MODELLING ANALYSIS TO BUILD TRUST IN CLOUD

Simriti Gupta and Akshat Uttam

guptasimi1234@gmail.com,
akshatuttam888@gmail.com

Abstract. Cloud computing is on-demand internet based services with pay as you go pricing system which allows users to share storage, hardware and many other resources over the network. It may be free or paid based on your selection. This paper describes various risks and uncertainty that cloud users and providers undergo and solution to these risks and uncertainties. The other important part of the paper is secured end-to-end data communication, basically encryption algorithms and to analyze these encryption standards to overcome the security issues as well.

Keywords: cloud providers, cloud trust issues, cloud users, trust models, encryption

1 Introduction

What does cloud computing means? Why should we trust something that we can't see? How to build the trust of the user?

These are just a few of the questions that a user or enterprise goes through when it thinks about shifting from on premises to cloud environment.

"Cloud computing is on demand delivery of compute, power, database, storage, application and other IT resources through cloud service platform via the internet with pay as you go pricing".

There is no doubt that cloud provides more benefits than on premises like trading capital expense with variable expenses, globally in minutes, cost optimization, eliminate guessing of capacity, elasticity and scalability etc.

Even though cloud provides so many advantages there are still demerits like lack of control, lack of security, lack of reputation, etc. All this leads to the lack of trust of users on the cloud services. In this paper we have built various trust models to build trust in the cloud. There are four main issues that a trust model should solve to give assurance and trust to the users. The first is the control. We all have habit, or we can say human nature of trusting things that we can see and have control of. On premises data is under our control and therefore we trust it while on cloud our data is under the control of cloud service provider or third party, this makes the user feel less in control and results in lesser trust in the cloud. The second is ownership, higher the level of ownership the more is the trust of the user. The third is the prevention, the level of trust will increase if the cloud providers provide the transparency with methods,

processes, techniques that are being used by them to protect the sensitive data of the user. The last and the most important is the security, security is the issue that all cloud providers and users are facing. It includes providing the security to the data from various attacks and maintaining Quality of service (QoS). There are various models that exist to build the trust of the consumer; we will study various techniques and methods in these models.

2 Cloud Architecture

Cloud computing is a detailed solution with many areas of vulnerabilities. Cloud Consumer is a person or organization that wants to use the cloud services and hence maintain business with cloud provider and use its services. Cloud provider is an organization that makes these services available to other organizations and various users. Cloud auditor is a third party that can conduct an assessment of cloud services and security of cloud implementation. Cloud auditor is an independent examination party. Cloud Carrier acts as an intermediate between cloud providers and cloud consumers to provide connectivity. Cloud carrier provide this connectivity through network, telecommunication and many other devices.

3 Risk and Uncertainty

Some of the risk and uncertainties are mentioned below:

3.1 Control over the data

Since the data is not stored in premises anymore, the user have no idea where the data is stored and how other sensitive data is stored on the same hardware where their data is stored. There are risk associated with it like due to improper isolation one user might able to access data of another user stored in the same hardware deliberately or unintentionally. There are other risks like Denial of service, DNS spoofing etc.

3.2 Dependency on the cloud Service providers

The data given is dependent on the cloud provider as when the data centers are affected by any reason like by natural disaster, human manipulations or by factors like downtime and maintenance of data centers it could really affect the access time.

3.3 Data Segregation

Data stored in cloud is shared among many users or systems at any time and pro- tected by different encryption algorithms. If the encryption somehow goes wrong then data integrity could be at risk.

3.4 Lack of Standardization

This indicates the differences in standards of different cloud providers. They may or may not inform users about it which may lead to uncertainty in decision-making.

3.5 Lack of Security

Security issues in the cloud are vast. Due to multi-tenancy and heterogeneous cloud resources which have been virtualized. Only security measures such as authentication and authorization are not enough to overcome the issues faced by virtual machines.

3.5.1 Shared Technology Vulnerabilities- Cloud provides high level scalability by allowing users to access shared devices by the help of hyper visor that lets guest systems

connect to host machines. This leads guest system to gain access to levels which may harm other connected systems.

3.5.2 Data Breach- Any machine can easily access the side channel timing informa- tion to guess the private keys used in encrypting the data by the help of other virtual machine in that present network.

3.5.3 DoS/DDoS- This service can affect all the users of that same network. The attacker tries to make resources unavailable by flooding the network with spam mails from either one or more sources at a time.

3.5.4Injection Vulnerabilities- Injection vulnerabilities, an attacker provides un- trusted information to the user or program which gets processed and further alters the output and execution of the program.

3.5.5 API and Browser Vulnerabilities- API are shared among users of similar cloud which is dependent on the standard policies followed by those APIs. If the policies are weak or not properly implemented then there is a security threat. 3.5.6Account hijacking- Attacks such as phishing and software exploitation are types of account hacking. These are carried out by stealing credentials.

3.6 Lack of reputation -Reputation of a company is the first line of trust for any company. When the user finds a cloud provider from different cloud service providers, he firstly analyzes it from the view of its present users, from their point of view and assessments, hence if a company lacks reputation it might not get selected in that pool of cloud service providers by a user.

4. DIFFERENT TRUST BUILDING MODELS

Trust in literature means having faith or confidence in the other person. Mapping the trust word in cloud computing we can express trust as faith or expectation a cloud consumer has towards cloud service provider to provide better and secure services. This trust can be increased or decreased according to the services provided by the cloud service provider to consumer. If consumer finds data not secure, face issues in availability and fault tolerance etc. then the trust of the consumer towards cloud might decrease. Whenever a enterprise decides to shift its existing on premises resources to cloud it evaluates the trustworthiness and confidence of cloud service providers. We can evaluate this trust using different trust models that exist. Trust models are nothing but various techniques, mechanisms and models to build the trust of cloud users in cloud service providers. Some of these trust models are deployed in the cloud computing environment to bring faith and trust of the consumer on the cloud. Increasing the trust in cloud increases the cloud usage. Some of the trust models are discussed below.

4.1 Agreement and certification based trust models

Agreement and certification model is the most common user trust based model. In the first stage of this model the user specifies all the requirements and expectation regarding elasticity, quality of services, scalability, 24X7 assistance and security. These service agreements are known as Service Level Agreements (SLA).In the second stage the model is transferred to the Cloud service provider for negotiation and better understanding of what the user is expecting from the cloud to build the trust. SLA also specifies that cloud service provider will suffer from or penalties they have to face in case of the violation of the agreement.

The main advantages include:

1 The user is able to explain or specify its expectations and needs to the cloud service provider in an easy way
2 Since there is clear specification of the user requirements, cloud service provider can focus on these requirements and build the trust of the user.
SLA gives an assurance to the customer that they can trust cloud and it services and it's totally worth to shift to the cloud platform. There are different standards and certifications that mark the quality of the problem. For example ISI mark for electronic products, ISI for gold ornaments and FPO for processed food products. Similarly we have certification like AWS is certified by ISO .All these certificates helps and increases the trust of the consumer.

4.2 Transparency based trust model

Transparency plays a very important role in cloud computing, this role is adaptability. The more transparent these cloud service providers are with their security, risk and management services, more buyers or users can put their trust on the cloud platform. Example of the trust based model is STAR which represents security, trust and assurance registry. STAR provides a full documentation on the risk, security provided by the cloud. The user or enterprise can compare these services to choose the best service for their business. Other than STAR, cloud service provider also provides CTP which stands for cloud trust protocol. Cloud trust protocol helps to establish the digital trust between the cloud providers and customers. CTP consist of 23 criteria of cloud transparency such as configurations, vulnerabilities, policy, authorization, access and many more.

4.3 Security based trust model

Cloud security is very similar to the security provided to the on-premises data but with no waste on money on the hardware and software by the user. There are many ways to secure your data. One way to secure data is store data on various data centers so that if one data center fails you still have your data secured in other data center.
Other ways to secure your data are cryptography, hashing, authentication, access control and public key infrastructure (PKI).Cryptography means the use of mathematical principles to encrypt and decrypt your in-transit or stored data whereas hashing converts your data to binary string of variable length which is called hash value. The hash value is calculated in such a way that it is collision free, pre-image resistant, deterministic and computational effective.
The cryptography can be of two types:

Symmetric cryptography is the simplest and oldest cryptography technique in which only one key is used on both the sides that is one on encryption side and other on decryption.

Asymmetric cryptography uses two keys ,these keys are known as public key and private key. The public key converts the plain text to cipher text and private key converts the cipher text to plain text.

4.3.1 Public key infrastructure

Public key infrastructure framework is build upon the two methods of encryption i.e. symmetric encryption and asymmetric encryption. PKI is the system that allows users to have secure communication over the internet by using public and private keys that are provided by certificate authority. PKI contain following elements. The Digital certificate is like an ID proof given to the user. The digital certificate differs as it can just not be issued to a person but can also be issued to software, enterprise or anything that needs an electronic identity. The digital certificate is based on the standard X.509 certificate and

issued by Certificate Authority. Certificate Authority is the one that issues the certificate .It is the responsibility of the certificate authority to make sure that the identity and information provided by the user is valid and up to date. Registration authority acts as the third party that keeps the check or makes proper investigation on the enterprise or user asking for the digital certificate. Certificate content management system is the managing authority that issues, revoke, suspend and renew the digital certificates.

4.3.2 Isolation in container based virtualization

Virtualization is one of the important features of the cloud computing .Virtualization as the name suggest is simply creating a virtual version of your storage, hardware etc. With the help of virtualization we can have various virtual machine connected to same operating system and same hardware increasing the utilization and flexibility of the system.

Multi tenancy is the central idea on which virtualization runs, so it's important that there must be a proper isolation between the virtual machine so that one virtual machine cannot interfere with another. This isolation is provided by the hypervisor.

Container based isolation is the type of virtualization to provide more isolations between the VMs and also increase the performance.

Container based virtualization provides various merits like better performance and efficiency. But it has some demerits as well like the weak isolation between the containers leads to the amplification of attacks as the attack can move one container to container. This weak kernel isolation can be harmful for the whole system since the user does not have their data stored on their own system, building trust of the user becomes an important task. To build the trust of the user, it's important to provide them the best data security and quality of service (QoS).

We can establish the trust of the user using RBAC which stands for Role Based Access Control. RBAC defines and assigns the user its roles and permissions including the security policies.

Now adding RBAC to all the individual containers the container can make decision on its own about the incoming request and moreover the host can treat each container individual and separately. This will decrease the load and minimize the decision making delay which will automatically improve availability and performance.

4.3.3 End to End Encryption

It is a system where only the end users can read the information being passed and no one in the middle can access it. It prevents eavesdropping and leakage of crucial information and hence protecting the data from attackers. In different messaging systems such as email and chats, messages go through intermediaries and are stored in that third party application from where the receiver retrieves the messages. The information is encrypted only when it is in-transit and not when storing the data in third party application. The third party application has decrypted messages hence allowing the application to search and scan within the information being transferred. Here the messages can be accessed and misused by an attacker by the help of a process called backdoor which means bypassing the authentication of a system to gain access to restricted data.

a. Identity-Based Encryption

It is a type of public-key encryption in which a user generates key from a unique identifier, this key is public key like user email address and then a third party server calculates and generates the corresponding private key from the given public key. This type of encryption decreases the complexity of whole encryption method. Some Identity based encryption algorithms are:

- Boneh-Franklin
- Sakai-Kasahara

b. Attribute Based Encryption

In attribute based encryption depending upon attributes like users country, name, his first school etc the data is encrypted. The decryption can only be done if the attributes of the cipher text and the user key match. Some attribute based encryption algorithms are:

- Key-policy attribute-based encryption
- Cipher text-policy attribute-based encryption

c. Homomorphic encryption

This encryption allows computation on the encrypted text which gives an encrypted result which when decrypted matches the result of the operations as if they were applied to the original text. This helps data to be encrypted and sent to commercial cloud environment for further processing. We can say it is a form with an addition of evaluation capability to compute over encrypted data without the need of the secret key. It can be seen as an extension to either symmetric or public key cryptography. It includes different types of schemes such as partially Homomorphic, somewhat Homomorphic, leveled Homomorphic and fully Homomorphic.

d. Data Encryption Standard

In data encryption standard only one single key is being used for both encryption as well as decryption of data. It can work on 64 bit of plain data which means 64 bit block data.It was developed in IBM in the early 1970's.

e. Rivest-Shamir-Adleman (RSA)

This algorithm is used to secure data transmission. In this the encryption key is public and the decryption key is different and kept secret. Here prime numbers are used to generate a public key and it must be kept secret. Anyone can use public key for encryption but only those can decrypt it who know the prime numbers. This algorithm is relatively slow and hence not widely used.

f. Blowfish

This is a symmetric block cipher algorithm. It is an alternative to the Data encryption standard and provides faster encryption rates than many other algorithms. It overcame many constraints related to other algorithms. The block size in blowfish is 64 bits and key size may range from 32-448 bits.

4.4 Reputation based trust model

In reputation based trust model, the trust of model is build by history of interaction that user have personally or through others people's review on the cloud services.

When the variable like performance, cost, and security remains steady or make improvement then more people build their trust on the cloud and its services. Cloud Spectators is the consulting firm that focused on the cloud industry and act as a benchmarking. Cloud Spectators provide full consulting service on strategy, planning, deployment as well as cloud migration services. Cloud spectators helps the cloud providers their position that they hold in market and what change they need to make it their strategy and services for more cost optimization. The main goal of the Cloud Spectators is to provide the users the transparency so that they can move to the cloud with trust and confidence.

4.5 Performance based trust model

Performance is also one of the most crucial part of building trust. Greater the performance, more are the cloud users. Performance can be increased by keeping in mind some basic things such as going global, this means keeping data replicated in many servers across globe which helps in faster retrieval of data and hence decreasing access

time and providing customers better experience at lower costs .Cloud also provides service like auto scaling. Auto scaling automatically maintains performance and availability with different workloads. When the demand spikes, scaling automatically increases the capacity to maintain the quality of service. We can keep check on our performance by monitoring its elastic compute cloud performance and capacity. Monitoring metrics can be used to raise the alarm when we exceed our capacity. These alarms are triggered automatically. Other reason for efficiency of cloud is use of server less architecture. With the use of server less architecture there is no need to maintain servers and spend money. With server less architecture we can experiment more often. Hence increasing the efficiency.

5. ANALYSIS

After studying these algorithms, we can analyze as follows:
The identity based encryption is a type of public key cryptography where the user gets a public key from the third party application server that uses a simple identifier similar to an email. The user then uses the key to encrypt and decrypt the electronic message. This process reduces the complexity from the encryption process at both the end, i.e. the user and the administrator. Comparing the DES and RSA algorithms, RSA algorithm takes the longest time to encrypt data as compared to DES and Blowfish. Also RSA takes the longest time to decrypt data than DES and Blowfish. RSA when compared to DES in accordance to memory used, it was found that DES uses less memory than RSA. According to the above comparisons we can say that Blowfish is better than DES and DES is on the other hand better than RSA. RSA has a number of flaws in its design and hence not used for encryption nowadays. It can be analyzed about the Homomorphic algorithm that it provides same level of privacy as any other algorithm but has one advantage that operations can be performed on the data without actually the need to see it. It provides complete privacy between user and server.

6. COMPARING THE VARIOUS TRUST MODELS

All the trust models unique roles to play to build the trust on the cloud.As the above figure we can see the initial stage to establish the trust id the reputation stage. As we know that reputation helps the person to build initial trust while taking the big step on moving the work load from on premises to the cloud environment. Cloud spectators and aws services can help the user to build this trust. The next stage is the transparency trust model , once the user have build the initial trust and know which service to be used, user needs to know about how the service will work and how the data will be stored so that data can be protected from various risk and uncertainty. After the reputation stage its security, Security trust model build the trust of the users that their data is under the safe hands. As we studied about security techniques like cryptography, PKI and SSL etc. Security is the most important criteria on which user build their trust on the cloud as data is the most important concern of the user. The last is the Agreement trust model, it acts as the agreement between the user and provider making the assurance the quality and secure service will be provided to them. Each of the trust models have some limitation but together they helps to establish trust.

7. CONCLUSIONS

Many conclusions can be established from this paper. First, even though cloud provides various services, cost optimization techniques, but it still faces risks and uncertainties. Second, the models studied in this paper need to work together for the trust to establish, if even one of them is missing, trust cannot be established. Third, reputation based trust model is the initial trust or soft trust required at the initial stage when the user plans to shift to the cloud. Data is increasing day by day at a rapid rate and hence more and more storage and security is required to keep the data safe from outside attack. Cloud computing has provided with a number or resources and that too at a lower price. It has

distributed the whole computational structure and so decreased the maintenance cost for different organizations. Data Security in cloud is a very crucial part and hence regular updates have to be made. For securing end-to-end data communication, basically encryption algorithms and standards are followed. Here we have analyzed a number of encryption standards to overcome the security issues. Major cloud service providers do not use end-to-end encryption because these services rely on their servers to process and cross-check the emails and files sent or received. Therefore the servers have access to user data. We also discussed various security threats and vulnerabilities in cloud computing such as the DoS/DDoS, Data Breach. The solution to these problems is end-to-end encryption as it encrypts data at the beginning and deciphers it only at the authorized recipients end and never at any intermediate point such as the cloud service providers. These encryption techniques can prevent any data leaks and also defend against hackers trying to make use of a point of attack

Also with more advancements and increased amount of users on the cloud platform, more new techniques and models will be required to provide security and transparency to the user.

8. REFERENCES

[1]Alabamian, I., Mackay, M., & Tso, P. (2016). Build Trust in the Cloud Computing - Isolation in Container Based Virtualisation. 2016 9th International Conference on Developments in eSystems Engineering (DeSE).

[2] Abir Awad, Sara Kadry, Brian Lee, Gururaj Maddodi, Eoin O'Meara. "Integrity Assurance in the Cloud by Combined PBA and Provenance",2016 10th International Conference on NextGeneration Mobile Applications, Security and Technologies (NGMAST), 2016

[3]Frank Joh n. K. Building trust into utility cloud computing. Ph.D Dissertations. University of Maryland
Baltimore County, 2010

[4] Anna Lena Bischoff Ethic and trust.A Literature Review on Cloud Computing Services,2017

[5] Khaled M khan and Quatibah M Muallahi,Establishing trust in cloud, Quatar University ,Press, 2010

[6] Frank. John K. et al. Introducing the Trusted VirtualEnvironment Module: A new Mechanism for Rooting Trust in Cloud Computing, Trust and Trustworthy Computing, vol. 6101, pp. 211-277, 2010

[7]Albert S. Horvath and Rajeev Agarwal,Trust in Cloud Computing, Computer Systems Technology, North Carolina A&T State University, Greensboro, USA,2015

[8] M. Carroll, A. Van der Merwe, and P. Kotze, "Secure cloud computing: Benefits, risks and controls," Information Security South Africa (ISSA), IEEE, August, 2011

[9]P. I. Bhosle, S. A. Kasurkar, "Trust in Cloud Computing", International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), vol. 2, no. 4, pp. 1541-1548, 2013.

[10] Dimitrios Z and Dimitrios, L. Addressing cloud computing security issues, Future Generation Computer Systems. Vol. 28, no. 3, pp. 583-592, 2010

[11]Talal H. Noor, Quan Z. Sheng, Zakaria Maamar, Sherali Zeadally,Managing trust in the cloud: state of the art and research challenges,vol. 49,2016

[12] S. Pearson, and A. Benameur, "Privacy, security and trust issues arising from cloud computing." Cloud Computing Technology and Science (CloudCom), IEEE, 2010

[13]F. Yahya1 , V. Chang2 , R.J. Walters1,Security Challenges in Cloud Storage, Int. J. Emerg. Technol. Adv. Eng., vol. 4, no. 2, pp. 1–6, 2014.

[14]M. Haghighat, S. Zonouz, & M. Abdel-Mottaleb (2015). CloudID: Trustworthy Cloud-based and CrossEnterprise Biometric Identification. Expert Systems with Applications, 42(21), 7905–7916