Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 7, July 2014, pg.680 – 688

RESEARCH ARTICLE

A Result Analysis on Secured Encryption in Cloud Computing using Symmetric Cryptography

Anand Darne[1], Rushikesh Longadge[2]

[1]Computer Science and Engineering G.H.Raisoni Academy of Engineering India

[2]Computer Science and Engineering, G.H.Raisoni Academy of Engineering India

[1] anadarne89@gmail.com; [2] rushi.longade@raisoni.net

Abstract-- The paper explains all the theoretical results related to privacy and security of cloud computing. We have implemented all these parameters in the form of basic cloud application and its deployment. Basically We have implemented attribute driven security model for cloud computing. Our application is able to resist the attacks from various fields over confidentiality, integrity, availability, accountability, and privacy-preservability. Because these are the most attacked parameters in cloud computing.

Cloud computing provides innumerable benefits to its customers but it fails to solve information security concerns especially in public cloud. Symmetric Cryptographic Key is sensitive data and it is required to be stored at cloud platform to solve several problems of encrypted data such as searching/manipulation on encrypted data. This paper is presenting a technique that will manage symmetric cryptographic keys on cloud-based environment. The technique is based on secret splitting technique enhanced Shamir's algorithm. Proposed technique will implemented in Open Stack private cloud environment for performance analysis.

We have identified five most representative security and privacy attributes (i.e., confidentiality, integrity, availability, accountability, and privacy-preservability). Beginning with these attributes, we present the relationships among them, the vulnerabilities that may be exploited by attackers, the threat models, as well as existing defense strategies in a cloud scenario. Future research directions are previously determined for each attribute.

Keywords- Cloud computing, security, privacy, trust, confidentiality, integrity, accountability, availability

I. INTRODUCTION

Recent advances have given rise to the popularity and success of cloud computing. However, when outsourcing the data and business application to a third party causes the security and privacy issues to become a critical concern. Throughout the study at hand, the authors obtain a common goal to provide a comprehensive review of the existing security and privacy issues in cloud environments. We have identified five most representative security and privacy attributes (i.e., confidentiality, integrity, availability, accountability, and privacy-preservability). Beginning with these attributes, we present the relationships among them, the vulnerabilities that may be exploited by attackers, the threat models, as well as existing defense strategies in a cloud scenario. Future research directions are previously determined for each attribute. Cryptographic key management includes all operations that can be performed on cryptographic key except encryption/decryption. These operations comprise but are not limited to generation, revocation, sharing and storage of cryptographic keys. One possible solution towards cryptographic key management for cloud is, to download data on client terminals for appropriate operation, and after that operation, upload data back on cloud server. This solution deviates from the benefits of cloud paradigm since all computations are performed on client machine. In addition, there is an overhead involved in upload and download. Section II will provide a detail analysis of other existing techniques related to cryptographic key management for cloud epitome. CLOUD computing has begun to emerge as a hotspot in both industry and academia; It represents a new business model and computing paradigm, which enables on demand provisioning of computational and storage resources. Economic benefits consist of the main drive for cloud computing due to the fact that cloud computing offers an effective way to reduce capital expenditure (CapEx) and

operational expenditure (OpEx). The definition of cloud computing has been given in many literatures but nothing has gained wide recognition. We defines cloud computing as: "A large-scale distributed computing paradigm that is driven by economies of scale, in which a pool of abstracted, virtualized, dynamically scalable, managed computing power, storage, platforms, and services are delivered on demand to external customers over the Internet.

II. ARCHITECTURE OF CLOUD COMPUTING

In this we present a top-level architecture of cloud computing that depicts various cloud service delivery models. Cloud computing enhances collaboration, agility, scale, availability and provides the potential for cost reduction through optimized and efficient computing. More specifically, cloud describes the use of a collection of distributed services, applications, information and infrastructure comprised of pools of compute, network, information and storage resources. Understanding the relationship and dependencies between these models is critical. IaaS is the foundation of all cloud services with PaaS building upon IaaS, and SaaS-in turn – building upon PaaS. An architecture of cloud layer model is depicted in Figure 1.

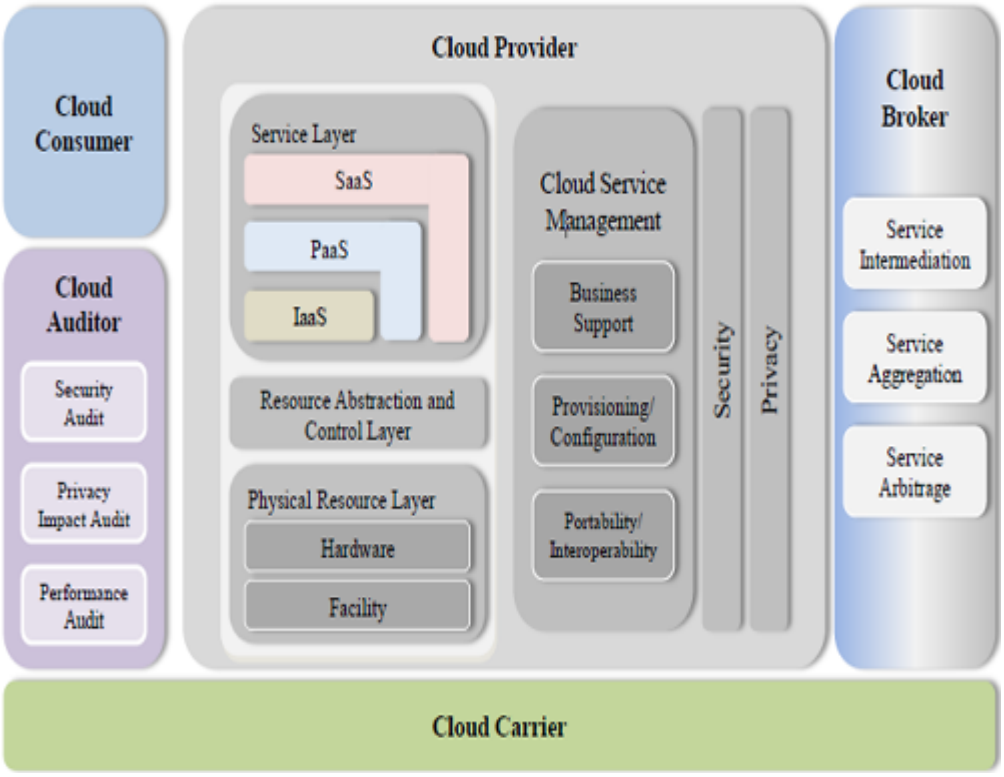

Fig 1: Architecture of Cloud Computing

A. *Software as a Service (SaaS):*

The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

B. *Platform as a Service (PaaS):*

The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.

C. *Infrastructure as a Service (IaaS):*

The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can

include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls).

III. DEPLOYMENT OF CLOUD COMPUTING

There are four types of cloud available in cloud computing i.e. private cloud, public cloud, hybrid cloud and community cloud as shown in Fig 2. These deployment models describe who owns, manages and is responsible for the services. The detail types of different type cloud are as follows:

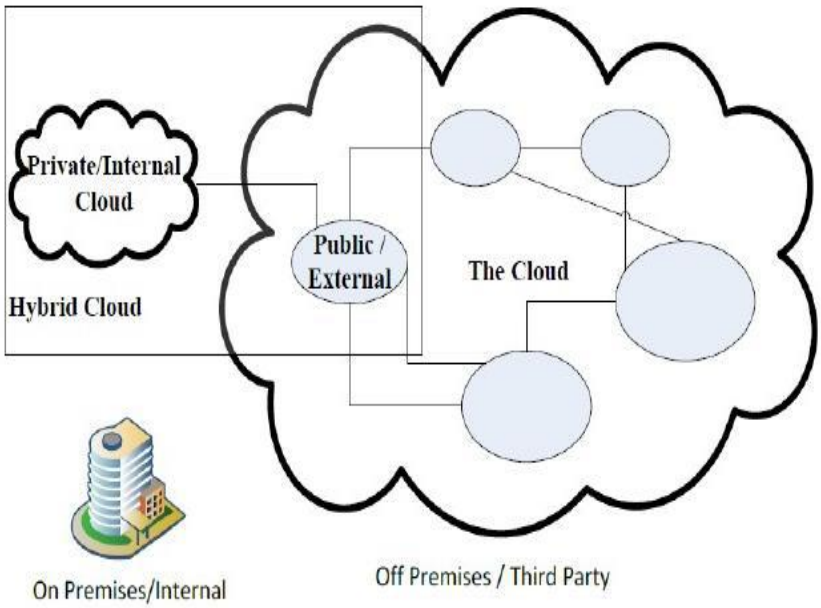

Fig 2. Deployment of Cloud Computing

1. *Four types of Cloud:*

A) Private cloud:

The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple Consumers (e.g. business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.

B) Public cloud:

The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider.

C) Community cloud:

The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises.

D) Hybrid cloud:

Hybrid cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that will be unique entities, but bound together by standardized technology that enables data and application portability.

2. *Cloud Characteristics and Security Challenges:*

The Cloud Security Alliance has summarized five essential characteristics [6] that illustrate the relation to, and differences from, traditional computing paradigm.

• On-demand self-service – A cloud customer may unilaterally obtain computing capabilities, like the usage of various servers and network storage, as on demand, without interacting with the cloud provider.

• Broad network access – Services are delivered across the Internet via a standard mechanism that allows customers to access the services through heterogeneous thin or thick client tools (e.g., PCs, mobile phones, and PDAs).
• Resource pooling – The cloud provider employs a multitenant model to serve multiple customers by pooling computing resources, which are different physical and virtual resources dynamically assigned or reassigned according to customer demand. Examples of resources include storage, processing, memory, network bandwidth, and virtual machines.
• Rapid elasticity – Capabilities may be rapidly and elastically provisioned in order to quickly scale out or rapidly released to quickly scale in. From customers' point of view, the available capabilities should appear to be unlimited and have the ability to be purchased in any quantity at any time.
• Measured service – The service purchased by customers can be quantified and measured. For both the provider and customers, resource usage will be monitored, controlled, metered, and reported.

Cloud computing becomes a successful and popular business model due to its charming features. In addition to the benefits at hand, the former features also result in serious cloud-specific security issues. The people whose concern is the cloud security continue to hesitate to transfer their business to cloud. Security issues have been the dominate barrier of the development and widespread use of cloud computing. There are three main challenges for building a secure and trustworthy cloud system:
• Outsourcing – Outsourcing brings down both capital expenditure (CapEx) and operational expenditure for cloud customers. However, outsourcing also means that customers physically lose control on their data and tasks.
The loss of control problem has become one of the root causes of cloud insecurity. To address outsourcing security issues, first, the cloud provider shall be trustworthy by providing trust and secure computing and data storage; second, outsourced data and computation shall be verifiable to customers in terms of confidentiality, integrity, and other security services. In addition, outsourcing will potentially incur privacy violations, due to the fact that sensitive/classified data is out of the owners' control.
• Multi-tenancy – Multi-tenancy means that the cloud platform is shared and utilized by multiple customers. Moreover, in a virtualized environment, data belonging to different customers may be placed on the same physical machine by certain resource allocation policy. Adversaries who may also be legitimate cloud customers may exploit the co-residence issue. A series of security issues such as data breach computation breach, flooding attack, etc.are incurred. Although Multi-tenancy is a definite choice of cloud venders due to its economic efficiency, it provides new vulnerabilities to the cloud platform. Without changing the multi-tenancy paradigm, it is imperative to design new security mechanisms to deal with the potential risks.
• Massive data and intense computation – cloud computing is capable of handling mass data storage and intense computing tasks. Therefore, traditional security mechanisms may not suffice due to unbearable computation or communication overhead. For example, to verify the integrity of data that is remotely stored, it is impractical to hash the entire data set. To this end, new strategies and protocols are expected.

3. *Supporting techniques:*

Cloud computing has leveraged a collection of existing techniques, such as Data Center Networking (DCN), Virtualization, distributed storage, MapReduce, web applications and services, etc. Modern data center has been practically employed as an effective carrier of cloud environments. It provides massive computation and storage capability by composing thousands of machines with DCN techniques.

Virtualization technology has been widely used in cloud computing to provider dynamic resource allocation and service provisioning, especially in IaaS. With virtualization, multiple OSs can co-reside on the same physical machine without interfering each other.

MapReduce is a programming framework that supports distributed computing on mass data sets. This breaks large data sets down into small blocks that are distributed to cloud servers for parallel computing. MapReduce speeds up the batch processing on massive data, which makes this become the preference of computation model for cloud venders. Apart from the benefits, the former techniques also present new threats that have the capability to jeopardize cloud security. For instance, modern data center suffers bandwidth under-provisioning problems, which may be exploited and may consequently perform a new DOS attack due to the shared infrastructure in cloud environments. Virtual Machine (VM) technique also has the capability to enable adversaries to perform cross-VM attacks and timing attacks due to VM co-residence.

4. *Notation System:*

To design the model we have used following notation:

Vi => Vulnerabilities

Ti, j => Denotes type of Threat

Di, j, k => Defense mechanism

Ti,j takes advantage of Vi which can be resist by Di, j, k.

IV. CLOUD VERNABILITIES

A) Co-residence(V1):

In cloud computing, co-residence (or co-tenancy) means that multiple independent customers share the same physical infrastructure. Concretely, virtual machines belonging to different customers may be placed in the same physical machine. VM co-residence has raised certain security issues, such as Cross-VM attack and Malicious Sys Admin.

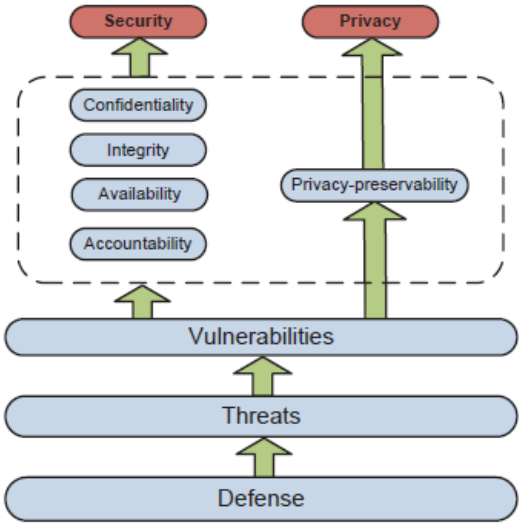

Fig.3 Ecosystem of cloud security and privacy

B) Loss of Physical Control(V2):

Cloud customers have their data and program outsourced to cloud servers. As a result, owners lose direct control on the data sets and programs. Loss of physical control means that customers are unable to resist certain attacks and accidents. For example, data or software may be altered, lost, or even deleted; in addition, it is difficult and impractical to ensure data/computation integrity and confidentiality with traditional methods.

C) Bandwidth Under-provisioning(V3):

A traditional DOS/DDOS attack does exist in cloud computing, and relative solutions have been given in prior researches specific to cloud computing, there is a new type of DOS attack that takes advantage of the current under-provisioned cloud-computing infrastructure. According to Cisco's design guide [24], a data center is usually designed to be under provisioned with a factor of 2.5:1 to 8:1, meaning that the actual network capacity is much less than the aggregate capacity of the hosts located in the same subnet.

D) Cloud Pricing Model(V4):

Cloud computing adheres to the pay-as-you-go pricing model that determines the cost of services in terms of metrics such as server hours, bandwidth, storage, etc. Since all cloud customers are financially responsible for the services they use, attackers always have incentives to harass the billing process by exploiting the pricing model. For example, Economic Denial of Sustainability (EDoS) attack [19] manipulates the utility pricing model and causes unmanageable costs for cloud customers.

We will focus on second and fourth Vulnerabilities: The first and third attack representation required heavy system configuration.

A) Loss of physical control(Cloud Integrity):

Data integrity implies that data should be honestly stored on cloud servers, and any violations (e.g., data is lost, altered, or compromised) are to be detected. Computation integrity implies the notion that programs are executed without being distorted by malware, cloud providers, or other malicious users, and that any incorrect computing will be detected.

Now, we will focus on Different integrity check mechanism (Defense Mechanism):

1) Naïve:

In this method the hash value of the file is computed and store on client side. When the client wants to check file integrity, it challenges the cloud by sending the hash value, if the value match, the file is not tampered.

Drawback: It cause heavy computational overhead and not a feasible solutions for cloud computing as cloud computing works on pay as you use basis.

2) Original Provable data possession (PDP):

In this method, the client keeps some part of the data as a metadata on client side for verification purpose. Once the client feels a necessity to check the data integrity at a later time, he/she sends a challenge to the cloud server, which will respond with a message based on the data content. After combining the reply and the local meta-data, the client is able to prove whether the integrity of the data is violated.

Drawback**:** PDP is applicable to only static files, that is the files that can be only append once uploaded to cloud.

3) Proof of Retrievability (POR) :

In this method, clients encrypt the file with the key and only store the key. The clients embed the bits of keys into file. For checking integrity client ask for subsets of bits and if that matches will proof the file is stored honestly and not tampered.
Drawback: The problem is same like PDP and can only apply on static files.

4) Third Party Auditor:

In this method client resides all these overhead of auditing data to the third party which is trustworthy and honest with both sides that is client and cloud. This method is most efficient than all above integrity check methods.
Drawback: The ttp again use the above parameter to check the integrity.

Solutions: Only solutions to above drawback are to efficiently manage defence mechanism and try to make computing more transparent.

B) Cloud Computing pricing:

Cloud computing pricing is based on pay as you go. It means customers have to pay for only the service he/she has used. The pricing is based on following metric.

1) Server Hour
2) Band width
3) Storage

V. CLOUD CONFIDENTIALITY

When dealing with cloud environments, confidentiality implies that a customer's data and computation tasks are to be kept confidential from both the cloud provider and other customers. Confidentiality remains as one of the greatest concerns with regards to cloud computing. This is largely due to the fact that customers outsource their data and computation tasks on cloud servers, which are controlled and managed by potentially untrustworthy cloud providers.

A) Threats to Cloud Confidentiality:

Cross-VM attack via Side Channels: It demonstrates the existence of Cross-VM attacks in an Amazon EC2 platform. A Cross-VM attack exploits the nature of multi-tenancy, which enables that VMs belonging to different customers may co-reside on the same physical machine. It regards timing side-channels as an insidious threat to cloud computing security due to the fact that a) the timing channels pervasively exist and are hard to control due to the nature of massive parallelism and shared infrastructure; b) malicious customers are able to steal information from other ones without leaving a trail or raising alarms. There are two main steps to practically initiate such an attack:

B) Malicious SysAdmin:

The Cross-VM attack discusses how others may violate confidentiality cloud customers that co-residing with the victim, although it is not the only threat. Privileged sysadmin of the cloud provider can

perform attacks by accessing the memory of a customer's VMs. For instance, Xenaccess enables a sysadmin to directly access the VM memory at run time by running a user level process in Domain.

VI. DEFENCE STRATERGIES

Approaches to address cross-VM attack fall into six categories: a)Placement prevention intends to reduce the success rate of placement; b) Physical isolation enforcement c) New cache designs d) Fuzzy time intends to weaken malicious VM's ability to receive the signal by eliminating fine-grained timers. e)Forced VM determinism ensures no timing or other non-deterministic information leaking to adversaries; f) cryptographic implementation of timing-resistant cache.

1) Placement Prevention: In order to reduce the risk caused by shared infrastructure, a few suggestions to defend the attack in each step are given in [17]. For instance, cloud providers may obfuscate co-residence by having Dom not respond in trace route, and/or by randomly assigning internal IP addresses to launched VMs. To reduce the success rate of placement, cloud providers might let the users decide where to put their VMs; however, this method does not prevent a brute-force strategy.

2) Co-residency Detection: The ultimate solution of cross-VM attack is to eliminate co-residency. Cloud customers (especially enterprises) may require physical isolation, which can even be written into the Service Level Agreements (SLAs). However, cloud vendor may be reluctant to abandon virtualization that is beneficial to cost saving and resource utilization. One of the left options is to share the infrastructure only with "friendly" VMs, which are owned by the same customer or other trustworthy customers. To ensure physical isolation, a customer should be enabled to verify its VMs' exclusive use of a physical machine. HomeAlone is a system that detects co-residency by employing a side-channel (in the L2 memory cache) as a detection tool. The idea is to silence the activity of "friendly" VMs in a selected portion of L2 cache for a certain amount of time, and then measure the cache usage to check if there is any unexpected activity, which indicates that the physical machine is co-resided by another customer.

3) NoHype: NoHype attempts to minimize the degree of shared infrastructure by removing the hypervisor while still retaining the key features of virtualization. The NoHype architecture provides a few features: i)
the "one core per VM" feature prevents interference between VMs, eliminates side channels such as L1 cache, and retains multi-tenancy, since each chip has multiple cores; ii) memory partition restricts each VM's memory access on a assigned range; iii) dedicated virtual I/O devices enables each VM to be granted direct access to a dedicated virtual I/O device. No- Hype has significantly reduced the hypervisor attack surface, and increased the level of VM isolation. However, NoHype requires tochange hardware, making it less practical when consider applying it to current cloud infrastructures.

4) Trusted Cloud Computing Platform: Santos present a trusted cloud-computing platform (TCCP), which offers a closed box execution environment for IaaS services. TCCP guarantees confidential execution of guest virtual machines. It also enables customers to attest to the IaaS provider and to determine if the service is secure before their VMs are launched into the cloud. The design goals of TCCP are: 1) to confine the VM execution inside the secure perimeter; 2) that a sysadmin with root privileges is unable to access the memory of a VM hosted in a physical node. TCCP leverages existing techniques to build trusted cloud computing platforms. This focuses on solving confidentiality problems for clients' data and for computation outsourced to the cloud. With TCCP, the sysadmin is unable to inspect or tamper with the content of running VMs.

5) Other opinions: retaining data control back to customer: Considering the customer's fear of losing the data control in cloud environments it propose to retain data control for the cloud customers by simply storing encrypted VMs on the cloud servers. Encrypted VM images guarantee rigorous access control since only the authorized users known as key-holders are permitted access. Due to the encryption, the data cannot be mounted and modified within the cloud without an access key, assuring the confidentiality and integrity. This approach offers security guarantees before a VM is launched; however, there are ways to attack the VM during running time and to jeopardize the data and computation.

VII. CLOUD INTEGRITY

Similar to confidentiality, the notion of integrity in cloud computing concerns both data integrity and computation integrity. Data integrity implies that data should be honestly stored on cloud servers, and any violations (e.g., data is lost, altered, or compromised) are to be detected. Computation integrity implies the notion that programs are executed without being distorted by malware, cloud providers, or other malicious users, and that any incorrect computing will be detected.

A. Threats to Cloud Integrity:

1) Data loss/manipulation: In cloud storage, applications deliver storage as a service. Servers keep large amounts of data that have the capability of being accessed on rare occasions. The cloud servers are distrusted in terms of both security and reliability which means that data may be lost or modified maliciously or accidentally. Administration

errors may cause data loss (e.g., backup and restore, data migration, and changing memberships in P2P systems. Additionally, adversaries may initiate attacks by taking advantage of data owners' loss of control over their own data.

2) Dishonest computation in remote servers: With outsourced computation, it is difficult to judge whether the computation is executed with high integrity. Since the computation details are not transparent enough to cloud customers, cloud servers may behave unfaithfully and return incorrect computing results; they may not follow the semi-honest model. For example, for computations that require large amount of computing resources, there are incentives for the cloud to be lazy. On the other hand, even the semi-honest model is followed; problems may arise when a cloud server uses outdated, vulnerable code, has misconfigured policies or service, or has been previously attacked with a root kit, triggered by malicious code or data.

B. Defense Strategies

1) Provable Data Possession (PDP): Integrity checking on data is a long-term research topic and traditional methods cannot be properly adopted to tackle the challenges of integrity checking presenting in cloud storage. The main challenge of integrity checking is that tremendous amounts of data are remotely stored on untrustworthy cloud servers; as a result, methods that require hashing for the entire file become prohibitive. In addition, it is not feasible to download the file from the server and perform an integrity check due to the fact that it is computationally expensive as well as bandwidth consuming. Each of the former notions is not acceptable in cloud environments.

VIII. CLOUD AVAILABILITY

Availability is crucial since the core function of cloud computing is to provide on-demand service of different levels. If a certain service is no longer available or the quality of service cannot meet the Service Level Agreement (SLA), customers may lose faith in the cloud system. In this section, we have studied two kinds of threats that impair cloud availability.

A. Threats to Cloud Availability:

1) Flooding Attack via Bandwidth Starvation:

In a flooding attack, which can cause Deny of Service (DoS), a huge amount of nonsensical requests are sent to a particular service to hinder it from working properly. In cloud computing, there are two basic types of flooding attacks:
Direct DOS – the attacking target is determined, and the availability of the targeting cloud service will be fully lost.
Indirect DOS – the meaning is twofold: 1) all services hosted in the same physical machine with the target victim will be affected; 2) the attack is initiated without a specific target.

2) Fraudulent Resource Consumption (FRC) attack:

A representative Economic Denial of Sustainability (EDoS) attack is FRC, which is a subtle attack that may be carried out over a long period (usually lasts for weeks) in order to take effect. In cloud computing, the goal of a FRC attack is to deprive the victim (i.e., regular cloud customers) of their long-term economic availability of hosting web contents that are publicly accessible. In other words, attackers, who act as legal cloud service clients, continuously send requests to website hosting in cloud servers to consume bandwidth, which bills to the cloud customer owning the website; seems to the web server, those traffic does not reach the level of service denial, and it is difficult to distinguish FRC traffic from other legitimate traffic. A FRC attack succeeds when it causes financial burden on the victim.

IX. CLOUD ACCOUNTABILITY

While accountability has been studied in other systems, it is essential in order to build trust relationships in cloud environment. Accountability implies that the capability of identifying a party, with undeniable evidence, is responsible for specific events. When dealing with cloud computing, there are multiple parties that may be involved; a cloud provider and its customers are the two basic ones, and the public clients who use applications (e.g., a web application) outsourced by cloud customers may be another party. A fine-grained identity, however, may be employed to identify a specific machine or even the faulty/ malicious program that is responsible.

1) SLA violation: A. Haeberlen addresses the importance of accountability in cloud computing where the loss of data control is problematic when something goes awry. For instance, the following problems may possibly arise: 1) The machines in the cloud can be misconfigured or defective and can consequently corrupt the customer's data or cause his computation to return incorrect results; 2) The cloud provider can accidentally allocate insufficient resources for the customer, an act which can degrade the performance of the customer's services and then violate the SLA; 3) An attacker can embed a bug into the customer's software in order to steal valuable data or to take over the customer's machines for spamming or DoS attacks; 4) The customer may not have access to his data either because the cloud loses it or simply because the data is unavailable at an inconvenient time.

3) Dishonest MapReduce: MapReduce is a parallel computing paradigm that is widely employed by major cloud providers (Google, Yahoo!, Facebook, etc.). MapReduce splits a large data set into multiple blocks, each of which

are subsequently input into a single worker machine for processing. However, working machines may be mis-configured or malicious, as a result, the processing results returned by the cloud may be inaccurate. In addition, it is difficult for customers to verify the correctness of results other than by running the same task again locally. Dishonest MapReduce may be viewed as a concrete case of computation integrity problem, as we discussed in Section III (i.e., cloud integrity). The issue will be further addressed by accountability, because even after customers have verified the correctness of MapReduce output, there is still a necessity to identify the faulty machines or any other possible reasons that resulted in wrong answers.

X. CLOUD PRIVACY

Privacy is yet another critical concern with regards to cloud computing due to the fact that customers' data and business logic reside among distrusted cloud servers, which are owned and maintained by the cloud provider. Therefore, there are potential risks that the confidential data (e.g., financial data, health record) or personal information (e.g personal profile) is disclosed to public or business competitors. Privacy has been an issue of the highest priority. Throughout this text, we regard privacy-preservability as the core attribute of privacy. A few security attributes directly or indirectly influence privacy-preservability, including confidentiality, integrity, accountability, etc. Evidently, in order to keep private data from being disclosed, confidentiality becomes indispensable, and integrity ensures that data/computation is not corrupted, which somehow preserves privacy. Accountability, on the contrary, may undermine privacy due to the fact that the methods of achieving the two attributes usually conflict. More details will be given in this section.

XI. CONCLUSION

Thus in this paper, the authors have systematically studied the security and privacy issues in cloud computing based on SHA algorithm. We have identified the most representative security/privacy attributes (e.g., confidentiality, integrity, availability, accountability, and privacy-preservability), as well as discussing the vulnerabilities, which may be exploited by adversaries in order to perform various attacks. Defense strategies and suggestions were discussed as well. We believe this review will help shape the future research directions in the areas of cloud security and privacy.

REFERENCES

[1] Yinqian Zhang, A. Juels, A. Oprea, and M. K. Reiter, "HomeAlone: Co-residency Detection in the Cloud via Side-Channel Analysis," in 2011 IEEE Symposium on Security and Privacy (SP), 2011, pp. 313- 328

[2] E. Keller, J. Szefer, J. Rexford, and R. B. Lee, "NoHype: virtualized cloud infrastructure without the virtualization," in Proc. 37th annual international symposium on Computer architecture, New York, NY, USA, 2010, pp. 350-361

[3] H. Chen and B. Sun, "Editorial," International J. Security and Networks, Vol. 6 Nos. 2/3, 2011, pp. 65-66.

[4] M. Barua, X. Liang, R. Lu, X. Shen, "ESPAC: Enabling Security and Patient-centric Access Control for eHealth in cloud computing ," International J. Security and Networks, Vol. 6 Nos. 2/3, 2011, pp. 67-76.

[5] N. Jaggi, U. M. Reddy, and R. Bagai, "A Three Dimensional Sender Anonymity Metric," International J. Security and Networks, Vol. 6 Nos. 2/3, 2011, pp. 77-89.

[6] M. J. Sharma and V. C. M. Leung, "Improved IP Multimedia Subsystem Authentication Mechanism for 3G-WLAN Networks," International J. Security and Networks, Vol. 6 Nos. 2/3, 2011, pp. 90-100.

[7] N. Cheng, K. Govindan, and P. Mohapatra, "Rendezvous Based Trust Propagation to Enhance Distributed Network Security," International J. Security and Networks, Vol. 6 Nos. 2/3, 2011, pp. 101-111.

[8] A. Fathy, T. ElBatt, and M. Youssef, "A Source Authentication Scheme Using Network Coding," International J. Security and Networks, Vol. 6 Nos. 2/3, 2011, pp. 112-122.

[9] L. Liu, Y. Xiao, J. Zhang, A. Faulkner, and K. Weber, "Hidden Information in Microsoft Word," International J. Security and Networks, Vol. 6 Nos. 2/3, 2011, pp. 123-135.

[10] S. S.M. Chow and S. Yiu, " Exclusion-Intersection Encryption," International J. Security and Networks, Vol. 6 Nos. 2/3, 2011, pp. 136-146.

[11] Resch, Jason; Plank, James (February 15, 2011). "AONT-RS: Blending Security and Performance in Dispersed Storage Systems" Usenix FAST'll, 2011.

