Available online at www.elixirpublishers.com (Elixir International Journal)

Computer Engineering

Elixir Comp. Engg. 98 (2016) 42718-42722

ISSN: 2229-712X

Cloud Computing

Anchal Jain and Srishti Aneja

ARTICLE INFO

Article history:
Received: 4 August 2016;
Received in revised form:
17 September 2016;
Accepted: 27 September 2016;

Keywords
Cloud computing,
Services,
Computing,
Virtual machine (VM),
Security.

ABSTRACT
Cloud computing is the emerging technology in IT industry Cloud Computing helps the startup companies to implement their ideas and grab opportunities without worrying about the capital needed to start their Business plan. It is built on the concept of virtualization, utility computing, networking and Autonomic computing. The aim of this paper is to provide better understanding of the security challenges of cloud computing and analyze the research direction in this widely used technology affecting people. In this paper, we present the prospect of cloud computing, its architecture and pros and cons of Cloud Computing.

Introduction

Cloud computing is introducing many huge changes to people's lifestyles and working patterns. Cloud computing simply means 'internet computing'. The term cloud refers to sharing of computing resources over the internet. It appears to have its origin in networks, providing different services and application over the internet so that instead of keeping data on your own hard drive or updating applications cloud helps in storing information at remote location .

It allows individuals and IT sector as a whole to use software and hardware that are managed by third parties at some other places. By using Cloud computing, users can access their database at any time and from anywhere without worrying about management of resources Any phone, tabs ,laptops ,iPad or any other PDA can be connected to cloud if it is connected over the internet.

The Cloud Computing foundation is-as-a-service usage model, service oriented architecture (SOA) and virtualization of software and hardware. Service consumers use 'what they need on internet' and 'pay only for 'what they use'.

The resource sharing at various levels results in various cloud offspring such as

1. Infrastructure Cloud (E.g.: hardware IT infrastructure management)
2. Software Cloud(E.g.: SAAS focus on middleware as a service)
3. Application cloud (E.g.: Application as a service ,UML modeling tool as a service)
4. Business Cloud (BAAS)
5. ABSTRACT
6. Cloud computing is the emerging technology in IT industry Cloud Computing helps the startup companies to implement their ideas and grab opportunities without worrying about the capital needed to start their Business plan. It is built on the concept of virtualization, utility computing, networking and autonomic computing. the aim of this paper is to provide better understanding of the security challenges of cloud computing and analyze the research direction in this widely used technology affecting people from all walks of life.
7. In this paper, we present the prospect of cloud computing, its architecture, and pros and cons of Cloud Computing.

Definition

A large scale distributed computing paradigm i.e. driven by economies of scale, in which a pool of virtualized dynamically managed computing power storage platform and services are delivered on demand to customers over the internet.

1.1 Types of Clouds

Deploying cloud computing can differ depending on requirements .Following are the types of cloud:

1. Private Cloud- It is also known as internal cloud .It is designed for single organization .[1]The cloud can be built and managed by the same organization or any other external third party on the premise.
2. Public Cloud - Cloud that can be used by public. It is owned by large companies like Google, Amazon. It is Pay per use service and enables a customer to develop and [2] deploy a service in cloud but it is less secure.
3. Community Cloud- It is shared by several organizations and setup for their requirements. It may help in reducing capital investment and having same deployment characteristics as private cloud.
4. Hybrid Cloud- It is the combination of all three models. It is more flexible and provides tighter control and security over application data, while still facilitating on-demand service. It can be managed, owned, located at both organization and third party side.

1.2 Advantages

1. Dynamically scalable: Users have to consume the amount of online computing resources according to the requirement. Any application would just obtain as many as few resources from cloud as required in a particular point in time.

Tele:
E-mail address: anchaljain14@gmail.com

2. Device independency: Cloud computing resources can be accessed from any computer on the internet. Any type of computer, be it a traditional desktop, smart phone, e book reader etc. It only has to have an internet connection and a browser.
3. Task Centric: The cloud usage model is based on the user's task rather than any particular software, hardware or network infrastructure. Users do not have to purchase or install any software before using a cloud computing resource.
4. Charged on usage basis: cloud computing do not have fixed cost but variable cost which is due to the dynamically scalable and task centric characteristics. Due to fixed initial cost, cloud computing suppliers including Clarizen, NetSuite, Salesforce etc. allow companies of all sizes to the latest type of business application.[3]

1.3 Disadvantages

1. Security- When using a cloud computing service, you are essentially handing over your data to a third party and users from all over the world, are accessing the same server can cause a security issue. some servers like Google Cloud Connect come with customizable spam filtering as security measure.
2. Privacy- Cloud computing lacks in authenticating the users who will be accessing the information. To protect against this , cloud computing services offer password protection using data encryption technology.
3.Loss of Control- This includes not only how much you have to pay to use the service, but also what information you can store, from where you can access it and some other factors. You depend on the provider for updates and backups. If for some reason, their server ceases to operate, you run the risk of losing all your information.
4.Internet Reliance- Internet access is still not available everywhere yet. If the area that you are in doesn't have Internet access, you won't be able to open any of the documents you have stored in the cloud. [4]

2. Cloud Architecture

Cloud computing is modular where each level performs individually. It allows wide range of application requirements while reducing management and maintenance overhead.

Architect of cloud computing environment can be divided into 3 layers-application layer, platform layer and infrastructure layer.

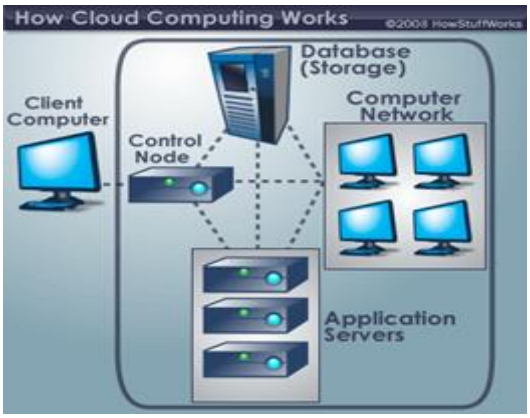
1. Infrastructure layer-it is also called as virtualization layer .it partitions the physical resources using virtualizations technique and transforms into pool of storage and resources .
2. Platform layer-it is above application layer consisting of application frameworks and operating system. It minimizes the load of deploying an application directly into VM container.
3. Application layer-it is topmost level in hierarchy, containing cloud applications which are more efficient fast and economical. [5]

2.1 Business model

Cloud computing builds a service driven business model which means platform level services are provided 'as-a – service' on demand basis. It works on 'pay-per-use' model.

2.2 Services

Cloud offer services that can be categorized as –software as a service (Saas), platform as a service (Paas), infrastructure as a service (Iaas).



1. Infrastructure as a service – (Host)-It is the lowest service model offers. It provides software such as storage, firewall that can be customize according to customer needs and can deploy his own operating systems and middleware. Examples of Iaas providers-Amazon EC2, Microsoft Dynamic CRM, Go Grid.
2. Platform as a service-(Build)-It is above Iaas layer where applications are developed using programming languages and tools. Paas refers to providing platform layer resources e.g. database, language execution environment, and web servers Consumers purchase access to its platform enabling them to deploy their own applications in cloud. Examples of Paas providers-Salesforce's CRM, IBMBlueMix.
3. Software as a service-(Consume)-It is the topmost service on cloud where users simply use web browser to access softwares that others have deployed and use services. Users donot have any control over the infrastructure and it is invisible for the customer. Application is offered as a service like web services, Email, games over the internet.

Examples of Saas providers-Zoho, Gmail. [6]

3. Different Computing

3.1 Grid Computing

It is a form of distributed computing which is collection of computer resources from multiple locations which are geographically dispersed to reach a common goal.. Cluster of computer constitutes a *grid* that enables access to shared computing power and storage capacity from your desktop. Grids are an open source technology.

Grid Computing takes the idle processing power of various computing units (or nodes that are loosely linked by the Internet or low-speed networks to do a job. The job itself is controlled by one main computer, and is broken down into multiple tasks which can be executed simultaneously on different machines. As the tasks complete on different computing units, the results are sent back to the controlling unit, which then compares them forming a combine effective output. [7]

Grid Computing differs from Cloud Computing by providing a complete server infrastructure but not applications and is less security. Cloud offers more services than grid computing. In fact almost all the services on the Internet can be obtained from cloud, e.g. web hosting, multiple operating systems, DB support and much more. Grids tends to be more loosely coupled and geographically dispersed compared to conventional cluster computing systems. Cloud computing goes one step further with on-demand resource provisioning. This eliminates over-provisioning when used with utility pricing. It also removes the need to over-provision in order to meet the demands of millions of users. Server computers are still needed to distribute the pieces of data and collect the results from participating clients on grids. [8]

3.2 Utility Computing

Utility computing is also known as Computer Utility. It is a model in which a service provider makes computing resources and infrastructure management available to the customer when needed, and charge them according to usage at the end of month just like an electricity bill. It is a type of on-demand computing the utility model maximizes the efficient use of resources and minimize associated costs. This model has the advantage of a low or no initial cost to have access to computer resources. Through utility computing companies which lack in resources can have efficient CRM program. [9]
"Utility computing" has some form of virtualization so that the amount of storage or computing power available is considerably larger than that of a single time-sharing computer. Multiple servers are used on the "back end" to make this possible.

Utility computing is an implementations of cloud computing .It does not require Cloud computing and it can be done in any server environment .It is economically inefficient when applied on a smaller scale ,so it is most often applied on cloud hosting where large resources are being managed.

Utility computing has direct access to third party services ,business are aware of source of services they are leasing in contrast in cloud computing company knows less about source of services and involves grid computing that supports multiple task at once so it is more powerful because utility computing relies only on a single source

Utility computing uses traditional programming approach whereas cloud uses virtual environment to benefit programmers and developers. Cloud computing has faster access on CRM over utility computing. [10]

3.3 Autonomic Computing

Recently, many of the concepts in computer world have been devised out of our biological systems. One of them being, autonomic computing by IBM [18]. It is a self-managing computing environment that completely hides its complexity, thus providing the user with an interface that exactly meets his/her needs. It has a true analogy with how the human system works. A human has a self-protecting and a healing system. Similarly, the autonomic systems have been designed to protect itself from any unauthorized access from anywhere and provide solution to the problems dynamically without any user intervention. The concept has been promoted by IBM. In fact, IBM has been putting an effort for open standards on autonomic computing and has distributed a document by the name of "A blueprint for building self-managing systems," along with associated tools to help put the concepts into practice.[11]

The goal of autonomic computing is to create systems that run themselves, capable of high-level functioning while keeping the system's complexity invisible to the user. In accordance to cloud computing, the main target is to lower the resource cost than to reduce system complexity. It involves four major areas:

1. Self-Configuration: Automated configuration of components and systems follows high level policies. Rest of the system adjusts automatically.
2. Self-Protecting: This involves anticipating identifying and protecting against attacks from anywhere.
3. Self-Optimizing: Monitoring and tuning the resources automatically with support for operating in unpredictable environments.
4. Self-Healing: Autonomic problem determination and resolving it accordingly.

Cloud Computing focuses on the storage and working of the services that has to be provided keeping in accordance with the resources that are being used.[12] Whereas, autonomic computing is a technique that supports cloud services in case there are any faults from which it has to recover on its own. It could simply be seen as an analogy to the "fault tolerance" mechanism for cloud computing. [13]

3.4 Virtualization Computing

Virtualization has been around in many forms for much longer than some realizes, things like Logical partitions (LPAR) on IBM Mainframes have been around since the 80's and have been extended to other non-mainframe platforms. Networks have been virtualized by creating VLANs for years. The main goal of virtualization is to manage workloads by radically transforming traditional computing to make it more scalable. Virtualization has been a part of the IT landscape for decades now, and today it can be applied to a wide range of system layers, including operating system-level virtualization, hardware-level virtualization and server virtualization.

Virtualization in all of its forms is a pillar of Cloud Computing especially in the private/internal cloud architecture. In simple terms, the ability to divide a single hardware device or infrastructure into separate logical components. Virtualization is key to building cloud based architectures because it allows greater flexibility and utilization of the underlying equipment. Rather than requiring separate physical equipment for each 'Tenant' multiple tenants can be separated logically on a single underlying infrastructure.

The most common server virtualization allows a single physical server to be divided into logical subsets by creating virtual hardware, this virtual hardware can then have an Operating System and application suite installed and will operate as if it were an independent server.

Server virtualization provides many benefits but the key benefits to cloud environments are:

i) Increased server utilization, and operational flexibility.
ii) Increased utilization means that less hardware is required to perform the same computing tasks which reduce overall cost.

The increased flexibility of virtual environments is key to cloud architectures. When a new application needs to be brought online it can be done without procuring new hardware, and equally as important when an application is decommissioned the physical resources are automatically available for use without server repurposing. Physical servers can be added seamlessly when capacity requirements increase. [14]

4. Security

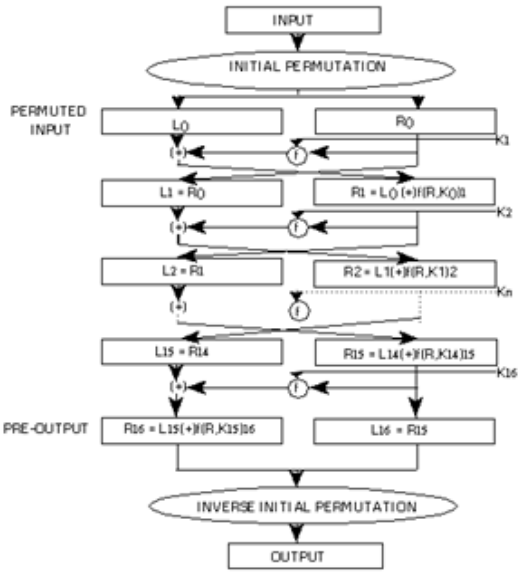
4.1 Working

4.1.1DES Working

The Data Encryption Standard is a block cipher, meaning a cryptographic key and algorithm are applied to a block of data simultaneously rather than one bit at a time. Encryption of a block of the message takes place in 16 rounds. From the input key, sixteen 48 bit keys are generated, one for each round. In each round, eight so-called S-boxes are used. These S-boxes are fixed in the specification of the standard. Using the S-boxes, groups of six bits are mapped to groups of four bits. The contents of these S-boxes have been determined by the U.S. National Security Agency (NSA).[20] The S-boxes appear to be randomly filled, but this is not the case.

The block of the message is divided into two halves. The right half is expanded from 32 to 48 bits using another fixed

table. The result is combined with the sub key for that round using the XOR operation. Using the S-boxes the 48 resulting bits are then transformed again to 32 bits, which are subsequently permutated again using yet another fixed table. This by now thoroughly shuffled right half is now combined with the left half using the XOR operation. In the next round, this combination is used as the new left half .[15]



In the figure, the left and right halves are denotes as L0 and R0, and in subsequent rounds as L1, R1, L2, R2 and so on. The function f is responsible for all the mappings described above.

DES uses a 64-bit key, but eight of those bits are used for parity checks, effectively limiting the key to 56-bits. [16]

4.1.2 RSA Working

RSA is named after Ron Rivest, Adi Shamir, and Leonard Adleman .RSA is one of the public-key cryptosystems and is widely used for secure data transmission. In such a cryptosystem, the encryption key is public and the decryption key is kept private. Messages encrypted with the public key can only be decrypted using the private key.

The RSA algorithm involves four steps:

Key generation, key distribution, encryption and decryption.

e, *d* and *n* are large positive integers such that with modular exponentiation for all *m*:

$$(m^e)^d \equiv m \pmod{n}$$

Key distribution

To enable Bob to send his encrypted messages, Alice transmits her public key (*n*, *e*) to Bob via a reliable route. The private key is never distributed.

Encryption

Suppose that Bob would like to send message *M* to Alice. He first turns *M* into an integer *m*, such that $0 \le m < n$ and $\gcd(m, n) = 1$; i.e., *e* and $\varphi(n)$ are co prime. He then computes the cipher text *c*, using Alice's public key *e*, corresponding to

$$c \equiv m^e \pmod{n}$$

Decryption

Alice can recover *m* from *c* by using her private key exponent *d* by computing

$$c^d \equiv (m^e)^d \equiv m \pmod{n}$$

Key generation

The keys for the RSA algorithm are generated the following way:

1. Choose two distinct prime numbers *p* and *q*.
2. Compute $n = pq$.
   - *n* is used as the modulus for both the public and private keys. It is the key length.
3. Compute $\varphi(n) = \varphi(p)\varphi(q) = (p-1)(q-1) = n - (p+q-1)$, where φ is Euler's totient function. This value is kept private. Choose an integer *e* such that $1 < e < \varphi(n)$ and $\gcd(e, \varphi(n)) = 1$
4. Determine *d* as $d \equiv e^{-1} \pmod{\varphi(n)}$; i.e., *d* is the modular multiplicative inverse of *e* (modulo $\varphi(n)$)

The *public key* consists of the modulus *n* and the public exponent *e*. The *private key* consists of the modulus *n* and the private exponent *d*. *p*, *q*, and $\varphi(n)$ must also be kept secret because they will be used to calculate *d*. [17]

Key Generation	
Select p, q	p, q both prime, p≠q
Calculate n = p×q	
Calculate $\phi(n) = (p-1)\times(q-1)$	
Select integer e	$\gcd(\phi(n),e) = 1;\ 1<e<\phi(n)$
Calculate d	
Public key	KU = {e, n}
Private key	KR = {d, n}

Encryption	
Plaintext:	M < n
Ciphertext:	$C = M^e \pmod{n}$

Decryption	
Ciphertext:	C
Plaintext:	$M = C^d \pmod{n}$

4.2 Security Issues

Security issues fall into two broad categories:

- Security issues faced at cloud side (organizations providing software-, platform-, or infrastructure-as-a-service via the cloud) and
- Security issues faced at customer side (companies or organizations who host applications or store data on the cloud).

Most security problems arise from:

1. Consumer's loss of control

– Data, applications, resources and other details are with the provider

– User identity (Authentication), User access control rules (Authorization) are managed by the cloud provider.

2. Lack of trust

– Trusting a third party requires taking risks so hard to balance trust and risk.

– Consumer relies on provider to ensure for Data security and privacy.

3. Multi-tenancy

- Conflict between tenants' opposing goals [18]

5. Proposed System Design

This proposed system uses AES & RSA algorithm to generate encryption when user data is in database in Cloud Storage and inverse AES & RSA algorithm to generate decryption when user download file from Cloud Storage, for increasing security.. The proposed system design focuses on the high security.

1) For Encryption

- Implementing the AES algorithm of Encryption to generate first level encryption.
- Implementing the RSA algorithm of Encryption to generate second level encryption
- Store Cipher Text into Database.

2) For Decryption

- Implementing the RSA algorithm of Decryption to generate first level decryption
- Implementing the AES algorithm of Decryption to generate Plain text.
- Display Plain Text to User

We have taken a combination of algorithms like: AES and RSA. AES (Advanced Encryption Standard) is a symmetric key algorithm, in which a variable key is used for both encryption/decryption of data. Whereas RSA is an asymmetric key algorithm, the algorithm that uses different keys for encryption and decryption purposes.

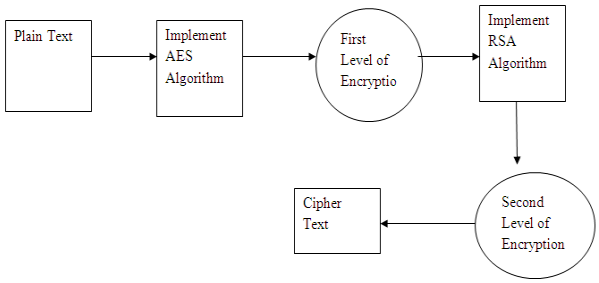


Diagram of Multilevel Encryption.

Conclusion

Information technology landscape has been completely changed with the introduction of cloud computing. It is booming as a strong supporting aspect of IT for managing and delivering services over the Internet. But with the advantage, comes great challenges for the researchers. With cloud computing in concern, there are areas that still need to be realized more of its potential like automatic resource usage, power management and security management in cloud. In this paper, we have surveyed the complete architecture of cloud computing, it's working including security concerns, key technologies as well as research directions. As the development of cloud computing technology is still at an early stage, we hope our work will provide a better understanding of challenges of cloud computing and help in other related researches.

References

[1] International Journal of Engineering Science and Innovative Technology 2012
[2] http://aws.amazon.com
[3] http://explainingcomputers.com/cloud.html
[4] http://www.moneycrashers.com/cloud-computing-basics
[5] Cloud computing state of the art and research challenges Journal
[6] https://aws.amazon.com/types-of-cloud-computing
[7]http://www.cloud-lounge.org/clouds-and-grids-compared.html
[8]http://www.brighthub.com/environment/green-computing/articles/68785.aspx
[9] https://en.wikipedia.org/wiki/Utility_computing
[10]http://cloudbyuchit.blogspot.in/2012/03/difference-between-cloud-computing-and.html
[11]http://whatis.techtarget.com/definition/autonomic-computing
[12] https://en.wikipedia.org/wiki/Autonomic_computing
[13] http://www.webopedia.com/TERM/A/autonomic_computing.html
[14] http://www.definethecloud.net/virtualization
[15] http://page.math.tu-berlin.de/~kant/teaching/hess/krypto-ws2006/des.htm
[16]http://www.iusmentis.com/technology/encryption/des/
[17] https://en.wikipedia.org/wiki/RSA_(cryptosystem)
[18] Anya-kim-bhargava-MCC workshop ppt