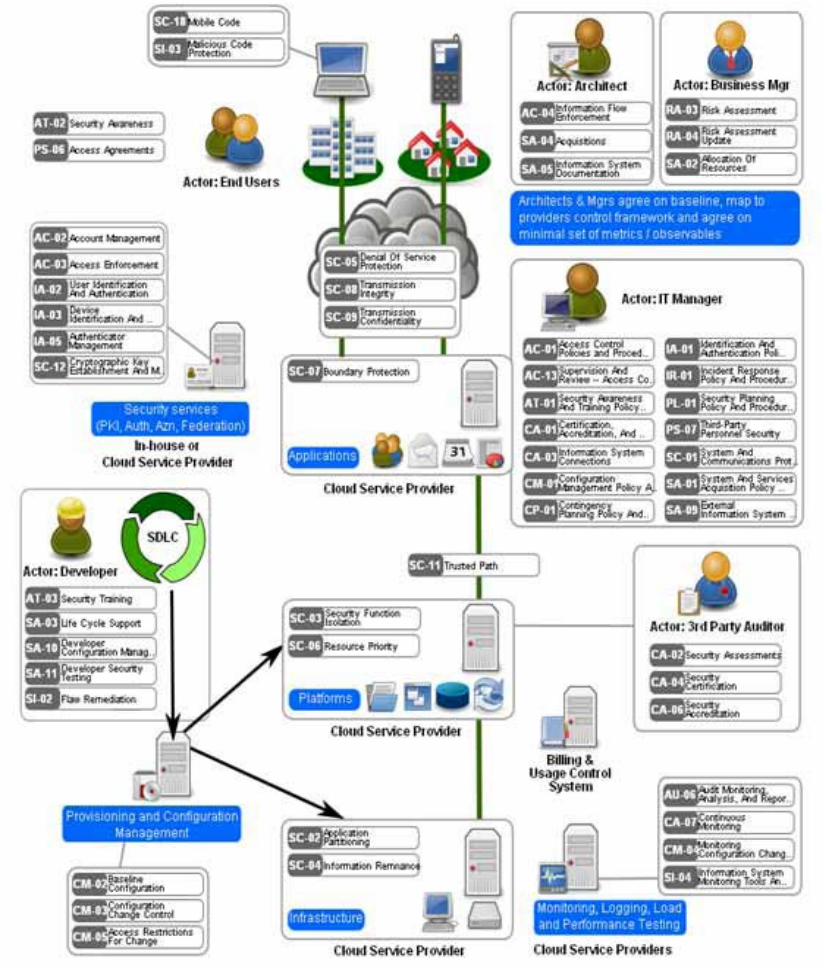

Figure 1. Cloud Computing Model - Open Secure Architecture [33]

There are a number of key control areas that should be considered carefully before moving the computing operations to cloud services: contractual agreements, certification and third-party audits, compliance requirements, availability, reliability, and resilience, backup and recovery, service levels and performance, decommissioning. If the process is comprised of a number of cloud services, then supporting services such as security, load monitoring & testing and provisioning and configuration management are required.

The important entities involved in the data flow are end users, developers, system architect, third party auditors and the cloud itself [4].

- **End Users.** End Users need to access certain resources in the cloud and should be aware of access agreements such as acceptable use or conflict of interest. In this model, end user signatures may be used to confirm someone is committed to such policies. The client organization should run mechanisms to detect vulnerable code or protocols at entry points.
- **System Architects.** System architects are employed with writing the policies that pertain to the installation and configuration of hardware components and software. They designate control protocols to direct the information flow within the cloud.
- **Developers.** Cloud computing can improve software development by scaling the software environment through elasticity of resources. The cloud also helps developers create multiple evaluation versions environments for their applications, bypassing the need to incorporate additional security within the application and placing the burden on the cloud provider. Software monitoring may be done by monitoring API calls for server requests. Security patches for the software as service approach, updating a patch is easier done in the cloud and shared with everyone seamlessly.
- **Third Party Auditors.** Third party auditors are used by clients and providers alike to determine the security of the cloud implementation. Depending on the level of commitment to security and usefulness in obtaining a competitive edge, a cloud vendor may choose to submit itself to regular security assessments in an attempt to obtain accreditation.

III. FEASIBILITY, THREATS, AND SECURITY OF CLOUD COMPUTING

This section analyzes the feasibility, threats, and security issues of Cloud Computing.

A. Feasibility of Cloud Computing

a) Advantages of cloud computing

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources that can be provisioned and released with minimal management effort or service provider interaction [30]. This section explains the various advantages of cloud computing [1, 12]

- **Virtualization**. The main advantage of cloud computing is Virtualization which is decoupling and separation of the business service from the infrastructure needed to run it.
- **Flexibility to choose vendor**. Cloud computing provides flexibility to choose among multiple vendors that provide reliable and scalable business services, development environments, and infrastructure that can be leveraged out of the box and billed on a metered basis—with no long term contracts.
- **Elasticity**. Elastic nature of the infrastructure allows rapidly allocating and de-allocating massively scalable resources to business services on a demand basis.
- **Cost Reduction.** Reduced costs due to operational efficiencies, and more rapid deployment of new business services. Cloud computing is particularly attractive to businesses in times of financial recession and credit squeezes, because using cloud services enables them to substitute capital expenditure on hardware and software to meet their worst-case computing requirements with operating expenditure that relates to the amount of computing that they actually use.
- Appearance of infinite computing resources on demand.
- Elimination of an up-front commitment by Cloud users.
- Ability to pay for use of computing resources on a short-term basis as needed.
- Economies of scale due to very large data centers [42].
- Higher utilization by multiplexing of workloads from different organizations.
- Simplify operation and increase utilization via resource virtualization.

b) Obstacles and Opportunities for Growth of Cloud Computing

The following table shows the main obstacles and opportunities for the growth of cloud computing as explained in the paper “A View of Cloud Computing” [12].

TABLE 1. OBSTACLES AND OPPORTUNITIES OF CLOUD COMPUTING

No	OBSTACLE	OPPORTUNITIES
1	Availability/Business Continuity	Use Multiple Cloud Providers
2	Data Lock-In	Standardize APIs; Compatible SW to enable Surge or Hybrid Cloud Computing
3	Data Confidentiality and	Deploy Encryption, VLANs,

	Auditability	Firewalls
4	Data Transfer Bottlenecks	FedExing Disks; Higher BW Switches
5	Performance Unpredictability	Improved VM Support; Flash Memory; Gang Schedule VMs
6	Scalable Storage	Invent Scalable Store
7	Bugs in Large Distributed Systems	Invent Debugger that relies on Distributed VMs
8	Scaling Quickly	Invent Auto-Scalar that relies on ML; Snapshots for Conservation
9	Reputation Fate Sharing	Offer reputation-guarding services like those for email
10	Software Licensing	Pay-for-use licenses

Despite of these obstacles as well as opportunities and advantages, cloud computing raises several security issues and hence security is still the primary concern of many customers who want to leverage public cloud services.

B. *Cloud Computing Security Threats*

Security is one of the major issues, which reduces the growth of cloud computing and complications with data privacy and data protection continue to plague the market [39, 48]. The advent of an advanced model should not negotiate with the required functionalities and capabilities present in the current model [36]. In this section we describe the threats appearing in the cloud computing.

Top seven security threats: Top seven security threats to cloud computing discovered by "Cloud Security Alliance" (CSA) are [21, 32].

1. Abuse and Nefarious Use of Cloud Computing
2. Insecure Application Programming Interfaces
3. Malicious Insiders
4. Shared Technology Vulnerabilities
5. Data Loss/Leakage
6. Account, Service & Traffic Hijacking
7. Unknown Risk Profile

Abuse and Nefarious Use of Cloud Computing [1]**:** Abuse and nefarious use of cloud computing is the top threat identified by the CSA. A simple example of this is the use of botnets to spread spam and malware. Attackers can infiltrate a public cloud, for example, and find a way to upload malware to thousands of computers and use the power of the cloud infrastructure to attack other machines.

Suggested remedies by the CSA to lessen this threat:

- Stricter initial registration and validation processes.
- Enhanced credit card fraud monitoring and coordination.
- Comprehensive introspection of customer network traffic.
- Monitoring public blacklists for one's own network blocks.

Insecure Application Programming Interfaces [2]: As software interfaces or APIs are what customers use to interact with cloud services, those must have extremely secure authentication, access control, encryption and activity monitoring mechanisms - especially when third parties start to build on them.

Suggested remedies by CSA to lessen this threat:

- Analyze the security model of cloud provider interfaces.
- Ensure strong authentication and access controls are implemented in concert with encrypted transmission.
- Understand the dependency chain associated with the API.

Malicious Insiders [3]: The malicious insider threat is one that gains in importance as many providers still don't reveal how they hire people, how they grant them access to assets or how they monitor them. Transparency is, in this case, vital to a secure cloud offering, along with compliance reporting and breach notification.

Suggested remedies by CSA to lessen this threat:

- Enforce strict supply chain management and conduct a comprehensive supplier assessment.
- Specify human resource requirements as part of legal contracts.
- Require transparency into overall information security and management practices, as well as compliance reporting.
- Determine security breach notification processes.

Shared Technology Vulnerabilities [4]: Sharing infrastructure is a way of life for IaaS providers. Unfortunately, the components on which this infrastructure is based were not designed for that. To ensure that customers don't thread on each other's "territory", monitoring and strong compartmentalization is required.

Suggested remedies by CSA to lessen this threat:

- Implement security best practices for installation/configuration.
- Monitor environment for unauthorized changes/activity.
- Promote strong authentication and access control for administrative access and operations.
- Enforce service level agreements for patching and vulnerability remediation.
- Conduct vulnerability scanning and configuration audits.

Data Loss/Leakage [5]: Be it by deletion without a backup, by loss of the encoding key or by unauthorized access, data is always in danger of being lost or stolen. This is one of the top concerns for businesses, because they not only stand to lose their reputation, but are also obligated by law to keep it safe [18].

Suggested remedies by CSA to lessen this threat:

- Implement strong API access control.

- Encrypt and protect integrity of data in transit.
- Analyze data protection at both design and run time.
- Implement strong key generation, storage and management, and destruction practices [49].
- Contractually demand providers to wipe persistent media before it is released into the pool.
- Contractually specify provider backup and retention strategies.

Account, Service & Traffic Hijacking [6]: Account service and traffic hijacking is another issue that cloud users need to be aware of. These threats range from man-in-the-middle attacks, to phishing and spam campaigns, to denial-of-service attacks.

Suggested remedies by CSA to lessen this threat:

- Prohibit the sharing of account credentials between users and services.
- Leverage strong two-factor authentication techniques where possible.
- Employ proactive monitoring to detect unauthorized activity.
- Understand cloud provider security policies and SLAs.

Unknown Risk Profile [7]: Security should always in the upper portion of the priority list. Code updates, security practices, vulnerability profiles, intrusion attempts - all things that should always be kept in mind.

Suggested remedies by CSA to lessen this threat:

- Disclosure of applicable logs and data.
- Partial/full disclosure of infrastructure details (*e.g.*, patch levels, firewalls, etc.).
- Monitoring and alerting on necessary information.

Multiple security technology combination [49]: Existing work on cloud security mainly focuses on cloud storage or Traffic Hijacking without taking computation security into consideration. [49] proposes a novel auditing scheme (SecCloud) to secure cloud computing based on probabilistic sampling schemes as well as designated verifier technique, which aims to consider multiple factors together: secure data storage, computation and privacy preserving. They also discuss how to optimize sampling size to minimize the auditing cost and finally get good service performance [48].

C. Security and Privacy in cloud computing

The security issue can be discussed in various layers of the cloud computing model. In this section, we have explained various security issues of cloud computing and how it can be addressed [31].

- **Infrastructure Security.** Infrastructure security can be ensured by addressing the threats at various levels namely network level, host level and application level. The security challenges at various levels are not specifically caused by cloud computing instead are exacerbated by its use. The issues of infrastructure security and cloud computing can be addressed by clearly defining trust boundaries by understanding which party provides which part of security [27].
- **Data Security and Storage.** Data security is a significant task, with a lot of complexity. Methods of data protection, such as redaction, truncations, obfuscation, and others, should be viewed with great concern. Not only are there no accepted standards for these alternative methods, but also there are no programs to validate the implementations of whatever could possibly be developed. Homomorphic encryption can be used for data security encryption. But with this approach key management is a problem.
- **Identity and Access Management (IAM).** The key critical success factor to managing identities at cloud providers is to have a robust federated identity management architecture and strategy internal to the organization. Using cloud-based "Identity as a Service" providers may be a useful tool for outsourcing some identity management capabilities and facilitating federated identity management with cloud providers [8]. Enterprises should prepare with an IAM strategy and architecture that allows them to extend their IAM practice using standard protocols, such as SAML, SPML, and XACML, to manage user account provisioning, authentication, and authorization in the cloud
- **Security Management.** From a security management perspective, a key issue is the lack of enterprise-grade access management features. The scope of security management of cloud services will vary with the service delivery model, provider capabilities, and maturity. Customers will have to make trade-offs with respect to the flexibility and control offered by the SPI services. The more flexible the service, the more control you can exercise on the service, and with that come additional security management responsibilities. In a virtualized environment where infrastructure is shared across multiple tenants, your data is commingled with that of other customers at every phase of the life cycle—during transit, processing, and storage. Hence, it is important to understand the location of the service, service-level guarantees such as inter-node communication, and storage access (read and write) latency.
- **Audit and Compliance.** A programmatic approach to monitoring and compliance will help prepare CSPs (Cloud Service Provider) and their users to address emerging requirements and the evolution of cloud business models. To drive efficiency, risk management, and compliance, CSPs need to implement a strong internal control monitoring function coupled with a robust external audit process. To gain comfort over their in-cloud

activities, CSP users need to define their control requirements, understand their CSP's internal control monitoring processes, analyze relevant external audit reports, and properly execute their responsibilities as CSP users.

- **Security-as-a service [43].** Security-as-a-service is likely to see significant future growth for two reasons. First, a continuing shift in information security work from in-house to out-sourced will continue. Second, several other information security needs are present for organizations currently, but they will accelerate in need and complexity with the growing adoption of cloud computing [28]. The two proactive controls are important to the growth of cloud computing: identity management that is inter-cloud and scalable to the cloud size, and (encryption) key management. The two reactive controls are needed for audit and compliance purposes as well: scalable and effective SIEM, and data leakage prevention (DLP). Providing solutions to each of these controls will be difficult and requires significant complexity that must be hugely scalable and yet easy to use.
- **Privacy.** The paper "Taking Account of Privacy when Designing Cloud Computing Services [9]" explains the various privacy challenges that are faced when cloud is used as production environment and also provides key design principles to address these issues.

Privacy is an important issue for cloud computing, both in terms of legal compliance and user trust and this need to be considered at every phase of design. Maintaining the levels of protection of data and privacy required by current legislation in cloud computing infrastructure is a new challenge, as is meeting the restrictions on cross-border data transfer [28]. As cloud services process users' data on machines that the users do not own or operate, this introduces privacy issues and can lessen users' control.

a) Privacy Challenge

The key challenge for software engineers to design cloud services in such a way as to decrease privacy risk and to ensure legal compliance [25]. As with security, it is necessary to design in privacy from the outset, and not just bolt on privacy mechanisms at a later stage.

It is also important to allay users' fears about usage of cloud services. Concerns arise when it is not clear to individuals why their personal information is requested or how it will be used or passed on to other parties: this lack of control leads to suspicion and ultimately distrust. There are also security-related concerns about whether the personal data in the cloud will be adequately protected.

Information that needs protection: The following types of information are privacy sensitive and hence needs to be protected.

- **Personally identifiable information (PII):** any information that could be used to identify or locate an individual (e.g. name, address) or information that can be correlated with other information to identify an individual (e.g. credit card number, postal code, Internet Protocol (IP) address).
- **Sensitive information:** information on religion or race, health, sexual orientation, union membership or other information that is considered private. Such information requires additional safeguards. Other information that may be considered sensitive includes personal financial information and job performance information.
- **Information considered being sensitive PII**, e.g. biometric information or collections of surveillance camera images in public places.
- **Usage data**: Usage data collected from computer devices such as printers; behavioral information such as viewing habits for digital content, users' recently visited websites or product usage history.
- **Unique device identities:** Other types of information that might be uniquely traceable to a user device, e.g. IP addresses, Radio Frequency Identity (RFID) tags, unique hardware identities.

b) Privacy threats and risks of cloud computing

Privacy risks for cloud computing: The main privacy risks are:

- **For the cloud service user:** being forced or persuaded to be tracked or give personal information against their will, or in a way in which they feel uncomfortable.
- **For the organization using the cloud service:** non compliance to enterprise policies and legislation, loss of reputation and credibility.
- **For implementers of cloud platforms**: exposure of sensitive information stored on the platforms (potentially for fraudulent purposes), legal liability, loss of reputation and credibility, lack of user trust and take-up [27].
- **For providers of applications on top of cloud platforms:** legal non compliance, loss of reputation, 'function creep' using the personal information stored on the cloud, i.e. it might later be used for purposes other than the original cloud service intention.
- **For the data subject:** exposure of personal information.

Key privacy requirement:

- **Notice, openness and transparency**. Anyone who wants to collect users' information must tell them what they want to collect, how they want to use it, how long they will keep it, with whom they will share it, and any other uses they intend for the information. They must also notify users if they want to make a change in how the information is

used. If information is to be passed on to third parties, this also has to be notified. Personal information must be collected directly from the person unless there are very good reasons why this is not possible. Privacy policies must be made available to clients, and be understandable [22].

- **Choice, consent and control**. Users must be given the choice of whether they want this information to be collected or not. Data subjects must give their consent to the collection, use and disclosure of their PII**.**
- **Scope/minimization.** Only information that is required to fulfill the stated purpose should be collected or shared. The collection of data should be minimized.
- **Access and accuracy**. Users must be able to get access to personal information, to see what is being held about them, and to check its accuracy. Every effort must be made to ensure that the personal information held is accurate.
- **Security safeguards.** Safeguards must prevent unauthorized access, disclosure, copying, use or modification of PII
- **(Challenging) compliance.** Clients must be able to challenge an agency's privacy process. Transactions must be compliant to privacy legislation. One aspect of this is respecting cross border transfer obligations.
- **Purpose**. Data usage has to be limited to the purpose for which it was collected. There must be a clearly specified purpose for the collection and sharing of personal information. Data subjects should be told why their data is being collected and shared at or before the time of collection.
- **Limiting use – disclosure and retention.** Data can only be used or disclosed for the purpose for which it was collected and should only be divulged to those parties authorized to receive it. Personal data should be aggregated or anonymized wherever possible to limit the potential for compute matching of records. Personal information should only be kept as long as is necessary.
- **Accountability.** An organization must appoint someone to ensure that privacy policies and practices are followed. Audit functions must be present to monitor all data accesses and modifications.

c) Guidelines while designing the cloud

1. *Carry out a Privacy Impact Assessment (PIA):* PIA assesses the privacy requirements of new and existing systems; it is primarily intended for use in public sector risk management, but is increasingly seen to be of value to private sector businesses that process personal data. A Privacy Impact Assessment should be initiated early in the design phase, and its output fed into the design process in an iterative manner.

2. Assess at different phases of design: **Differing privacy requirements need to be considered according to the product lifecycle stage, namely:**

- **Initiation**: setting high level recommendations
- **Planning:** describing privacy requirements in detail
- **Execution:** identifying problems relating to the privacy solutions which have been proposed, considering alternative solutions if necessary, and documenting issues and any privacy exposures
- **Closure:** using audit and change control procedures in the production environment; considering privacy protection during backup, fault repair, business continuity and disaster recovery
- **Decommission:** ensuring secure deletion and disposal of personal and sensitive information

3. Use Privacy Enhancing Technologies (PETs) whenever appropriate: Privacy Enhancing Technology can be broadly thought as any technology that exists to protect or enhance individual's privacy, including facilitating individuals' access to their rights under the Data Protection Act 1998. For example privacy management tools that enable inspection of service-side polices about the handling of personal data

Recommended privacy practices: The following tips are recommended for cloud system designers, architects, developers and Testers.

Minimize personal information sent to and stored in the cloud

- Protect personal information in the cloud
- Maximize user control
- Allow user choice
- Specify and limit the purpose of data usage
- Provide feedback

d) Open issues

There are still many open issues exist in the field of cloud computing. Some of them are covered below.

- Policy enforcement within the cloud could prove very challenging.
- It may only be possible to determine that data processing takes place somewhere within the cloud, and not the specific places where this takes place.
- It may be difficult to determine the processors of data – for example, if subcontractors are involved.
- It may be difficult at the outset of the design of a cloud computing service to know exactly how the later evolutions of that service will turn out. In particular, cloud computing is subject to a paradigm shift in user requirements from traditional approaches, in the sense that a full design specification in advance is not always appropriate, and user requirements need to be tested more frequently. Therefore, methodologies such as Agile software development may be particularly relevant.

IV. EXISTING SOLUTIONS TO CLOUD COMPUTING SECURITY THREATS

In this section we will discuss some of the existing solutions to the security threats mentioned in the above section and also discuss few of the pros and cons in them.

A. Mirage Image Management System

Mirage Image Management System [13] addresses the security related risks associated with Virtual Machine image sharing that are faced by image publishers, image retrievers and administrators of the cloud repository. This new image management system proposed in the paper "Managing security of virtual machine images in a cloud environment" controls access to images, tracks the provenance of images, and provides users and administrators with efficient image filters and scanners that detect and repair security violations.

One of the security problem associated with cloud computing is secure management of the virtual-machine images that encapsulate each application of the cloud. The initial state of each virtual machine in the cloud is determined by these images and hence these images have high integrity. Users must be able to share images safely. Users should also be able to use the images built by the third parties.

A cloud provides three types of resources:

- A collection of virtual machine (VM) images
- A set of computer servers on which the VM images can be run
- A storage pool to store persistent user data optionally.

The security and integrity of VM images are the foundation for the overall security of the cloud since many of them are designed to be shared by different and often unrelated users.

a) Security Risks in an Image Repository

Cost reduction in cloud computing is achieved by sharing the knowledge of how to manage a piece of IT asset via VM images. Thus VM image sharing is one of the fundamental underpinnings of cloud computing.

VM image sharing unavoidably introduces security risks.

- **Security concerns from the perspective of owner:** The publisher, or owner, of an image is the one who contributes the original image to the repository. She is mostly concerned about confidentiality
- **Security concern from the perspective of consumer:** The retriever, or consumer, of an image is the one who retrieves the image from the repository and runs it on the compute servers. She is mostly concerned about safety
- **Security concern from the perspective of administrator:** The administrator is concerned with the security and compliance of the cloud system as a whole and the integrity of individual images. The administrator assumes the liability of potential damages caused by malware contained in any image stored in the repository.
- **Publisher's Risk.** By publishing an image, the publisher risks releasing sensitive information inadvertently. Although traditional software publishers run similar risks, the problem is larger for image publishers because images contain installed and fully configured applications: the configuration might require dangerous operations like creating password-protected user accounts and, if the publisher sets up the application by running an instance of the image, she may unwittingly create files that should not be made public. The publisher may want to share her image with only a limited set of users. Therefore, the store should support some form of access control for images.
- **Retriever's Risk.** The retriever risks running vulnerable or malicious images introduced into the repository by a publisher. Virtual machine image sharing provides an easier way of developing and propagating Trojan horses. Using a virtual machine image as a carrier for the Trojan horse makes the hacker's job easier, because the virtual machine image encapsulates all software dependencies of the Trojan horse. The retriever also risks running illegal software contained in the image.
- **Repository Administrator's Risk.** The repository administrator risks hosting and distributing images that contain malicious or illegal content. The security level of a dormant VM image is not constant and degrades over time, because vulnerability may be unknown when the VM image is initially published but become known and exploitable later. Administrators carry a latent security risk that stems from long-lived but inactive images. As the number of VM images grows, so does the risk and along with it the cost of maintenance.

b) Mirage Image Management System

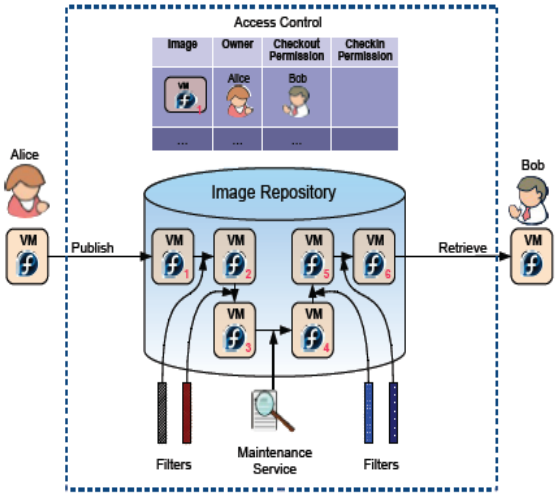

Figure 2. Architecture of Mirage Image Management System.

Figure 2 shows the architecture of Mirage Image Management System. Mirage Image Management System consists of 4 major components:

- An access control framework that regulates the sharing of VM images,
- Filters that remove unwanted information from images at publish and retrieval time,
- A provenance tracking mechanism that tracks the derivation history of an image, and
- Repository maintenance services, such as periodic virus scanning, that detect and fix vulnerabilities discovered after images are published.

A detailed explanation of these components is given below.

- **Access Control.** Each image in the repository has a unique owner, who can share images with trusted parties by granting access permissions. All other operations on an image, such as granting and revoking access to the image, require the operator to be the owner. By default an image is private, meaning that no one but the owner and the administrator can access the image.
- **Image Transformation by Running Filters.** Filters at publish time can remove or hide sensitive information from the publisher's original image. Two types of filters can be applied at publish time: repository- specific filters and user-specific filters. Repository-specific filters are system-wide filters that reflect security best practices. Some of them are mandatory and some of them are optional. The publisher can specify the composition of the optional filters. User-specific filters are intended to remove or hide user-specific sensitive content from the images. For the safety of the repository, user-supplied filters are never executable code. Instead, they are high-level specifications of transformation rules that are interpreted by the repository. The order in which filters are applied matters. For example if the user-specific filters were allowed to run after critical repository-specific filters, they could invalidate the latter's guarantees. Filters can also be applied at retrieve time. Such filters may be specified by the publisher or the retriever.
- **Provenance Tracking.** The image management system tracks the derivation history of an image by recording the parent image information when a new image is deposited into the repository, along with the information about the operation that resulted in the creation of the new image. The provenance information is used in two ways. It can be consumed by an audit system to trace the introduction of illegal or malicious content. It can also be used to alert the owners of derived images when the parent image is patched, so that the derived images can be patched as well. Although not a security feature, the provenance information can also be displayed to the end user for her to visually inspect the derivation history of her images.
- **Image Maintenance.** Repository provides a set of maintenance services that can be efficiently run over the entire repository. Example maintenance services include malware detectors (e.g., virus scanners), license compliance managers, and security patches.

c) Advantages:

- Filters mitigate the risk in a systematic and efficient way.
- The system stores all the revisions which allows the user to go back to the previous version if the current version if she desires.
- The default access permission for an image is private so that only owner and system administrator can access the image and hence untrusted parties cannot access the image.

d) Limitations:

- Filters cannot always be 100% accurate, since what constitutes illegal or private content is highly application dependent. This system does not eliminate that risk entirely, but it does mitigate the risk, in a systematic and efficient way.
- By the same token, virus scanning does not guarantee to find all malware in an image.
- Using simple pattern matching to support user-specific filters may render the resulting VM image unusable in some cases.
- It may seem counter intuitive, but "the ability to monitor or control customer content" might increase the liability of the repository provider

B. A Client-Based Privacy Manager

The paper “A Client-Based Privacy Manager for Cloud Computing” [11] provides a client-based privacy manager that helps reduce the risk of data leakage and loss of privacy of the sensitive data processed in the cloud, and that provides additional privacy-related benefits

a) Requirements

A client based privacy manager should meet the following set of requirements that arise from privacy legislation.

R1. **Minimization of personal and sensitive data used and stored within the cloud infrastructure.**

R2. **Security protection of data used and stored within the cloud infrastructure [29]**: safeguards must prevent unauthorized access, disclosure, copying, use or modification of personal information.

R3. **Purpose limitation:** data usage within the cloud has to be limited to the purpose for which it was collected and should only be divulged to those parties authorized to receive it.

R4. **User centric design:** the user should be given choice about whether or not his information is collected to be used within the cloud, his consent should be solicited

over the gathering and usage of such information and he should be given control over the collection, usage and disclosure of personal and sensitive information.

R5. **User feedback:** notice about data collection should be provided to the user about what information will be collected, how it will be used, how long it will be stored in the cloud, etc. and there should be transparency about how personal information that is collected is going to be used within the cloud.

b) Privacy Manager Architecture

Figure 3 shows the overall architecture of the privacy manager.

Features of Privacy Manager: The typical features of the privacy manager include:

1. Obfuscation
2. Preference setting
3. Data Access
4. Feedback
5. Personae

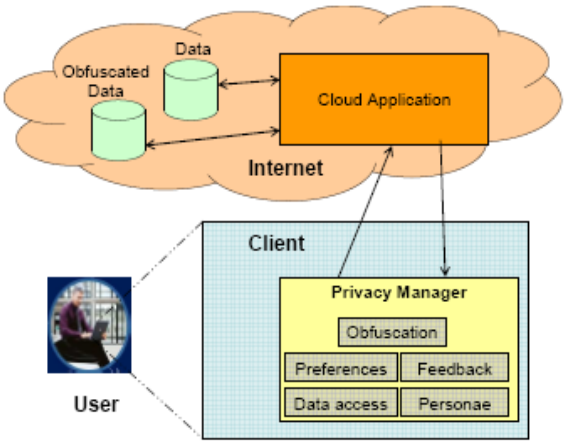

Figure 3. Overview of Privacy Manager

- **Obfuscation.** Privacy Manager provides obfuscation and de-obfuscation of data. This feature can automatically obfuscate some or all of the fields in a data structure before it is sent off to the cloud for processing, and translate the output from the cloud back into de-obfuscated form. The obfuscation and de-obfuscation is done using a key which is chosen by the user and not revealed to cloud service providers. This feature meets the data minimization requirement (**R1**) of privacy legislation.
- **Preference setting.** This is a method for allowing users to set their preferences about the handling of personal data that is stored in an un-obfuscated form within the cloud. Unlike the obfuscation feature, this feature is only useful if there is a corresponding policy enforcement mechanism within the cloud. This feature along with its server side components addresses Purpose limitation requirement (**R3**) of privacy legislation. This feature allows the user greater control over the usage of his data, and the personae feature makes this more intuitive. Hence the design is user centric thus satisfying the requirement **R4** of privacy legislation.
- **Data Access.** The Privacy Manager contains a module that allows users to access personal information in the cloud, in order to see what is being held about them, and to check its accuracy. This is essentially an auditing mechanism which will detect privacy violations once they have happened, rather than a mechanism to prevent violations from happening in the first place. The service providers need to be able to make this information accessible to the user. This module enables, organizes and logs this access on the client machine.
- **Feedback.** The Feedback module manages and displays feedback to the user regarding usage of his personal information, including notification of data usage in the cloud. This module could monitor personal data that is transferred from the platform. This feature along with data access feature satisfies the feedback requirement (**R5**) of the privacy legislation.
- **Personae.** This feature allows the user to choose between multiple personae when interacting with cloud services. The user's choice of persona may drive the strength of obfuscation that is used.

This architecture assumes that access control, etc. will be deployed on the services side in order to protect any data stored within the cloud.

c) Typical Problems Solved by Privacy Manager

1. Sales force automation

- **Problem.** For the cloud services, the business uploads its sales data to databases on Salesforce.com's computers. Detailed sales data is generally **commercially** sensitive – businesses are not willing to share it with their competitors – and in many cases will also contain individual information about the customers who have made purchases, such as their email addresses and product preferences. The security threat in this scenario is the theft of sales data from the service provider's system, followed by possible resale to business competitors or identity thieves.
- **Solution.** Figure 4 shows the process of using a cloud service with obfuscation to find the address of the customer who has spent most on CoolWidgets. An enterprise sales rep wants to find the email address of the customer who has spent most on the CoolWidget product. His client runs Privacy Manager software, whose integrity is protected by a Trusted Platform Module. The obfuscation feature of the Privacy Manager obfuscates his query, and sends the result to a cloud-based application for sales force automation, running on the service

provider's hardware. The application consults the obfuscated sales database for the enterprise and sends back an answer. The answer is in obfuscated form: the software de-obfuscates it to reveal the required email address.

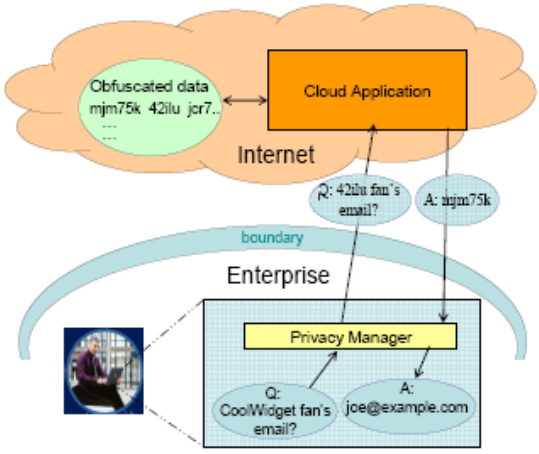

Figure 4. Using a cloud service with obfuscation to find the address of the customer who has spent most on CoolWidgets.

2. Customized End-User Services

Problem. Information may be automatically gathered about end-user context and user data in the cloud assessed, in order to provide targeted end user services.

The main threats in this type of scenario involve:

- Personal information about a user being collected, used, stored and/or propagated in a way that would not be in accordance with the wishes of this user.
- · People getting inappropriate or unauthorized access to personal data in the cloud by taking advantage of certain vulnerabilities, such as lack of access control enforcement, data being exposed 'in clear', policies being changeable by unauthorized entities, or uncontrolled and/or unprotected copies of data being spread within the cloud.
- Legal non-compliance. In particular, restrictions on trans-border data flow may apply, and also some of the data may be of types subject to additional regulations.

Solution. In this scenario, the user sets his preferences at to the treatment of personal data using the Preference setting feature of the privacy manager. The Privacy Manager can use this preference information to determine the appropriate degree of obfuscation to be carried out on the data.

The user's preferences are sent by the Privacy Manager on the client to a service-side component which governs enforcement of the policies. The service-side component ensures that these preferences remain attached to any personal information stored, used and shared in the cloud, and follow that data if it were transferred or propagated, preventing it being used in any way that is not compatible with that policy and thereby ensuring that the user has control over the usage of his data.

3. Share Portfolio Calculation

Problem. The application is the calculation of the current value of a user's share portfolio. The threat in this scenario is a leak of information about the user's share ownership from the service provider's system, followed by possible misuse.

Solution. For this scenario it is possible to use obfuscation to protect information about the user's share ownership from being misused. The client constructs two different portfolios such that the true portfolio is some linear combination of these. The client sends the two portfolios to the application separately, as the obfuscated input data. When the user wishes to know the current value of his portfolio, the client sends a request for the current value of each of the two of portfolios in the obfuscated data. It then combines the two answers from the cloud using the linear equation to obtain the current value of the user's portfolio.

The unobfuscated data describing the user's true portfolio is never present in the service provider's system. So it cannot leak from this system, even if the service provider is malicious.

d) When the solution is not applicable

A user with data x and a service provider with data y could use Yao's protocol for secure two-party computation to enable the user to learn $f(x,y)$ without the service provider learning x or the user learning y, where f is any polynomial-time functionality. The implementation of Yao's protocol on a large data set x in general may require the user to have a rather large amount of storage and computation power. For users with limited computing resources there is thus a tradeoff between the extent to which data is obfuscated and the set of applications that can effectively be used, even when the service provider gives full cooperation. If the service provider cooperates then the other features of Privacy Manager can still be used.

If the service provider does not provide full cooperation the features of the Privacy Manager other than obfuscation will not be effective, since they require the honest cooperation of the service provider.

The ability to use obfuscation without any cooperation from the service provider depends not only on the user having sufficient computing resources to carry out the obfuscation and deobfuscation, but also on the application having been implemented in such a way that it will work with obfuscation.

C. Transparent Cloud Protection System (TCPS)

The paper "Transparent Security for Cloud" [15] discusses the integrity protection problem in the clouds and sketches a novel architecture, Transparent Cloud Protection System (TCPS) for increased security of cloud resources.

a) Requirements

The core set of requirements to be met by a security monitoring system for clouds is the following

- **Effectiveness**: the system should be able to detect most kinds of attacks.

- **Guest Maintenance Tolerance**: the system should be able to (ideally) avoid false-positives.
- **Transparency**: the system should minimize visibility from VMs.
- **Immunity to attacks from the Guest**: the host system and the sibling guests should be protected from attacks proceeding from a compromised guest.
- **Deployability**: the system should be installable on the vast majority of available middleware.
- **Dynamic Reaction**: the system should detect an intrusion attempt over a guest and, if required by the security policy, take appropriate actions against the attempt or against the compromised guest and/or notify remote middleware security-management components.

b) The Transparent Cloud Protection System (TCPS)

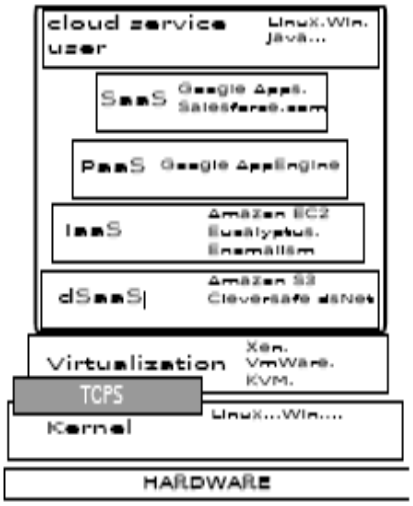

Figure 5: Cloud layers and Examples

Figure 5 shows the various cloud layers. The Transparent Cloud Protection System (TCPS) is a middleware whose core is located between the Kernel and the virtualization layer. TCPS is intended to protect the integrity of guest VMs and of the distributed computing middleware by allowing the host to monitor guest VMs and infrastructure components.

TCPS Architecture: Figure 6 shows the architecture of TCPS. TCPS is a protection system for clouds aimed at transparently monitoring the integrity of cloud components. TCPS is transparent to guest machines: it is hard to attack even from a compromised or untrusted VM and can inspect guest status and data. In Transparent Cloud Protection System (TCPS), a middleware whose core is located between the Kernel and the virtualization layer is intended to protect the integrity of guest VMs and of the distributed computing middleware by allowing the host to monitor guest VMs and infrastructure components. TCPS is a pure host side architecture and this allows deploying unmodified guest virtual appliances. Key components that would be affected by attacks are monitored to protect VMs and cloud infrastructure [29]. By either actively or passively monitoring such key kernel and cloud components any possible modification to kernel data and code can be detected, thus guaranteeing that kernel and cloud middleware integrity has not been compromised and consequently no attacker has made its way into the system. To monitor accesses to cloud entry points the integrity of cloud components can be checked via periodic checksum.

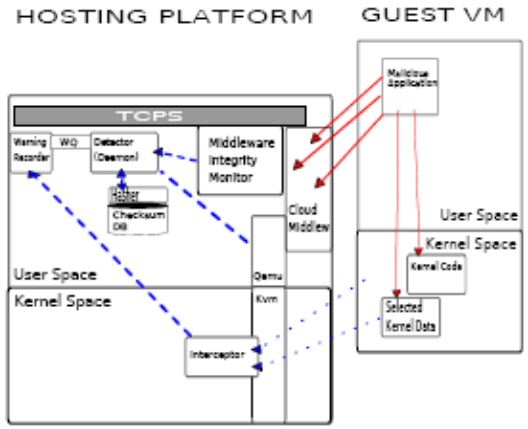

Figure 6: TCPS Architecture Continuous lines: potentially dangerous data flows Dashed lines: monitoring data flows

All TCPS modules reside on the Host and Qemu is leveraged to access the guest. Suspicious guest activity can be noticed by the Interceptor and they are recorded by the Warning Recorder into the Warning Queue where the potential alteration will be evaluated by the Detector component. TCPS can locally react to security breaches or notify the distributed computing security components of such an occurrence. In order to avoid false positives as much as possible, an administrator can notify TCPS of the new components' checksum.

Advantages: TCPS can be tailored to different cloud middleware implementations and can monitor cloud components integrity. This allows increased protection from most kind of attacks in a way that is completely transparent to guest VMs.

D. Secure and Efficient Access to Outsourced Data

The paper “Secure and Efficient Access to Outsourced Data” [10] proposes a mechanism to solve the problem of providing secure and efficient access to large scale outsourced data in owner-write-users-read applications. This method uses over-encryption and/or lazy revocation to prevent revoked users from getting access to updated data blocks. This mechanism handles both updates to outsourced data and changes in user access rights.

a) Problem Definition

Application Scenario and Basic Assumptions. The data owner stores a large amount of information on the service provider. Since the service provider is untrusted, the owner will encrypt the outsourced data before putting them on the server. To provide fine-grained access control, the encryption will be conducted at the block level. Only the owner can make updates to the outsourced data. Here the operations include updates to data blocks, and deletion, insertion, and appending of blocks. The outsourced data can

be accessed by many different end users that are distributed all over the network. Computationally expensive operations on the data blocks should be avoided and also the amount of information that is stored on the end users must be reduced. The access rights of the end users are different and they may change (grant and revocation) as time proceeds. Therefore, right keys must be provided to the end users to control their access.

An end user will send a data access request to the owner. The owner will refer to its access control matrix and send back corresponding encryption keys through the secure channel between them. At the same time, the owner will send back a data access certificate to the end user. The user will then present the certificate to the service provider. The provider will verify it and send the corresponding encrypted data blocks to the end user.

More Assumptions

- The smallest information access unit is called a `block'.
- There exist pre-distributed secrets between data owner and service provider, and between data owner and end-users.
- The service provider adopts a curious but not malicious model. That means, the provider will not intentionally send wrong data blocks to an end user but it will try to get access to the plaintext of the stored information.

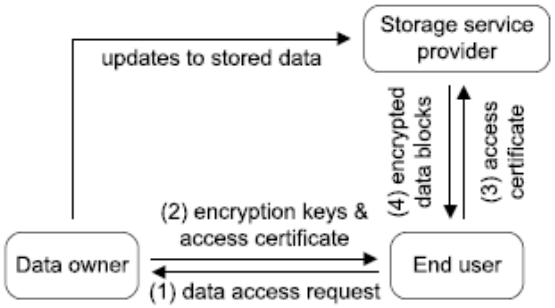

Figure 7. Illustration of Application Scenario

System Requirements:

- The outsourced data could be huge and the service provider may charge the owner based on used space.
- In addition to providing the storage space, the service provider may or may not offer the service of over-encryption when it sends the data blocks to end users.
- Since the service provider may have a pay-per-use pricing policy, the data owner should reduce the number of information accesses to the service provider when they are not caused by updates to data block
- Reduce the storage, communication, and computation overhead on the data owner and end users to promote the wide adoption of the proposed approach.

b) Secure and efficient data access

Determining keys for data encryption: An efficient mechanism must be designed to allow data owner and end users to manage the encryption keys. The key derivation method is being chosen. This method generates the data block encryption keys through a hierarchy. Every key in the hierarchy can be derived by combining its parent node and some public information. Since the derivation procedure uses a one-way function, the secret keys of the parent node and the sibling nodes cannot be calculated. Hence the data owner will need to maintain only the root nodes of the hierarchies. During the key distribution procedure, the owner can send the secrets in the hierarchy to end users based on their access rights. The end user will derive the leaf nodes in the hierarchy to decrypt the data blocks. The cost of this approach is the calculation of one-way functions during key derivation. Figure 8 shows the key derivation hierarchy.

There are various issues that need attention.

- When choosing the height of the hierarchy, there should be some room for the insertion and appending operations to the outsourced data.
- Encryption keys of the blocks that are temporarily missing from the outsourced data should not be disclosed.

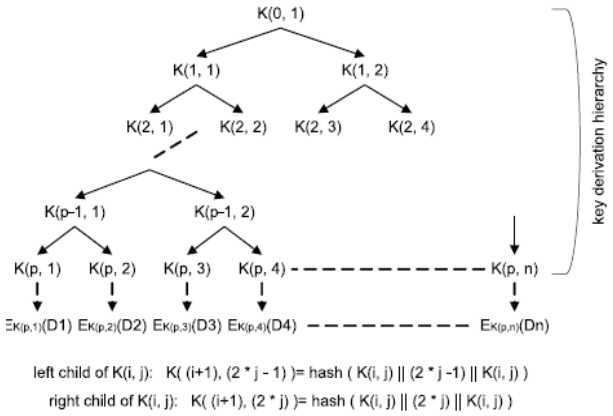

Figure 8. Key Derivation Hierarchy

Data Access Procedure:

Symbols used in the procedure

- *O*: data owner
- *S*: service provider
- *U*: end user.
- *kOU* and *kOS* : pair wise keys shared by *O* with U and S respectively.

Procedure:

1. *U* will send a data access request to *O*.

U -> O: {*U, O,* E_{Kou}, (*U, O, request index, data block indexes, MAC code*)}

The request index will be increased by 1 every time *U* sends out a request and it is used by *O* to defend against

replay attacks. The request contains the index numbers of the data blocks that *U* wants to access. The Message Authentication Code (MAC) will protect the integrity of the packet.

2. When *O* receives this message, it will authenticate the sender and verify the integrity and freshness of the request.

It will then examine its access control matrix and make sure that *U* is authorized to read all blocks in the request. If the request passes this check, the owner will determine the smallest set of keys K' in the hierarchy such that (1) K' can derive the keys that are used to encrypt the requested data blocks; and (2) *U* is authorized to know all keys that can be derived from K'. K' can be determined by a greedy algorithm and we ignore its details here.

The owner will then generate the reply to the end user.

O-> U: { *U, O,* E_{Kou}, (*O, U, request index, ACM index, seed for P(),* K'*, cert for S, MAC code*)}

Here the request index is used to uniquely label this reply. The ACM index is used by *O* to label the freshness of the Access Control Matrix (ACM). This index will be increased by 1 every time *O* changes some end user's access rights.

The updated ACM index will be sent to *S* by *O* to prevent those revoked users from using old certificates to access data blocks. The seed is a random number to initiate *P*() so that *U* can decrypt the over-encryption conducted by *S*. *U* will use K' to derive the data block encryption keys. The cert in the packet is a certificate for the service provider and it has the following format:

{E_{Kos}, (*U, request index, ACM index, seed, indexes of data blocks, MAC code*)}

3. The user U will send {*U, S, request index, cert*} to the service provider. When S receives this packet, it can verify that *O* generates the *cert,* since only they know the secret kOS. *S* will make sure that the user name and request index in cert match the values in the packet. If the ACM index in cert is smaller than the value that S receives from *O*, some changes to the access control matrix have happened and *S* will notify *U* to get a new cert. Otherwise, the service provider will retrieve the encrypted data blocks and conduct the over-encryption as follows. Using seed as the initial state of *P*(), the function will generate a long sequence of pseudo random bits. S will use this bit sequence as one-time pad and conduct the *xor* operation to the encrypted blocks. The computation results will then be sent to *U*.

4. When *U* receives the data blocks, it will use seed to generate the pseudo random bit sequence and use K' to derive the encryption keys. It will then recover the data blocks.

Advantages:

- Reduces the overhead of the data owner
- Prevent revoked users from getting access to the outsourced data

c) Handling Dynamics in System

Dynamics in user Access Rights:

- **Grant Access Right.** When an end user U is authorized to read a data block Di, the owner will change its access control matrix and increase the value of ACM index. The next time that U submits a data access request, the owner will recalculate the key set**.** K' based on the new access rights. The service provider and the end user do not need to change to adapt to this update.
- **Revoke Access Right.** When the access right to data blocks Di of the user U is revoked, the access control matrix in O will be updated and the ACM index increased. At the same time, O will label this data block to show that some user's access right has been revoked since its last content update. Before Di is updated for the next time, the owner will not change the block on the outsourced storage. When the owner needs to change the data block from Di to D'i, it will check the label and find that some user's access right has been revoked. Therefore, it cannot encrypt the updated data block with the current key. To solve this problem, the owner will encrypt a control block with the secret kp,i and put it at the slot for Di. The control block will contain a pointer to another block in which the updated data is stored. It will also contain enough information for the owner to derive the new encryption key. The owner will derive the new key and send it back to the user. At the same time, a new cert will be generated so that the user can get the new block from the service provider. A revoked user will be able to get access to the control block.

Dynamics in Outsourced Data:

- **Block Deletion.** When a data block Di is deleted from the outsourced data, the owner will use a special control block to replace Di. The special block will be encrypted by kp,i and stored at the original slot for Di on the service provider. At the same time, the owner will label its access control matrix to show that the block no longer exists. The end users can still access this control block but they will not get any useful information from the contents.
- **Block Update.** If no user's access right to this data block has been revoked since its last update, the owner can update its value in the current storage place. The owner will first locate the slot in which Di is currently stored and derive its encryption key. It will then use the key to encrypt D'i and write the new value to the storage place. The end users will not be impacted by this operation and they will automatically get the new data when they access the block.

If some user's access right to Di has been revoked since its last update and the service provider refuses to conduct

over- encryption during data transmission, we cannot encrypt the new block D'i with the current key. On the contrary, we will encrypt a control block with kp,i and write it to the i-th block of the outsourced data. The control block will contain the following information: (1) a pointer to the data block in which D'i is currently stored; (2) information used by the data owner to derive the encryption key of D'i ; (3) information used by the data owner to verify the integrity of the control block. The owner will also use the new secret to encrypt D0i and write it to the corresponding place in S.

When a user needs to access D'i, it will get the encrypted control block from the service provider and submit it to the owner. The owner will verify the authenticity and integrity of the control block and derive the current encryption key. It will then return the key with a cert to the user through a secure channel so that the user can access D'i from S. A revoked user can get the control block but it will not get the new encryption key and the cert.

- **Block insertion and Appending.** The data owner may need to generate new information and put it on the outsourced storage. Here we do not intentionally distinguish insertion from appending and follow the same procedure to handle the two operations. The data owner will locate an unused block index, derive the encryption key in the hierarchy using $k_{0,1}$, encrypt the data block, and store it on the service provider.

Advantages:

- Data access procedure reduces the overhead of the data owner and prevents the revoked users from getting access to the outsourced data.
- This approach is robust against collusive attacks if the hash function is safe.
- Over-encryption conducted by the service provider defends against eavesdroppers even when they have the data block encryption keys.
- This approach has less communication and overhead for data retrieval when they have infrequent update operations.
- This approach handles user revocation without impacting service provider.

Disadvantages:

- This approach is applicable only for owner-write-users-read applications and hence not generic.
- There is a lengthened data retrieval delay caused by the access to updated data blocks.

Security of the Approach:

- The adversaries have to have a non-negligible advantage in breaking the hash function to accomplish this task. Therefore, the proposed approach is robust against collusive attacks if the hash function is considered safe.
- To defend against the replay attack, the data owner must verify the freshness of the control block.
- Over-encryption conducted by the service provider can defend against eavesdroppers even when they have the data block encryption keys.

E. Securing Elastic Applications on Mobile Devices for Cloud Computing

The paper "Securing Elastic Applications on Mobile Devices for Cloud Computing" [16] gives an overview of how elastic applications work and some features of the elasticity framework, and focus on the security issues in designing elastic applications.

a) Overview of elastic application for mobile devices:

Figure 9 shows the overview of elastic application for mobile device. An elastic application can consist of one or more weblets, which function independently, but communicate with each other. When the application is launched, an elasticity manager running on the device monitors the resource requirements of the weblets of the application, and make decisions where they should be launched.

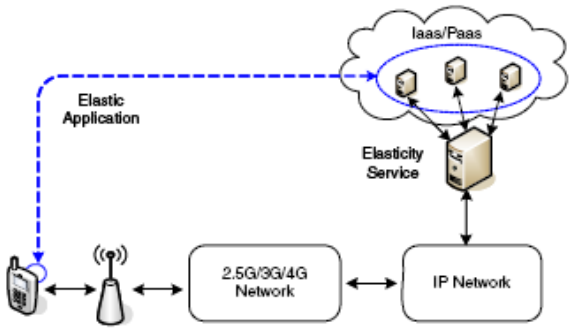

Figure 9. Overview of elastic application for mobile device.

If one weblet should be launched on the cloud, the elasticity manager talks to elasticity service residing on the cloud, which arranges the execution resources of the weblet. The service also returns some information after successfully launching the weblet, such as its endpoint URL. The elasticity manager can also make decisions about migrating running weblets from the device to cloud or from cloud to device, according to changes in computing constraints on the device or changes in user preferences. During execution, the weblets of a single application can communicate with each other, with an RPC mechanism or RESTful web services. The elasticity service organizes cloud resources and delegates application requirements from mobile devices.

Challenges:

- A new application model is needed in order to launch or migrate some parts of an application in the cloud and others on the device. The new application model should support applications partitioned into multiple components, each of which can run autonomously from the others.
- An appropriate protocol is needed between weblets during runtime

- A set of cost objective functions are needed, which should be optimized when elastic scheduling decisions are made
- Security and privacy are important factors when considering some sensitive weblets and data migrating from device to cloud.

b) Elastic Applications for Mobile Platform

Concept and Benefits: The objective of an elastic application is to dynamically leverage cloud computing for resource-constrained mobile devices. An elastic device should have the ability to migrate functionality between the device and cloud. This ability allows the device to adapt to different work loads, performance goals, and network latencies.

Benefits:

- Elastic applications need not be constrained by the current compute capabilities of mobile devices. If more compute (or storage) is needed then this can be obtained from the cloud. As devices become more powerful, compute and storage can shift back to the device
- Device resources can be modest since the more demanding applications can acquire resources from the cloud.
- The ability to allocate resources in the cloud and migrate functionality gives the device great flexibility.
- Application components that are partitioned for migration can also be replicated. The failure then of one instance of a replicated component need not compromise the application [37].

Elastic Framework Architecture:

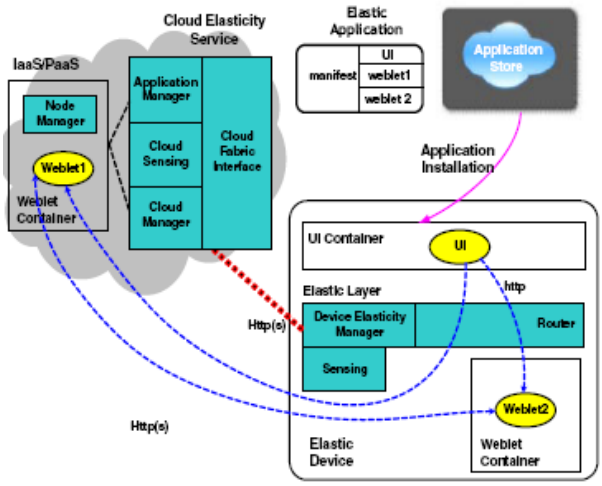

Figure 10: Elastic framework architecture

Figure 10 shows the architecture of an elastic framework.

- **Device Elasticity Manager (DEM):** DEM is responsible for configuring applications at launch time and making configuration changes during run time. The elasticity manager maintains a cost model which accounts the various monetary costs. The elasticity manager runs an optimizer which is responsible for determining the best application configuration given costs and user goals. The router passes requests from UI components to weblets. It insulates the UI logic from weblet location. The sensing data of each device is made available to the elasticity manager and is used by the cost model.
- **Cloud elasticity service (CES):** CES consists of cloud manager, application manager, and sensing information collection. Cloud manager which maintains the usage information is responsible for allocating resources from, and releasing to, the underlying cloud platform. The application manager provides functions to install and maintain applications on behalf of elastic devices, and helps to launch weblets in different cloud nodes. CES provides a web service, referred to as the cloud fabric interface (CFI) to elastic devices and applications.
- **Node manager:** A node manager on each node oversees resources associated with a particular node (server) within the cloud. It communicates directly with the cloud manager and application manager. Each node runs one or more weblet containers which are the weblet runtime environments hosted on the cloud platform.

Elastic Application Model:

- **Partitions of an elastic application:** Each application should be partitioned into components called weblets.
- **Data dependency of weblets:** An elastic application should allow reasonable data dependency between weblets of the same application or different applications.
- **Communication protocols between weblets:** As an elastic application is naturally distributed between the cloud platform and a mobile device, weblets should communicate with each other.

c) Security Assumptions, Threats and Requirements

Security Assumptions:

- As part of the elastic framework the elasticity manager on each device is trusted.
- CES is trusted including cloud manager, application manager, cloud node manager, and CFI.

Threat Model:

There various types of threats are:

1. **Threats to Mobile Devices:** Malware targeting mobile devices have become prevalent. Some of the attack include:

- Attacks on integrity and confidentiality of application code and user data on a device

- drain power on the device by changing the configuration of an application
- Attack on device's sensing components could cause the DEM to manage weblets based on incorrect data.
- Malware could bypass the elasticity manager and launch weblets on cloud platforms on behalf of the user, which would be billed to the user's account.

2. **Threats to Cloud Platform and Application Container:**

- Malicious entities can change network and cost settings, or even cloud sensing information to confuse the CES into making decisions such as using overly expensive network connections to devices.
- Consume resources of cloud platform could lead to degradation of performance and network bandwidth of the cloud platform and generate hidden bills to the application user.

3. **Threats to Communication Channels [45]**

- Attacker can sit in the middle of the network and generate tremendous network traffic to both sides
- DDoS attacks can not only exhaust bandwidth resources, but also result in excessive charges to user accounts or disable them if they exceed their quotas.

Security Objectives:

- **Trustworthy weblet containers (or VMs) on both device and cloud:** Weblets must be installed and execute in trusted runtime environments in all locations. The elasticity manager on both the cloud and device should have some assurance that the weblet's execution environment can adequately protect its expected functionalities.
- **Authentication and secure session management:** The elastic framework should provide a mechanism to authenticate weblets belonging to the same application and user to each other. This is especially important when they are running on different platforms
- **Authorization and access control:** A weblet on the cloud should adhere to the property of least privileges.
- **Logging and auditing:** Behaviors of weblets should be logged and audited routinely to prevent malicious activities.

d) Authentication and Secure Session Management

Secure Installation of Elastic Applications: When a user downloads and installs an application, the integrity of all weblets are verified by the installer of the elastic device by re-computing and comparing their hashes and with those in the bundle.

After successful integrity verification, the installer registers the application with the DEM. The DEM maintains a table of installed applications on the device which need elasticity manager support, each with detailed information of weblets. Parts of the elastic application can be installed by the application manager into the CES. To do this, the user has to register and authenticate with the CES during installation. The cloud-based application manager also can download the same application from an application store instead of uploading from the device.

Building Authentication between Weblets:

- Whenever an elastic application wants to launch a weblet, it first connects to the DEM, which decides where to launch the weblet.
- DEM generates a pair of weblet session keys (wsk) and a secret (wss) for the application if this is the first weblet to be launched. These are shared by all weblets during a single session.
- When DEM decides to launch a weblet in local device, it executes the installed weblet binary with LaunchWeblet (localhost,wid,wss,wsk). Upon invoking, the weblet construction method records wid, wsk, and wss into its member variables. Also, the weblet returns a valid URL endpoint which is used to communicate with other weblets with http(s). DEM then updates a weblet table which records the active weblet's URL, wid, and wsk.
- If DEM decides to launch a weblet in a cloud, it calls the CFI's web method LaunchWeblet(cfi,wid,wsk,wss).
- Based on its service logic, the CFI queries its cloud manger and decides on which cloud node the weblet will be loaded. Once this is decided, CFI call the target node manager's LaunchWeblet(nodeid, wid, wsk,wss), again with https as it goes via public Internet.
- The node manager executes weblet binaries provided by the application manager of the CES. A code transportation mechanism is needed between the node manager and CES. The successfully launched weblet returns a valid URL endpoint to the node manager, which in turn is passed back to CFI and DEM. DEM updates the weblet table with returned result. Before updating, DEM verifies if the WebletOK message is generated by the launched weblet, by checking the HMAC value with wss.
- A local weblet can query DEM to obtain the list of all active weblets in the same session by call DEM::GetWeblet(wsk). DEM returns the URLs of all weblets by querying the table.
- The local weblet can broadcast the URLs to any other weblet that needs to communicate.

Security Analysis:

- Only weblets and the DEM know about wss, which reduces the risk of a compromised CES and node managers using the secret

- Communication between weblets are authenticated by the shared secret, and identified by the session token

Secure Migration:

- Usually a migration request is triggered by the DEM.
- Upon this request, the weblet enters a migration state and saves its current running state including its session secret
- Weblet returns to DEM.
- The DEM then sends the migration request to the CFI.
- CFI then decides where the weblet should be migrated, by either picking one cloud node in an available node pool or creating a new node.
- Node Manager launches new weblet with the state of migrating weblet from device.
- To make this migrated weblet visible to other weblets, the node manager updates its new URL to the routing table on the device after successful migration, and the migrated weblet broadcasts its new URL to other weblets by querying the DEM.

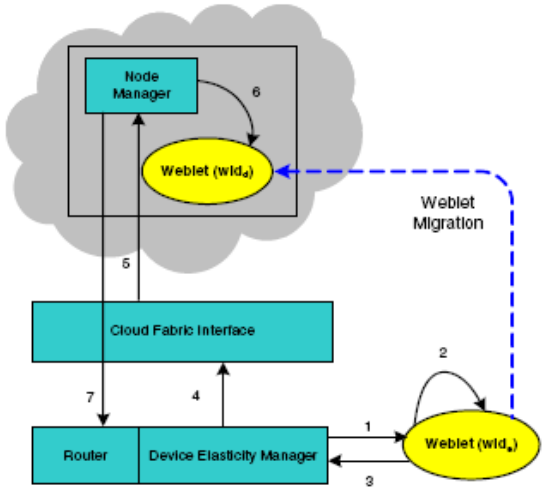

Figure 11 Secure weblet migration from device to cloud

e) Authorization of Weblets.

Various approaches:

1. Shared user credentials: Each weblet has user credentials such as username and password or digital certificate of the web service.

A method can be implemented by weblets to retrieve this via the UI component.

Disadvantage: A hostile environment on cloud node can save the user credentials and impersonate the user later.

2. Shared session information: After a device weblet authenticates with the web server, it shares ask and ass with other weblets. A method can be implemented by the weblet class to share or broadcast secret.

Advantage: The session secret is only valid for a short time period after authentication and hence safer than the previous approach.

3. Use session information only on device weblet: Whenever a cloud weblet needs access to user data on external web services, it forwards the requests to the authenticated device weblet, which has ask and ass

Advantage: This approach enhances the security as session information is only available on the device.

Disadvantage: Multiple re-directions are needed in this approach, thereby introducing communication overhead to the device.

4. OAuth-like authentication: When the cloud weblet accesses the web service, it generates an authentication challenge on behalf of the user and redirects any responded authentication URL to the UI or device weblet. When the web server authenticates the user successfully, the UI or device weblet re-directs the resulting session information to the original requesting cloud weblet.

Advantage: Fine-grained authorization is supported.

Disadvantage: Extra authorization management should be considered in application logic, thus more burden for application developers.

F. DDoS Defense in Cloud Computing

Lacking trust between service providers and cloud users has hindered the universal acceptance of cloud computing as a service on demand. In the past, trust models have been developed to protect mainly e-commerce and on-line shopping provided by eBay and Amazon. For web and cloud services, trust and security become even more demanding, because leaving user applications completely to the cloud providers has faced strong resistance by most PC and server users. Cloud platforms become worrisome to some users for lack of privacy protection, security assurance, and copyright protection. Trust is a social problem, not a pure technical issue. However, the social problem can be solved with a technical approach.

We desire a healthy cloud ecosystem that is free from abuses, violence, cheating, hacking, viruses, rumors, pornography, spasm, privacy and copyright violations. We assess the security demands of three cloud service models: IaaS, PaaS, and SaaS that have used in cloud practices. These models are based on various *service level agreements* (SLAs) between providers and users.

There're mainly three basic cloud security enforcements. Firstly, facility security in datacenters demands on-side security all year round. Biometric readers, CCTV (close-circuit TV), motion detection, and man traps are often deployed. Secondly, network security demands fault-tolerant external firewalls, intrusion detection systems, and third-party vulnerability assessment. Thirdly, platform security demands SSL and data decryption, strict password policies, system trust certification, etc. Servers in the cloud can be physical machines or virtual machines. User interfaces are applied to request services. The provisioning tool carves out the systems from the cloud to satisfy the requested service. A security-aware cloud architecture demands security enforcement. Malware-based attacks like

worms, viruses and DDoS exploit the system vulnerabilities. These attacks compromise the system functionalities or provide the intruders an unauthorized access to critical information. Thus, security defense is needed to protect all cluster servers and datacenters.

Listed below are some cloud components that demand special security protection [51]:

- Protection of servers from malicious software attacks like worms, viruses, and malwares.
- Protection of hypervisors or VM monitors from software based attacks and vulnerabilities.
- Protection of VMs and monitors from service disruption and denial of service attacks.
- Protection of data and information from theft, corruption and natural disasters.
- Providing authenticated and authorized access to critical data and services.

A case study is Amazon Web Services (AWS) Elastic Compute Cloud (EC2). Amazon acknowledges that maintaining security and privacy in a cloud environment is more complex than when managing a single datacenter. Table 1 identifies 6 of our 20 security recommendations that Amazon has incorporated into their security models.

"A 50 megabit/sec attack used to be a big deal. Now we're seeing 84 gigabits of sustained traffic. No enterprise on the planet can withstand the bandwidth capability for that attack," Petro says. "If you have a 10 megabit pipe, and you receive a 10.1 megabit attack, you're done. That's why DDoS has to be mitigated in the cloud." The survey found that DDoS attacks accounted for 33% of website downtime. Perhaps not surprisingly, more than two-thirds of respondents said their downtime impacted customers and half reported lost revenue as a result [55].

Therefore, a DDoS defense system must be designed to cover multiple network domains spanned by a given cloud platform. These network domains cover the edge networks where the protected cloud resources are physically connected. DDoS attacks come with widespread worms. The flooding traffic is large enough to crash the victim server by buffer overflow, disk exhaustion, or connection saturation, etc. Figure 12 (a) shows a flooding attack pattern launched from 4 zombies towards a victim server attached at the bottom router R0. The flooding traffic flows essentially form a tree pattern as shown in Figure 12 (b). Successive attack-transit routers along the tree detect the abnormal surge of traffic at their I/O ports. This DDoS defense system is based on change-point detection along all attack-transit routers. The defense scheme works across multiple network domains.

In a DDoS flooding attack, the attacker often recruits many zombies over the Internet. The flooding traffic flows through multiple AS (autonomous system) domains before reaching the edge network where the victim machine is attached. Routers at the upstream domains observe the suspicious traffic flows ahead of routers at the downstream domains. Figure 13 illustrates an example network covering six AS domains. The victim server is located in the AS1 domain. Zombies are scattered widely in the Internet. By detecting abnormal traffic changes, the detection server at each domain creates a traffic flow subtree locally.

TABLE 1 AWS SECURITY FEATURES ALIGNMENT WITH CLOUD SECURITY RECOMMENDATIONS [54]

Recommendation	Amazon implementation
Do not implicitly trust the cloud or any instances in the cloud; every interaction in the cloud demands authorization and authentication	Every AWS interaction requires a "signed" API call.
Virtually "shred" retired instances and data when no longer needed	When customer storage is no longer used, every block of data is automatically wiped. AWS also uses a proprietary disk virtualization layer to ensure customer data remains private when virtual disk blocks are returned to resource pool.
Utilize a single management, logging, and monitoring system capable of supporting the entire cloud	AWS utilizes bastion hosts for cloud management
Restrict console access (physical and virtual) to users with a defined business need	Administrative access, both physical and virtual, is strictly controlled according to legitimate business requirements. Those access privileges are immediately revoked when an employee no longer has a need for access. Each administrator is assigned unique cryptographically strong SSH keys. Access to bastion hosts is logged and audited on a regular basis.
Provide centralized authentication and authorization services	AWS utilizes bastion hosts for cloud management.
Digitally sign control messages within the cloud in order to prevent tampering and unauthorized use	Customers are issued a unique key. This key, or an authorized X.509 certificate, must be used to sign all Amazon EC2 API calls. Signing API calls ensures that control messages within the cloud are authorized and prevents tampering. API calls in transit are encrypted with SSL.

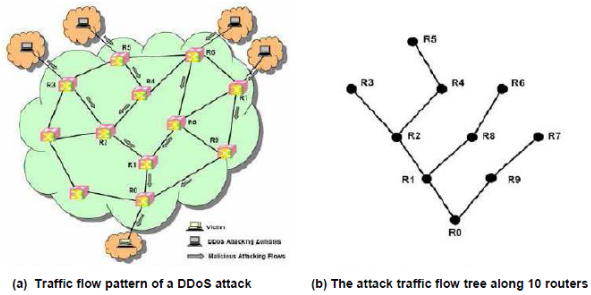

Figure 12 DDoS attacks and defense by change-point detection at all routers on the flooding tree [52].

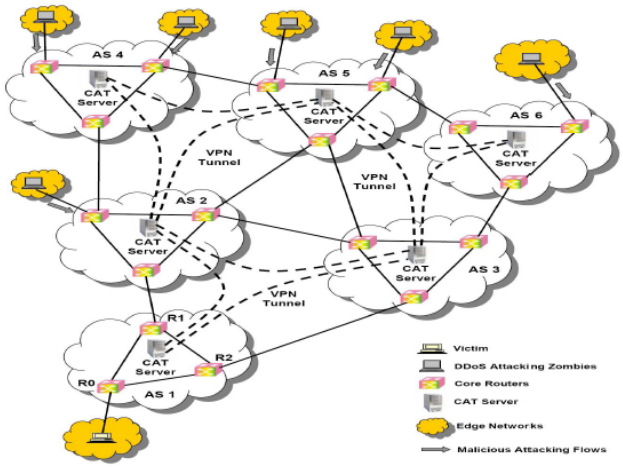

Figure 13 Distributed defense against DDoS attacks over multiple network domains [53].

Multiple traffic subtrees are merged to form the global traffic flow tree. Once the global tree is detected at the end router, all servers in the covered domains will be alerted with the eminent DDoS attacks. The Packet dropping could stop attack from the suspected upstream routers beamed towards the victim.

To sum up, the above defense system detects abnormal traffic changes at attack-transit routers. Based on the anomaly pattern detected in covered network domains, the scheme detects a DDoS attack before the victim is overwhelmed. The detection scheme is suitable for deployment at the cloud provider core networks. The provider-level cooperation eliminates the need of intervention by edge networks. Experimental results reported in [53] prove that 4 to 8 domains are sufficient to yield a 98% detection success rate of TCP SYN and UDP flooding attacks. Based on Internet AS domain distribution, the defense scheme can scale well to protect almost one hundred AS domains in a real-life Internet environment.

VeriSign [56] has added an extra layer of security to the Internet's .com domain, but e-retailers, banks and other Web site operators will need to upgrade their DNS hardware, software or services to take advantage of .com's new cryptographic features. Verisign is expanding its cloud-based DDoS protection service to cover small and midsize businesses that are increasingly frequent targets. Until now, Verisign has been offering a high-end DDoS protection service to major financial services firms. Now, Verisign is taking that same set of home-grown DDoS detection and mitigation tools to a broader market.

Soon Hin Khor et al. [57] proposed DaaS, which is a service that protects a server against all 3 types of Distributed Denial-of-Service (DDoS), arbitrary packet, legit user-mimicking and economic attacks. For arbitrary packet DDoS defense, DaaS's framework facilitates harness of intermediaries that relay traffic to a server so that their total resource exceeds those of DDoS bots. For legit user-mimicking DDoS defense, DaaS's unique self-verifying Proof-of-Work (sPoW) empowers a sender to compete with bots by solving a more difficult sPoW puzzle to discover a more obscure "ephemeral" intermediary channel that has been designated to relay a single connection to its desired destination. For economic DDoS (eDDoS) defense, obscure ephemeral channels force bots to continuously expend resource to discover them before the bots can trigger channel utilization billing. Although neither intermediaries nor PoW is new, DaaS represents a leap forward for mainly two reasons. First, DaaS framework tackles the incentive issue of harnessing intermediary resource to a volume sufficient for arbitrary packet DDoS defense, an issue ignored by existing work. Second, sPoW protects against eDDoS, which conventional PoWs cannot, servers are billed, in principle, for only legitimate traffic relayed with bot traffic quietly discarded.

In the paper [58], it explains how maneuver IT virtualization strategy could be used in responding to a denial of service attack. After picking up a grossly abnormal spike in inbound traffic, targeted applications could be immediately transferred to virtual machines hosted in another data center.

Elastic cloud computing is an attractive proposition, such as Amazon EC2, which offers convenience in setup, on-demand capacity and a highly dependable computing platform with little maintenance requirement. However, a DDoS can rack up a cloud adopter's utilization bill resulting in an economic DDoS (eDDoS)—a debilitating bill incurred by using highly elastic capacity to unwittingly serve a large amount of undesired traffic [59]. sPoW explores how to cobble an on-demand network and application-level eDDoS mitigation mechanism using existing cloud(s) to protect servers in clouds against eDDoS or even DDoS in general. Since cloud-based eDDoS mitigation mechanism itself, is susceptible to eDDoS, it is imperative to drop eDDoS traffic before it triggers the billing mechanism. In the paper [59], Soon Hin Khor et al. proposed two key ideas. The first one is that transform network level eDDoS into traffic that can be distinguished and filtered using basic packet pattern matching. The second one is that prioritize legitimate looking traffic, which is a mix of legitimate and application level DDoS traffic using capabilities and our self-verifying Proof of-Work (sPoW) scheme. The first one rids network-level eDDoS before the billing perimeter, and the latter one reduces the number of application-level eDDoS connection requests thereby minimizing the portion of server utilization incurred by eDDoS but at the expense of protracted connection establishment time for legitimate clients. Neither proposed features, requires special technology on existing cloud platforms, make them deployable now.

V. OPEN RESEARCH PROBLEMS AND CHALLENGES

This section explains some other threats that are discovered in the Cloud Computing Journal "A security analysis of Cloud Computing" [5].

- **Failures in Provider Security.** In a cloud environment, all security depends on the security of the cloud provider. They control the hardware and the hypervisors on which data is stored and applications are run. Cloud provider security must be top-of-the-line.

- **Attacks by Other Customers.** The cloud environment is shared among customers. If the barriers between customers break down, one customer can access another customer's data or interfere with their applications.
- **Availability and Reliability Issues.** Cloud data centers are generally as reliable as enterprise data centers or more so. However, outages do occur. Also, the cloud is only usable through the Internet so Internet reliability and availability is essential.
- **Legal and Regulatory Issues.** The virtual, international nature of cloud computing raises many legal and regulatory issues. First, export of data out of a jurisdiction may be restricted. If such export is permitted, which jurisdiction's rules apply in case of conflict? And who is liable for errors such as security breaches? These issues must be addressed for any sensitive applications of cloud computing.
- **Perimeter Security Model Broken.** Many organizations use a perimeter security model with strong security at the perimeter of the enterprise network. This model has been weakening over the years with outsourcing and a highly mobile workforce. Cloud computing strikes its death knell. The cloud is certainly outside the perimeter of enterprise control but it will now store critical data and applications.
- **Integrating Provider and Customer Security Systems.** Enterprises have spent decades developing a unified directory and other components of their security architecture: automated provisioning, incident detection and response, etc. Cloud providers must integrate with these systems or the bad old days of manual provisioning and uncoordinated response will return.

A. Fear of The Cloud

Security concerns are categorized as [14]:

- Traditional Security
- Availability
- Third-party data control

a) Traditional Security

These concerns involve computer and network intrusions or attacks that will be made possible or at least easier by moving to the cloud.

Concerns in this category include

- **VM-level attacks.** Potential vulnerabilities in the hypervisor or the VM technology used by the cloud vendors.
- **Cloud provider vulnerabilities**. These could be platform-level, such as an SQL-injection or cross-site scripting vulnerability in salesforce.com
- **Phishing cloud provider.** Phishers and other social engineers have a new attack vector.
- **Expanded network attack surface.** The cloud user must protect the infrastructure used to connect and interact with the cloud, a task complicated by the cloud being outside the firewall in many cases.
- **Authentication and Authorization.** The enterprise authentication and authorization framework does not naturally extend into the cloud.
- **Forensics in the cloud.**

b) Availability

These concerns center on critical applications and data being available.

Concerns in this category include

- **Uptime.** Besides just services and applications being down, this includes the concern that a third-party cloud would not scale well enough to handle certain applications.
- **Single point of failure.** Cloud services are thought of as providing more availability, but perhaps not – there are more single points of failure and attack [47].
- **Assurance of computational integrity.**

c) Third-party data control.

The legal implications of data and applications being held by a third party are complex and not well understood. There is also a potential lack of control and transparency when a third party holds the data. Concerns in this category include:

- **Due diligence**
- **Auditability.** Audit difficulty is another side effect of the lack of control in the cloud.
- **Contractual obligations.** One problem with using another company's infrastructure besides the uncertain alignment of interests is that there might be surprising legal implications.
- **Cloud Provider Espionage.** This is the worry of theft of company proprietary information by the cloud provider.
- **Data Lock-in.** The data might itself be locked in a proprietary format, and there are also issues with training and processes.
- **Transitive nature.** The contracted cloud provider might itself use subcontractors, over whom the cloud user has even less control, and who also must be trusted.

B. New Problems

This section explains some of the new problems areas in security that arise from cloud computing [14]

- **Cheap data and data analysis.** Because of cloud computing collection and analysis of data is now possible cheaply. Because of the cloud, attackers potentially have massive, centralized databases available for analysis and also the raw computing power to mine these databases. Because of privacy

concerns, enterprises running clouds collecting data have felt increasing pressure to anonymize their data.

- **Cost-effective defense of availability.** Availability also needs to be considered in the context of an adversary whose goals are simply to sabotage activities. Increasingly, such adversaries are becoming realistic as political conflict is taken onto the web. The cloud computing model encourages single points of failure. It is therefore important to develop methods for sustained availability, and for recovery from attack.
- **Increased authentication demands.** The development of cloud computing may, in the extreme, allow the use of thin clients on the client side. Thin clients result in a number of opportunities related to security; - their security is managed by the cloud, which maintains the software they run. The movement towards increased hosting of data and applications in the cloud and lesser reliance on specific user machines is likely to increase the threat of phishing and other abusive technologies aimed at stealing access credentials, or otherwise derive them.
- **Mash-up authorization.** As adoption of cloud computing grows, we are likely to see more and more services performing mash-ups of data. This development has potential security implications, both in terms of data leaks, and in terms of the number of sources of data a user may have to pull data from – this, in turn, places requirements on how access is authorized for reasons of usability.

VI. CONCLUSION

We explored a lot of research articles about the cloud computing, including the advantages of cloud computing, risks in cloud computing and various approaches to solve those risks each with their pros and cons. Each algorithm is aimed at solving a particular risk. However cloud computing is still struggling in its infancy, with positive and negative comments made on its possible implementation for a large-sized enterprise. IT technicians are spearheading the challenge and pursuing research to improve on its drawbacks. Several groups have recently been formed, such as the Cloud Security Alliance or the Open Cloud Consortium, with the goal of exploring the possibilities offered by cloud computing to establish a common language among different providers. Cloud computing is facing several issues in gaining recognition for its merits. Its security deficiencies and benefits need to be carefully weighed before we make a decision to implement it [4].

ACKNOWLEDGMENTS

In this paper, Naixue Xiong is the corresponding author.

REFERENCES

[1] S. Bennett, M. Bhuller, R. Covington, Oracle White Paper in Enterprise Architecture – Architectural Strategies for Cloud Computing. August 2009. DOI= http://www.oracle.com/technology/architect/entarch/pdf/architectural_strategies_for_cloud_computing.pdf.

[2] Microsoft. Azure Services Platform. DOI = http://www.microsoft.com/windowsazure/.

[3] net-security. org Top 7 threats to cloud computing. DOI= http://www.net-security.org/secworld.php?id=8943.

[4] T. Andrei, R. Jain, Cloud Computing Challenges and Related Security Issues. A Survey Paper. DOI = http://www.cse.wustl.edu/~jain/cse571-09/ftp/cloud.pdf.

[5] St. Hanna, A security analysis of Cloud Computing. Cloud Computing Journal. DOI = http://cloudcomputing.sys-con.com/node/1203943.

[6] J. Du, W. Wei, X. Gu, T. Yu, RunTest: Assuring Integrity of Dataflow Processing in Cloud Computing Infrastructures. ***ASIACCS'10:*** *Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security*, pages 293- 304, April 2010.

[7] S. C. Wang, K. Q. Yan, S. S. Wang, C. P. Huang, Achieving High Efficient Agreement with Malicious Faulty Nodes on a Cloud Computing Environment**.** *ICIS '09: Proceedings of the 2nd International Conference on Interaction Sciences: Information Technology, Culture and Human*, pages 468-473. November 2009.

[8] K. Sripanidkulchai, S. Sahu, Y. Ruan, A. Shaikh, C. Dorai, Are Clouds Ready for Large Distributed Applications? *SIGOPS Operating Systems Review, Volume 44 Issue 2*, pages 18-23. April 2010.

[9] S, Pearson, Taking Account of Privacy when Designing Cloud Computing Services. *CLOUD '09: Proceedings of the 2009 ICSE Workshop on Software Engineering Challenges of Cloud Computing*, pages 44-52. May 2009.

[10] W. Wang, Z. Li, R. Owens, B. Bhargava, Secure and Efficient Access to Outsourced Data. *CCSW '09: Proceedings of the 2009 ACM workshop on Cloud computing security*, pages 55-65. November 2009.

[11] M. Mowbray, S. Pearson, A Client-Based Privacy Manager for Cloud Computing**.** *COMSWARE '09: Proceedings of the Fourth International ICST Conference on COMmunication System softWAre and middleware*. June 2009.

[12] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, Randy Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, M. Zaharia, A view of cloud computing. *Communications of the ACM, Volume 53 Issue 4*, pages 50-58. April 2010.

[13] J. Wei, Xi. Zhang, G. Ammons, V. Bala, P. Ning, Managing security of virtual machine images in a cloud environment. *CCSW '09: Proceedings of the 2009 ACM workshop on Cloud computing security* pages 91-96. November 2009.

[14] R. Chow, P. Golle, M. Jakobsson, E. Shi, J. Staddon, R. Masuoka, J. Molina, Controlling Data in the Cloud

Outsourcing Computation without Outsourcing Control. *CCSW '09: Proceedings of the 2009 ACM workshop on Cloud computing security*, pages 85-90, November 2009.

[15] F. Lombardi, R. D. Pietro, Transparent Security for Cloud. *SAC '10: Proceedings of the 2010 ACM Symposium on Applied Computing*, pages 414-415, March 2010.

[16] X. Zhang, J. Schiffman, S. Gibbs, A. Kunjithapatham, S. Jeong, Securing Elastic Applications on Mobile Devices for Cloud Computing. *CCSW '09: Proceedings of the 2009 ACM workshop on Cloud computing security*, pages- 127-134. November 2009.

[17] Amazon, Amazon Elastic Compute Cloud (ec2), DOI = http://aws.amazon.com/ec2/.

[18] T. Ristenpart, E. Tromer, H. Shacham, S. Savage. Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds. *CCS '09: Proceedings of the 16th ACM conference on Computer and communications security*, pages: 199-212. November 2009.

[19] IBM- Cloud Computing. DOI = http://www.ibm.com/ibm/cloud/.

[20] Amazon. Amazon EC2, Developer Guide. DOI = http://docs.amazonwebservices.com/AWSEC2/latest/DeveloperGuide/.

[21] Security Guidance for Critical Areas of Focus in Cloud Computing, April 2009. DOI = http://www.cloudsecurityalliance.org/guidance/csaguide.pdf.

[22] Open Crowd. Open crowd cloud taxonomy. DOI = http://cloudtaxonomy.opencrowd.com/ . 2010.

[23] Arista, "Cloud Networking: Design Patterns for 'Cloud Centric' Application Environments", January 2009. DOI = http://www.aristanetworks.com/media/system/pdf/CloudCentricDesignPatterns.pdf. January 2009.

[24] Amazon CloudFront. DOI = http://aws.amazon.com/cloudfront/.

[25] R. Gellman, Privacy in the clouds: Risks to privacy and confidentiality from cloud computing. Tech. rep., February 2009. DOI = http://www.worldprivacyforum.org/.

[26] Google App Engine. DOI = http://appengine.google.com/.

[27] N. Santos, K. P. Gummadi, and R. Rodrigues. Towards trusted cloud computing. DOI = http://www.mpi-sws.org/~gummadi/papers/trusted_cloud.pdf.

[28] M. Armbrust, A. Fox, R. Grifith, A. D. Joseph, and et al. Above the clouds: A berkeley view of cloud computing. Technical Report UCB/EECS-2009-28, 2009. DOI =

http://www.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-28.pdf.

[29] A. V. Konstantinou, T. Eilam, M. Kalantar, A. A. Totok, W. Arnold, E. Snible, An architecture for virtual solution composition and deployment in infrastructure clouds. *VTDC '09: Proceedings of the 3rd international workshop on Virtualization technologies in distributed computing*, Pages: 9-18. June 2009.

[30] P. Mell and T. Grance, The NIST Definition of Cloud Computing, version 15, October 7, 2009, National Institute of Standards and Technology (NIST), Information Technology Laboratory (www.csrc.nist.gov).

[31] T. Mather, S. Kumaraswamy, S. Latif, Cloud Security and Privacy: An Enterprise perspective of Risks and Compliance, O'Reilly Media, Inc., 2009.

[32] Top 7 threats to cloud computing DOI = www.net-security.org/secworld.php?id=8943.

[33] Open Security Architecture http://www.opensecurityarchitecture.org/.

[34] D. Jamil, H. Zaki, Cloud computing security, International Journal of Engineering Science and Technology, 3478-3484, 2011.

[35] Y. Chen, V. Paxson, R. H. Katz, What is new about cloud computing security? Technical report, University of california at Berkeley, 2010.

[36] S. Subashini, V. Kavitha, A survey on security issues in service delivery models of cloudcomputing, Journal of Network and Computer Applications, vol. 34, iss. 1. 2011, 1-11.

[37] P. Bodík, I. Menache, M. Chowdhury, Surviving Failures in Bandwidth-Constrained Datacenters, SIGCOMM 2012.

[38] L. Popa, G. Kumar, M. Chowdhury, FairCloud: Sharing the Network in Cloud Computing, SIGCOMM 2012.

[39] Y. Song, M. Zafer, and K. Lee, Optimal Bidding in Spot Instance Market, INFOCOM 2012.

[40] H. Liu, D. Orban, Cloud MapReduce: a MapReduce Implementation on top of a Cloud Operating System, technical reporter in Accenture Technology Labs.

http://www.google.com/search?client=safari&rls=en&q=Cloud+MapReduce:+a+MapReduce+Implementation+on+top+of+a+Cloud+Operating+System&ie=UTF-8&oe=UTF-8.

[41] J. Sherry, V. Sekar, S. Hasan, C. Scott, A. Krishnamurthy, and S. Ratnasamy, Making Middleboxes Someone Else's Problem: Network Processing as a Cloud Service, SIGCOMM 2012.

[42] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, Privacy-Preserving Multi-keyword Ranked Search over Encrypted Cloud Data, IEEE INFOCOM'11.

[43] K. Ren, C. Wang and Q. Wang, Security Challenges for the Public Cloud, IEEE Internet Computing, Vol. 16, No. 1, pp. 69-73, Jan. 2012.

[44] Y. Yuan, Z. Li, and K. Ren, Modeling Load Redistribution Attacks in Power System, IEEE

Transactions on Smart Grid, Vol. 2, No. 2, pp. 382-390, June, 2011.

[45] K. Ren, H. Su and Q. Wang, Secret Key Generation Exploiting Channel Characteristics in Wireless Communication, IEEE Wireless Communications, Vol. 18, No. 4, pp. 6-12, 2011.

[46] Q. Wang, P. Xu, K. Ren, and X. Y. Li, Towards Optimal Adaptive UFH-based Anti-jamming Wireless Communication, IEEE JSAC, Special Issue on Game Theory in Wireless Communications, Vol. 30, No. 1, pp. 16-30, Jan, 2012.

[47] N. Xiong, A. V. Vasilakos, J. Wu, Y. Richard Yang, A. J. Rindos, Y. Pan, A Class of Practical Self-tuning Failure Detection Schemes for Cloud Computing Networks, IPDPS 2012, Shanghai, China, May 21-24, 2012.

[48] L. Wei, H. Zhu, Z.Cao, X.Dong, W.Jia, Y.Chen, A.V.Vasilakos, "Security and Privacy for Storage and Computation in Cloud Computing," Information Sciences, to appear 2013.

[49] L. Wei, H. Zhu, Z. Cao, W. Jia, and A. V. Vasilakos, SecCloud: Bridging Secure Storage and Computation in Cloud, ICDCS-spcc 2010, Genova, Italy, June 21-25, 2010, pp: 52-61.

[50] A. Weiss. Computing in the Clouds. netWorker, 11(4):16-25, ACM Press, New York, USA, Dec.2007.

[51] Kai Hwang, Geoffrey Fox, and Jack Dongarra. Distributed Computing: Clusters, Grids and Clouds. May 2, 2010.

[52] Y. Chen, K. Hwang, and W. S. Ku, "Collaborative Detection of DDoS Attacks over Multiple Network Domains", IEEE Trans. on Parallel and Distributed Systems , Vol. 18, No.12, Dec. 2007, pp.1649-1662.

[53] C. Clark, K. Fraser, J. Hansen, E. Jul, I. Pratt, and A. Warfield, "Live Migration of Virtual Machines", Proc. of Symp. on Networked Systems Design and Implementation. Boston, May 2, 2005. 273 – 286.

[54] Nick Antonopoulos et al. Cloud Computing: Principles, Systems and Applications. 2010.

[55] Carolyn Duffy Marsan. Verisign expands cloud-based DDOS protection. May 09, 2011. Available at http://www.networkworld.com/news/2011/050911-verisign-ddos.html

[56] Carolyn Duffy Marsan.Tight security available to .com sites, but upgrades required. March 2011. available at http://www.networkworld.com/news/2011/033111-verisign-dns-security.html.

[57] H. Soon, A. Nakao, DaaS: DDoS Mitigation-as-a-Service. IEEE/IPSJ 11th International Symposium on Applications and the Internet (SAINT). Munich, Bavaria, 2011.

[58] A. Bakshi, et al. Securing Cloud from DDOS Attacks Using Intrusion Detection System in Virtual Machine. Second International Conference on Communication Software and Networks, ICCSN '10. Singapore, 2010.

[59] H. Soon, A. Nakao, sPoW: On-Demand Cloud-based eDDoS Mitigation Mechanism. Available at "http://wwwse.inf.tu-dresden.de/hotdep/S3-2-hin-bare_conf20090510b.pdf".