Asian Journal of Information Technology 15 (7): 1199-1206, 2016
ISSN: 1682-3915

Examining the Security and Privacy Practices in Cloud Computing

[1]P. Thinakaran and [2]S. Chitra
[1]Department of Computer Science and Engineering, SNS College of Technology, Coimbatore, Tamil Nadu, India
[2]Er. Perumal Manimegalai College of Engineering, Hosur, Krishnagiri, Tamil Nadu, India

Abstract: The recent advancements in cloud computing in business and data applications provides computing and storage capabilities on demand. The key idea in cloud computing is outsourcing of data to a third party where the security and privacy issues can arise. The previous systems related to cloud environments are studied and five attributes relating to security and privacy are identified. The relationship among these attributes is presented along with their vulnerabilities, security and problem strategies.

Key words: Cloud computing, privacy, security, attributes, vulnerabilities, problem strategies

INTRODUCTION

The cloud computing has began to emerge both in the field of industry and academics representing the business models and computing environments. It provides resources for computing and storage on need by providing an effective way to reduce initial and equipment costs. The cloud computing literally means a distributed computing environment which delivers cost effective services to the customers over the internet during their needs (Foster *et al*., 2008; Geelan, 2004; Buyya *et al*., 2008).

Cloud architecture: Cloud offers various services from bottom layer to the top where each and every layer represents a service models as (Fig. 1).

Infrastructure as a Service (IaaS): It forms the bottom layer outsourcing the equipments for supporting operations which includes storage space, hardware, servers and network components. Providers of these services are responsible for running and maintaining it for which the customers are charged on the basis on consumption.

Platform as a Service (PaaS): It forms the middle layer which rents the hardware, operating systems and storage and network components over internet.

Software as a Service (SaaS) It forms the top layer in which the software applications are made available to the customers over the internet.

Characteristics of cloud: There are five important characteristics which are addressed in cloud as,

On-demand self service: The customer of cloud can gain access to servers and storage space on need without disturbing the provider of cloud services.

Broad network access: The services are scattered over the network which can be accessed using standard mechanisms.

Resource pooling: Multiple servers can share the computing resources of the provider dynamically as per the customer's need.

Rapid elasticity: The services appear unlimited to the customer's which can be accessed at any time.

Measured service: The resources used by both the customer's and providers can be monitored, controlled, reported about the utilization.

Threats to cloud computing: The four main challenges focused are.

Data loss: The providers of cloud hold a voluminous amount of data communicated from one end to the other. The increasing amount of sensitive information within the server of providers could be lost, corrupted (or) accidentally deleted.

Account hijacking: It is another serious threat that occurs when an user access the sensitive information

Corresponding Author: P. Thinakaran, Department of Computer Science and Engineering, SNS College of Technology, Coimbatore, Tamil Nadu, India

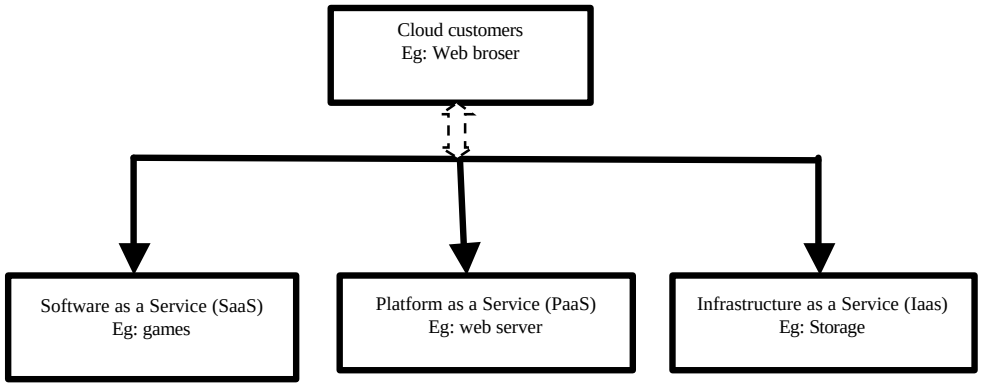

Fig. 1: Cloud architecture

from the cloud via remote machines without enough security features.

Denial of service: The data stored in the cloud servers cannot be accessed by the genuine customers temporarily.

Handling data: It increases the risk of handling the data. Many times the servers of cloud are configured to work with few customers but when additional customers get added up the data can be accessed wrongly

MATERIALS AND METHODS

Techniques supported: The following techniques are discussed which has its influence from the existing methods and they are.

Data center: It provides voluminous computing and storage capacity for thousands of machines over the networks.

Virtualization: It provides dynamic allocation of resources and services in IaaS. This technique allows multiple operating systems to reside in a same physical machine without any interference.

Mapreduce: The study proposes a programming framework for large data sets over distributed computing which works by breaking large data sets into small blocks which are distributed inside the servers for parallel processing.

Vulnerability to cloud: The following new threats are also accounted in cloud computing as:

- The data center can suffer bandwidth starvation (Lombardi and Pietro, 2010)
- Denial of Service can occur due to the shared architecture
- In cloud computing multiple independent customers can share the same physical infrastructure which causes security issues (Ristenpart *et al*., 2009)
- The customers of cloud have their data and program outsourced to cloud as a result the owner of data lose their control
- The services of the cloud are provided as pay per use which can cause financial risk

Privacy and security system: The security and privacy in cloud computing is viewed as five attributes as, confidentiality, integrity, availability, accountability and privacy preservation. In Fig. 2, the privacy and security are separated from each other due to its importance. The privacy is a component of security since, the security is an essential attribute for a networked system (Vimercati *et al*., 2007; Ateniese *et al*., 2007; Juels and Kaliski, 2007; Dodis *et al*., 2009).

Confidentiality in cloud: The task is to keep the customer data secure from both cloud provider and the customer. Confidentiality remains a key challenge since the customer outsources their data and computation which is hold within the servers. These data and computations must be secured from the third party users.

Threats: The threats in cloud system occur when the third party users tries to steal the information without leaving any evidences. The two main aspects which initiate the attack are placement and extraction of third party users to the system. The system admin can attack behaving like trusted party and tries to attack the memory of the customer's machine.

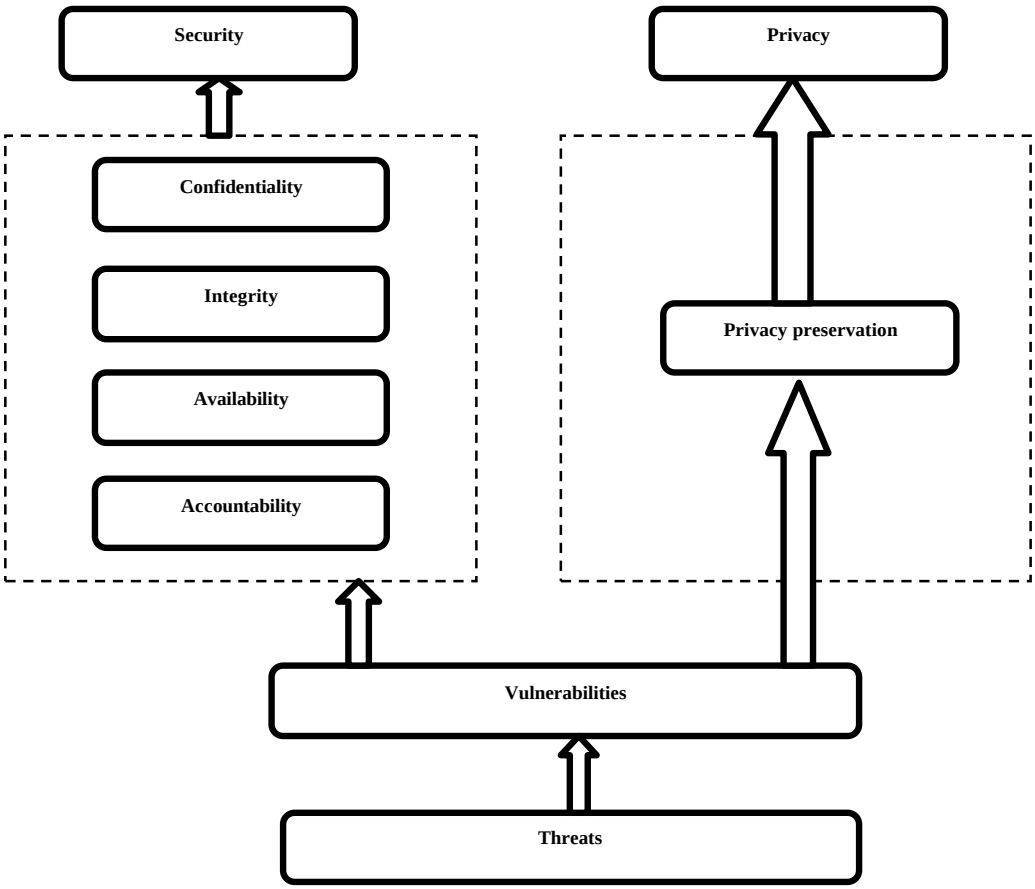

Fig. 2: Privacy and security system

Security: The following are the approaches to address the attack:

- Prevention of placement risk by shared infrastructure (Ristenpart *et al*., 2009)
- Physical isolation for cloud customers as per the service agreement so, to save the cost and computation
- Minimizing the shared infrastructure by removing the hypervisor but still containing virtualization (Vaquero *et al*., 2011)
- The trusted cloud computing enables the IaaS providers and determines the security in service before uploading into cloud. A privilege is needed to unable the access of customer's memory (Buyya *et al*., 2008; Geelan, 2009)

It focuses on customer security upon outsourced data and computing. The study proposes a control over data in cloud by encryption. The authorized key holders can only access the cloud data. Due to the encrypted data mounted which cannot be modified using access key it offers security and integrity (Xiao and Xiao 2013).

Problem:

- It is possible for the customer to check whether the physical isolation is well imposed
- The hardware changes should be focused since it accommodates data and hardware changes which are also to be addressed

Integrity in cloud: It refers both the data and computation integrity. The data integrity address that the data are stored into the cloud servers where violations can also be

detected. Computational integrity address that the programs are not defected by malware and incorrect computing will also be detected.

Security: The storage is also provided as service that holds large volume of data (Ateniese *et al*., 2008). The servers are distributed by means of both security and reliability which may cause loss in data (or) modification. The data loss may also occur as a result of administration errors. The owner of the data might lose the control over the data.

The cloud is the providers of outsourced based computing where the integrity in computation cannot be predicted. Due to the hiding of customer information within the cloud may result in incorrect results from the cloud servers known as partial honest model.

The traditional methods cannot be adapted properly to handle challenges in integrity. The key challenge occurs when large amount of data gets stored into unfaithful servers thus requiring hashing for entire file. It is also not possible to perform integrity check since it consumes large bandwidth thus increasing the computation costs.

The study proposes a special method where the client computes a hash value for the file using key and sending that file to the server for accessing a file. (Ateniese *et al*., 2007). The key is released and send to the server where the key is recomputed for hash value of the file and key. This result is communicated to the client for comparison. The client performs multiple checks for different files and keys. A proof will be provided that the file still remains in the file.

Demerits: During every verification the server runs the hash function over entire file. The study proposes a original provable data possession which processes the data in setup phase to leave some description of data on the client side verification. A respond message based upon the data content is obtained upon which it is combined with local data description where the client tries to prove integrity violation. The PDP is applied to static files meaning that the data should not be changed after uploading it to the server.

The study proposes a full dynamic operations which provides rank based insert and delete functions (Ateniese *et al*., 2008). It introduces three new operations like prepare for update, processing the update and verifying the update.

The study proposes a trusted third party both on customer and provider side for verifying the integrity over data.

The study proposes outsourcing the computations from one machine to the other without any local computations and tries to verify the correctness of result obtained by other machine. The integrity check can be done as:

- It requires the local machines to perform re-computation and then comparing the results
- By assigning the computations over multiple machines and then comparing the results
- The computations are recorded during the critical events which are sending to one (or) multiple auditors for review purposes
- The computer should have consistency both in hardware and software (Geelan, 2004; Vaquero *et al*., 2010)

Problems:

- The integrity checking should be done with some realistic environment
- Some practical verification methods should be done to compute integrity

Availability in cloud: It provides on-demand service at different levels. In case, certain services are no longer available (or) quality of service is compromised the service level agreement cannot be met. The customers may lose faith in cloud based system.

Threats: The flooding attack can deny the large amount of non-sensual request which are send to particular server thus hindering its normal working. The types of flooding are:

- Direct Denial of Service restricts the users from accessing the required resources
- Indirect Denial of Service is initiated by third party i.e., uses someone's machine to launch an attack which are difficult to address

The study points out that the consequences of flooding attack is that if the quality of service is compromised the subscribers gets affected and continues to pay the bill (Ateniese *et al*., 2008). It is necessary that the providers of cloud should have a signed service level agreement with customers thus enabling the customers to be aware about the degree of service degradation.

Security: The defending denial of service attacks differ from traditional DOS (Lombardi and Pietro, 2010). The traditional DOS sends traffic to the host directly while new DOS attack does not. The service migration is required to avoid DOS which also deals with new flooding attacks (Foster *et al*., 2008).

The bandwidth degradation can be detected by setting up a monitoring agent located outside the cloud. Once detecting the bandwidth degradation the monitoring agent will not stop the service but shift the current application unknown by the attacker.

Problems:

- The DOS avoidance cannot entirely provide security against attack but it can be overcome by identifying the origin
- The behavior of sufferer and their reaction along with the identification of attacks were not presented

Accountability in cloud: In cloud environment accountability is essential for constructing a dependable relationship (Ristenpart *et al*., 2009; Ateniese *et al*., 2007; Gruschka and Jensen, 2010). The cloud involves more than one party as the provider of cloud and the customers form the basic blocks and the other is the cloud applications outsourced to the customers.

Threats: The study proposes the problem which occurs in controlling the data loss (Ristenpart *et al*., 2009). The following are the problems that could arise:

- The machine in cloud can be defective resulting in corrupting the user data thus providing inappropriate results
- By allocating insufficient resources by cloud providers arises performance problem
- An attacker can intrude the customer software and introduces bug in order to steal the valuable customer data
- The customer cannot access his data due to unavailability

The study proposes map reduce which splits the large data sets into blocks (Buyya *et al*., 2008). Each of the blocks is input to single machine for computing. An error may occur if the working computer are not properly configured thus resulting in defect in accuracy and correctness of data.

Due to privacy concerns it is not possible for cloud providers to disclose the information related to customer. The problem can be overcome using secret access which requires the entire information of customer to be hidden.

The pay per use model provides the customer a way to access the services along with the financial situation. It becomes a drawback that customers cannot track the expenses since the cloud providers for keeping high access integrates the applications of different users. The integration may add up additional costs to the customer's.

RESULTS AND DISCUSSION

Security: The study proposes a audit for customer's to check whether the cloud providers have satisfied the services. The building blocks are provided as:

- Bookmarking the action of applications
- The recorded history can be used to audit the actions of other applications using virtualization
- The time stamp to detect fault in performance
- Sampling to improve efficiency in replaying the recorded actions

The study proposes an accountable verifiable machine which enables the users to audit software execution on the remote machines for (Vimercati *et al*., 2007):

- Detecting faults
- Detecting fault node
- Providing evidence for particular fault

The virtualization accounts to correctness of code in the system by customers. This mechanism records interference proof of the software. In case a reference implementation is made it defines the correctness by replaying the recorded logs and comparing it with the reference copy. During inconsistency mismatches will be detected.

Demerits: It detects only the faults occurred by network operations. The study proposes solution similar to verifiable machine by maintaining an external state machine which validates the correctness of data. A service end point acts as bridge to deliver services to the end users. It is assumed that the data is accessed through end points between cloud providers and the end users. The key idea is to cover each end point with an adapter to record all operations that captures the input and output of end point. These records are sent to external state machines for safety purposes. Merkle B-tree is used to authenticate the data stored in cloud.

The study proposes task duplication for double verification of processed results (Vaquero *et al*., 2011). It uses secure map reduce which requires twice the two different machines that doubles the total execution time of performing the task.

Demerits: When identical fault program process the data it produces false results. The study proposes an accountable map reduce for detecting fault nodes by establishing auditors which applies test on each working machine. The test picks up a completed task and re-executes it to compare it with the generated results.

Demerits: It involves large computation costs. Secure providence aims to verify the proof provided by original data owner and modified logs using bilinear pairing techniques (Squicciarini *et al*., 2010).

The study proposes a resource computing which can be proved but it requires the customer's of cloud to ensure (Pearson *et al*., 2009):

- They only consume the resource they pay for
- The consumption should agree with the policy

For practical intension of accountability in cloud a life cycle is described as:

- Policy plan
- Gather and trace
- Recording
- Securing the records
- Reporting
- Replaying the logs
- Auditing
- Rectification

Problems:

- Replication in cloud is not efficient which can be improved by sampling but it reduces the accuracy
- The accuracy can be obtained by semi-trust model

Privacy in cloud: The privacy in cloud computing remains a key challenge since the customer's private and personal data is present inside the distributed servers. These servers are hold and maintained by the providers of cloud which increases the risk in sharing the private and personal information to the other users. Due this reasons privacy is given the top priority (Juels and Kaliski, 2007; Dodis *et al*., 2009; Ateniese *et al*., 2008).

These are the attributes that openly (or) closely preserve the privacy. They can be secrecy and reliability which ensures the source of the data. The term accountability can be used along with the privacy since the attributes within these two methods can conflict.

Threats: The privacy preservation is needed with secrecy since both retards the information leakage. In case, if the secrecy is compromised, privacy preservation will also be compromised. It is most common like in other security services but in cloud computing privacy is preserved for data and computation.

Security: The study proposes privacy preservation in cloud is provided by encrypting the data stored in distributed servers by cloud providers (Ateniese *et al*., 2008). The user can access without decrypting the data. The cloud server may (or) may not hold the information related to the input data, the method of dealing input, the intermediate and final results. Hence, the computation occurs in a fully protected manner.

Merits: It enforces privacy preservation in cloud.

Demerits: It is practically impossible scheme and it requires reduced complexity. The study proposes a manager for privacy preservation by making the information opaque and visible to the users (Juels and Kaliski, 2007; Dodis *et al*., 2009). It significantly reduces the private data access to public. The goal is to store encrypted information into the cloud.

Demerits: The provider of cloud will not add up additional services. It requires the fullest cooperation from cloud service providers.

The study proposes indexing of data in order to avoid information out flow (Squicciarini *et al*., 2010). A three tier protection system for data protection at different levels is presented.

The study proposes privacy as a service in order to provide security and computing the private data by pulling against interference using cryptographic schemes.

Merits: It protects the customer data from attackers. The study deals that pure cryptographic solution on fully homomorphic and verifiable encryption suffers high transfer rate in real time to provide cloud outsourcing to distributed cloud service providers (Pearson, 2009). A trusted hardware token is proposed with accessing security function on encrypted data. It does not allow information overflow and is validated. The ultimate focus is to reduce the communication time for effective cloud service outsourcing. The hardware token safeguards against attacks where the client's data processing is associated with this token attached to the distributed servers. The token ensures the computation on data is secret as well as validate.

The study proposes a solution by setting up an inference free token in pre-processing phase which performs only symmetric cryptographic operations (Pearson, 2009). They are performed without interacting with the token.

Suggestions:

- The study disagrees that only cryptography cannot provide overall solutions for preserving privacy in cloud (Lombardi and Pietro, 2010)
- An application should only process a data owned by a single client without the knowledge of other parties
- Applications operates on a set of data involving more clients since, the privacy preservation among multiple clients becomes more complicated so, certain access control mechanism are to be followed
- The access control mechanism depends upon the computation history
- The study proposes an architecture to overcome the privacy preservation challenges as
- Ranking setup can help the customer's of cloud to identify a provider that fits the best in privacy requirements
- The automated policy generation combines both the policies and requirements from both the participants and a specific agreed policy is produced
- Ranking of policies occurs by comparing the requirements of customer with the policies of multiple servers and picking the highest rank. The client (or) provider (or) brokers may compare the policy for which policy algebra generates the policy. The three enforcements ensure the fulfillment of policy

Problems:

- Conflicts can occur between accountability and privacy
- The amount of privacy (or) security offered is needed to be evaluated

CONCLUSION

In this study, the privacy and security issues in cloud computing has been studied methodically. The essential security and privacy issues have been identified and discussed along with vulnerabilities to overcome attacks. For which the problems and suggestions are also well studied.

REFERENCES

Ateniese, G., R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson and D. Song, 2007. Provable data possession at untrusted stores. Proceedings of the 14th ACM Conference on Computer and Communications Security, October 29, 2007, Alexandria, Virginia, USA., pp: 598-609.

Ateniese, G., R. di Pietro, L.V. Mancini and G. Tsudik, 2008. Scalable and efficient provable data possession. Proceedings of the 4th International Conference on Security and Privacy in Communication Networks, September 22-25, 2008, New York, USA., pp: 1-11.

Buyya, R., C.S. Yeo and S. Venugopal, 2008. Market-Oriented cloud computing: Vision, Hype and reality for delivering IT services as computing utilities. Proceedings of the 10th IEEE International Conference on High Performance Computing and Communications, September 26-28, 2008, Houston, USA., pp: 5-13.

Dodis, Y., S. Vadhan and D. Wichs, 2009. Proofs of Retrievability via Hardness Amplification. In: Theory of Cryptography. Reingold, O. (Ed.). Springer Berlin Heidelberg, Heidelberg, Germany, ISBN: 978-3-642-00456-8, pp: 109.

Foster, I., Y. Zhao, I. Raicu and S. Lu, 2008. Cloud computing and grid computing 360-degree compared. Proceedings of the Grid Computing Environments Workshop, November 12-16, 2008, Austin, TX., USA., pp: 1-10.

Geelan, J., 2009. Twenty-one experts define cloud computing. Cloud Comput. J., 2: 1-5.

Gruschka, N. and M. Jensen, 2010. Attack surfaces: A taxonomy for attacks on cloud services. Proceedings of the IEEE 3rd International Conference on Cloud Computing, July 05-10, Miami, Florida, pp: 276-279.

Juels, A. and B.S. Kaliski Jr, 2007. PORs: Proofs of retrievability for large files. Proceedings of the 14th ACM Conference on Computer and Communications Security, October 29-November 02, 2007, ACM, New York, USA, ISBN: 978-1-59593-703-2, pp: 584-597.

Lombardi, F.and R.D. Pietro, 2010. Transparent security for cloud. Proceedings of the ACM Symposium on Applied Computing, March 22-26, 2010, ACM, New York, NY, USA., ISBN: 978-1-60558-639-7, pp: 414-415.

Pearson, S., 2009. Taking account of privacy when designing cloud computing services. Proceedings of the ICSE Workshop on Software Engineering Challenges of Cloud Computing, May 22-23, 2009, Vancouver, Canada, pp: 44-52.

Ristenpart, T., E. Tromer, H. Shacham and S. Savage, 2009. Hey, you, get off of my cloud: Exploring information leakage in third-party compute clouds. Proceedings of the the 16th ACM Conference on Computer and Communications Security, November 9-13, 2009, Chicago, IL., USA., pp: 199-212.

Squicciarini, A., S. Sundareswaran and D. Lin, 2010. Preventing information leakage from indexing in the cloud. Proceeding of the 3rd International IEEE Conference on Cloud Computing, July 5-10, 2010, IEEE, Miami, Florida, ISBN: 978-1-4244-8207-8, pp: 188-195.

Vaquero, L.M., L. Rodero-Merino and D. Moran, 2011. Locking the sky: A survey on IaaS cloud security. Computing, 91: 93-118.

Vimercati, S.D.C.D., S. Foresti, S. Jajodia, S. Parabosch and P. Samarati, 2007. A data outsourcing architecture combining cryptography and access control. Proceedings of the ACM Workshop on Computer Security Architecture, October29-November 02, 2007, ACM, Alexandria, VA, USA., ISBN: 978-1-59593-890-9, pp: 63-69.

Xiao, Z. and Y. Xiao, 2013. Security and privacy in cloud computing. Commun. Surv. Tutorials IEEE., 15: 843-859.