Cloud Computing Architecture And Applications Security

Waleed T. Al-Sit

Abstract: Cloud computing is developed to tackle storage limitations and information security. It's being considered as a new computing paradigm that offers dynamic and flexible resource allocation. Business owners have become more attracted in the possibilities of using cloud computing because it increases the reachability of their services and reduces the need for physical resources. In this paper, the cloud computing architecture is described with a brief actors' roles based reference model. This model allows the stakeholders to understand the overall view of functions, activities, and responsibilities to evaluate and assign the risk of services. At the end of this work, several open researches for security applications is concluded and discussed.

Index Terms : Cloud computing, Cloud architecture, NIST, Reference model, 3DES, AES, Security applications.

1. INTRODUCTION

Cloud computing presents the next generation of highly scalable distributed systems. In cloud technology, the data is stored and accessed by the internet rather than computers hard disk, that means moving the data from the physical device such as portable personal computers in a large data center — many technologies used in cloud computing, such as virtualization, web services, and multi tenancy. The goal of cloud computing is to provide virtualized services to the costumers. Elasticity enables the system [1] to provision and de-provisioning the resources automatically. That means the available resources match the current service demands. Multi tenancy enables a group of users to share common access to the same service. These characteristics concentrate on improving services availability, cost, and resource utilization. The NIST cloud computing reference architecture (CCRA) presented in this paper is the complement to the NIST cloud computing definition. It is a standard high-level conceptual model which defines a set of actors, activities, responsibilities, and functions that can be used in the process of developing the requirements, structures, and operations of cloud computing. Cloud computing can be considered a new computer technology that has a lot of benefits. One of the main benefits is cost-efficiency. In cloud computing, the clients do not need to use high-precision devices to run their applications online. Also, the users can access the information at any time and from anywhere. Cloud computing supports the backup service, that means the client can get the last version of the data without paying. As cloud computing provides different benefits, but the security still one of the major challenges also the ability of the applications and the services access without internet.

2 CLOUD COMPUTING DEFINITION

Many technologies are used in cloud computing to provide different services to the end-users. The National Institute of Standards and Technology (NIST), is known for its quality of information technology work.

- *Waleed T. Al-Sit: Department of Computer Engineering, Mu'tah University. Al-Karak-Jordan.*
- *E-mail: w_sitt@hotmail.com*

The definition of NIST [2] for cloud computing is accepted. NIST defines the cloud as a 3 model of service provisioning. The definition model is shown in Fig. 1. MaiFnly the model can be considered as essential characteristics, service models, and deployment model. Each one of them will be presented below in light of NIST definition.

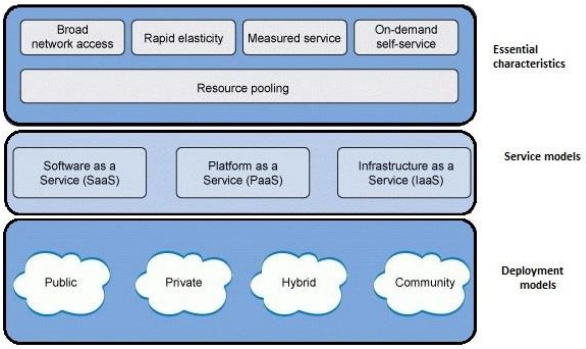

***Fig. 1**. NIST definition of cloud computing [2]*

The essential characteristics of cloud computing can be presented as five main keys are presented below[3]: On-demand self-service: the services can be requested and managed from the cloud without the interaction with the service provider. The provision of the computing capabilities is accomplished when required automatically.A broad network access: the standard mechanism used to enable the user services and application to be accessible to the customers. The availability of the services should be heterogeneous using thin and thick clients.

- Resource pooling: The resources are shared to serve different costumers using multi-tenancy model. The mapping between the physical and the virtual resources provided to the end-user.
- Rapid elasticity: The resources are scaled-down and up as required. The current service matches the available resources.
- Measured service: Up-down scaling for the resources is automatically performed as well as controlling the resource usage by provisioning a metering ability for different kinds of services provided by the cloud.

A. SERVICE MODELS

- The NIST classifies the cloud computing services into three categories, as shown in Fig. 2. The service models referred to as an SPI model (software, platform, and infrastructure).

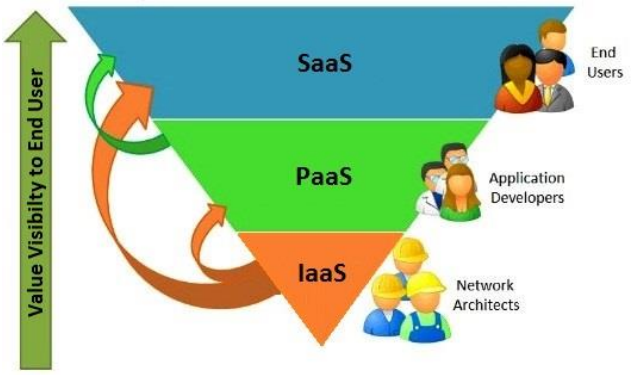

Fig. 2. *Services Model*

- The fundamental services [4][5][6]are presented below
- Software as a service: is the delivery of the service, to the customer over the network (public or private network). The customer remains unwired about the infrastructure that is used in the backend. The customers cannot create an application. However, the service provider manages the services and responsible for the access and the performance of the applications.
- Platform as a service: The customers can create their applications using the provided tools. The provider tools include the operating system, programming languages, and the integrated development environment. These tools allow the end-user to build, test, and deploy the application. The customer can manage only the deployed application but have no control over the cloud infrastructure such as operating system storage and the network.

B. Deployment Models

The cloud computing services and applications can be deployed over different types [5][6][7] of delivery models as shown in Fig. 3.

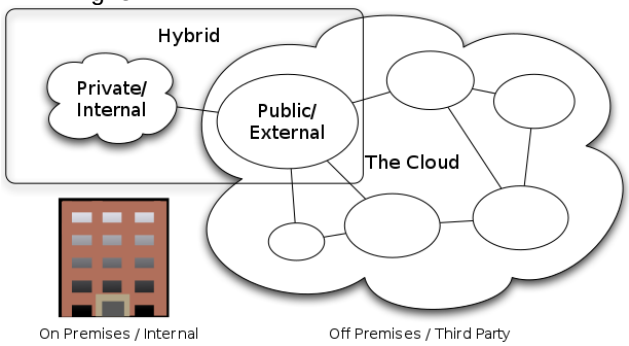

Fig. 3. *Cloud Computing Types*

The deployment models include four models that are presented below:

- Public cloud: The cloud infrastructure can be available and accessible for multiple customers. Usually, the cloud computing services provided through the internet connection. The resources are dynamically allocated through the web application, but the resources are controlled and managed by the service provider. It's located at an off-site location. Public cloud can provide multiple benefits such as the location is independent, that means the service can arrive whenever the customer requests over the internet, cost-effective, and pay on demand. But one of the fears is security for the public cloud is open to all.
- Private cloud: The cloud is available for only one organization. All the resources in this cloud are accessible for only the costumers that belonged to the organization. Private clouds provide more security than the public cloud since the access is limited. But the private cloud has high cost compared with a public cloud.
- Community cloud: community cloud means that the cloud is shared by more than an organization; these organizations have shared exciting topics such as security requirements and policy. One of the organizations or third party can manage the community cloud. The community cloud minimizes the cost associated with the private and the risks of the public cloud.
- Hybrid cloud: Hybrid cloud is a mix of multiple clouds to present a unique entity, also can be named as multiple cloud system. After getting this combination, the services and the data can be easily moved among the different deployment models.

3 CLOUD COMPUTING ARCHITECTURE DEFINITION

Cloud Computing Architecture is the structure of the system, which is based on the needs of end-user and includes the set of actors required for cloud computing. The main objectives are provided by the design of the NIST cloud computing reference architecture which (i) provide a technical reference to USG agencies and other consumers to understand, discuss, categorize, and compare cloud services (ii).described various cloud services in the context of an overall cloud computing conceptual model and (iii) facilitate the analysis of candidate standards for security, interoperability, and portability and reference implementations. The Conceptual Reference Model [8] described the architecture of the five actors standards cloud consumer, cloud provider, cloud broker, cloud auditor, and cloud carrier. Also contains their roles, activities, responsibilities, and functions in cloud computing. The conceptual reference model in details is presented below:

A. CLOUD CONSUMER

Cloud consumer is an organizer that finds, evaluates, purchase, and uses the service from a cloud provider. A cloud consumer request the function sets up of service contracts with the cloud provider, and maintain the appropriate service. The cloud consumer may be billed for the service in advance so that he needs to arrange payments accordingly [9]. Service level agreements (SLAs) are agreements signed between a service provider and another party, such as a service consumer, broker agent, or monitoring agent. Cloud computing provides different services to a cloud consumer

according to the service requested, whether it is software, platform, or infrastructure as the following services:

- SaaS Consumer: provides ERP, Human Resources, Social media, Financials, Content Management, Email, and Office Productivity, Document Management, Collaboration, CRM, Sales, and Billing.
- PaaS Consumer: provides Application Deployment, Integration, Development and Testing, Business Intelligence, and Database.
- IaaS Consumer: provides Services Management, Platform Hosting, Compute, Backup and Recovery, CDN, and Storage.

B. CLOUD CONSUMER

Cloud provider or organizer provides an available service for requesting by managing computing infrastructure required for various services and managing cloud programs. There were many developments to evaluate the cloud provider's transparency of the security, also the privacy, and the service level of competencies via its self-service such as the web publications, then to empirically evaluate cloud service providers [10]. Cloud Provider's activities represented in five main areas such as; service deployment, service orchestration, cloud service management, security, and privacy, as shown in Fig. 4, these components are used for managing and providing cloud services.

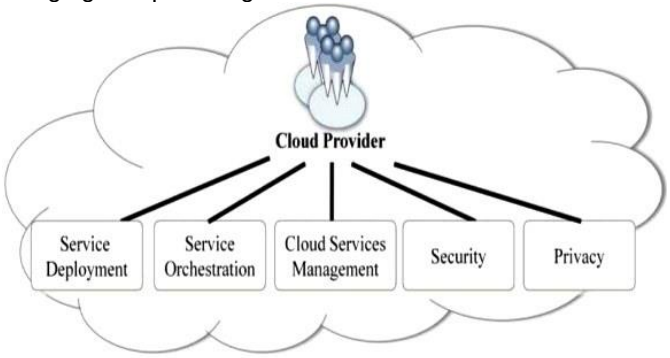

Fig. 4*. Major activities of Cloud Provider [8]*

C. CLOUD BROKER

Cloud broker manages the performance and uses of cloud services and intermediation between cloud consumers and cloud providers. In general, a cloud broker has the ability to provide services in three categories (i) Service Intermediation (ii) Service Aggregation, and (iii) Service Arbitrage. In the first one, a cloud broker improves a given service and provides value-added services to cloud consumers. According to these enhancements, we can manage access to cloud services, identity management, enhanced security, performance reporting, and other services. In the second category, cloud broker combines and integrates multiple services into one or more new services. The broker can provide the information to integrate and ensure the security of the provided information movement between the cloud consumer and many cloud providers. A broker in third category can choose services from multiple agencies based on the aggregation and intermediation clouds between cloud service providers and service customers to help negotiate the complexities of cloud services. In general, service arbitrage is the practice of buying something to resell immediately at a profit[11] [12].

D. CLOUD AUDITOR

A cloud auditor takes all responsibility of conducting an independent evaluation of cloud services. The assessment of a cloud provider service can be made by using information system operations, privacy impact, performance, and security controls of the cloud implementation [13]

E. . CLOUD CARRIER

An entity provides connectivity and transport of cloud services between cloud consumers and cloud providers via accessing points; network, access device, telecommunications, and other access devices [14]. Distribution can be provided by network and telecom carriers or a transport agent who provides the physical transport of storage media such as high-capacity hard drives. Carrier clouds can be set up as public, private, or hybrid clouds, and In general, it might be required to provide dedicated and encrypted connections.

4 CLOUD APPLICATIONS

Cloud computing covers a wide range of small business applications [7]. It serve users and keep abreast of technological developments as follows.

A. Customer Relationship Management (CRM)

Social Customer Relationship Management (Social CRM) is a new customer relationship strategy based on management interactivity and collaboration provided by the emergence of Web 2.0 and Big Data Technologies [15]. The main benefit of CRM is to enhance customer participation and satisfaction. The implementation of Social CRM is a complex task that involves different organizational, human, and technological aspects like SalesForce.

B. Business Continuity Management (BCM)

Business Continuity Management (BCM) is a strategy to improve organizational performance by managing the process, resources, and systems in the environment. Also, it manages addresses connecting, planning, and controlling the various elements in the business application event during or after of the crisis or disaster. BCM involves in various applications such as information/data, communication, technology, process, etc.

C. Email and Instant Messaging (IM)

Instant Messaging (IM) is a type of online chat such as text transmission, chat messages, photos, and video clips over the Internet. Its services such as AIM, MSN Messenger, Google Talk, and WhatsApp revolutionized the way people communicate with each other A LAN messenger operates similarly over a local area network. In general, the short messages are sent between two clients when the client chooses to complete and select "send." Some IM applications can use push technology to provide real-time text, which transmits messages character by character, as they are composed. Many messaging allows the user to attach files, clickable hyperlinks, and Voice over IP.

D. Business Accounting Systems

The business accounting system software is similar to traditional, on-premises, or self-install accounting software, only the accounting software is hosted on remote servers, similar to the SaaS (Software as a Service) business model. Data is sent into "cloud" where it is processed and returned to the user. All application functions are performed off-site, not on the personal desktop. Cloud computing allows the clients to access many software applications through the Internet,

also by other networks such as the cloud application service provider. It allows the system to install and maintain software on different desktop computers. It also allows a participant from other departments remotely accessing the same data and the same version of the software by security authentication. QuickBooks and Peachtree [16] are such examples of the business accounting system.

E. **Office Productivity**

Office Productivity can be considered as one of the main categories of office application programs. These programs help customers to produce things such as documents, worksheets, and databases. Many productivity applications are intended for business use, as mentioned in a previous application. There are many examples of office productivity software such as word processors, database management systems (DBMS), and graphics software. The definition of productivity software is extended to several type applications that are used to help people do their jobs, including collaboration, coordination, and communication programs. Almost known examples are MS Office and Office 365.

F. **Google**

There are many applications provided by Google as a web-based software suite within its Google Drive service. There are many educational applications available such as Gmail, Google Calendar, Google Classroom, Google Docs, Google Drive, etc. All Google applications are compatible with the user's demands.

G. **Line-of-Business Applications**

Line-of-business (LOB) is an application that describes the products or services offered by a business or manufacturer. A company that manufactures solid-state disk drives, for example, might claim their LOB is data storage. It is one of the sets of critical computer applications that are vital to running an enterprise. LOB applications are usually large programs that contain a number of integrated capabilities and tie into databases and database management systems; there are much recent research into LOB such (E-solution for Next Line of Business and Education using Cloud Computing) [17]. Line-of-Business

H. **Online Storage Management**

Cloud storage is a cloud computing online space in which data is stored on remote servers accessed from the internet; it saves a backup of the files on physical storage devices. It is controlled and managed by the cloud storage service provider that resides on storage servers. In addition, cloud storage providing security for storing the data; it is the best solution for the large network and big data having full tools for managing the virtual cloud storage [18]. There are many cloud storage providers, some of the most known names include: Amazon drive, Google drive, Apple cloud, One Drive, Next Cloud, and Backblaze.

I. **Communications and Collaboration Applications**

Cloud collaboration is a type of enterprise collaboration providing integrated voice, video, data, messaging, conferencing, mobility, and other communications that help users plan and share tasks, sync on projects and communicates more efficiently. Users use a cloud-based collaboration platform to share, edit, and work together on projects. Cloud collaboration enables working as groups on a project simultaneously. The most popular examples of collaboration tools [19] are; confluence, real-time board, G Suit, online calendar, time tracker, Spreadsheet, and for communications tools; voicemail, instant messages (IM), VoIP (voice over IP), etc.

J. **Medical Imaging and Urgent Care**

Cloud is used as a solution for medical data and image management; providing flexibility, scalability, effectively cost storage and modern options with a highly interoperable of medical imaging and progress for health care providers. The cloud has different tools for medical groups & urgent care, such as; Am bra Health CMO [20], Mini Peiris, and Account Executive Mark Grenga, highlighted are the main innovative cloud applications.

5 CRITICAL CLOUD APPLICATIONS PROTECTION METHODS

Healthcare data hosted within the cloud is one of the particular applications of the cloud and influential trend in the healthcare industry due to the availability of patient's health history especially during emergency interventions, punctuality, and economics of data management. It aims toward accessing any healthcare information no matter when or where beside data generated must not only be stored but must also be achieved for several years. As per the Health Insurance Portability and Commutability Act (HIPAA) requires healthcare providers to keep the records archived for at least six years after discharge [21]. With the advance in information and communication technologies, healthcare is a data-intensive domain in the last decade where a large amount of data is accessed daily, disseminated, and stored. For example, when a patient undergoes a test, a result will be stored at the hospital and might need to be accessed by another hospital within the network. Thus, the quality of care for a patient will be enhanced by efficiently allocating medical information. Health records can be in electronics forms called EMRs (Health Electronics Records), it contains clinical data related to the patient and its stored by the healthcare provider. The following list is some cases where cloud computing can bring value to healthcare data:

- Enterprise Recourse Planning system (ERP).
- Hospital-based Electronic Health Records (EHRs).
- Personal Health Records (PHRs).
- Patient Accounting and financial system.
- Community-based health information sharing.
- Integrated Delivery Networks (IDN).
- Ambulatory HER and practice management.

To manage all medical records, Health Information System (HIS) are responsible to store the records, and create new ones. It is capable of describing the information as a GUI (Graphical User Interface) or a web service. There is a need to share the EMRs between the hospitals both internally or externally for a given country. Accordingly, EMRs need to formalize their data structural. However, in order to share the data in real-time regardless of the graphical locations, cloud computing is a potential solution. Is in spite of that, there are new risks to use cloud computing with healthcare data, such as [22]:

1) Security and malicious intrusions
2) Transparency in a cloud environment
3) Possibility of cloud supplier bankruptcy
4) Customer financial model is compatible with the cloud.

5) Incompatibility of the cloud with service management
6) Privacy risks, non-complaint with privacy rules, identity disclosures.

The main challenge for all is privacy and security as healthcare records contain sensitive and personal information that might be attractive to the cybercriminal. For example, they can steal the data and sell it to a third party who can analyze them, whatever is. Moreover, the privacy must be protected not just from the external attacker but also from unauthorized access from the inside network. Therefore, the security of EMRs and HIS is critical. As in other types of cloud computing, approaches of cryptography can ensure the privacy and integrity of the data. Nevertheless, healthcare data will limit the search ability because the healthcare provider needs to decrypt the date prior searching; thus, the resulting data will take longer time, and the cost will be increased for data retrieval. Regarding internal attacks, there is an approach to integrate access control with some cryptographic primitives, e.g., attributes based encryption.

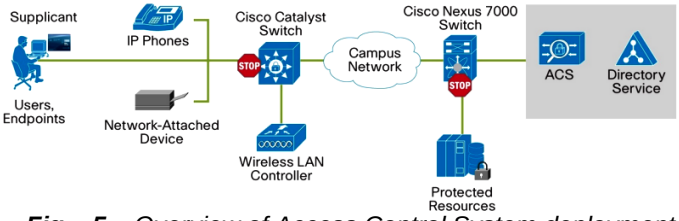

Fig . 5. *Overview of Access Control System deployment [23]*

There is recent research [24] [25] [26] to utilize blockchain (most of them made by successful Bitcoins) and secure healthcare data management. Blockchain is revolutionary technology which is able to distribute online database, which consists of a list of records called blocks that are linked using cryptography. Each block has its cryptography hash, timestamp, and transaction data. In healthcare filed, it also has a patient's data and healthcare provider information. Fig. 6 illustrates the concept of blockchain-based on EMR or other electronic medical data. Whatever healthcare data is updated for the patient, such as surgery, a new block is instantiated and distributed to all nodes in the patient network. Once the majority of nodes approved the new block, the system will insert the new block in the chain. Therefore, the patient information will be globally viewed with all medical history since the block content is publicly accessible. While block-chain can offer extreme opportunities for health care data management, using data integrity and distributed storage/access, this does not come without its own challenges. One of the challenges would be the result of strong data integrity in block-chain, as it results in immutability of the data, where any data that is stored in a block-chain can no longer be altered or deleted, the challenge here arises of the fact that personal health care data is protected by privacy laws, many of which do not allow perpetual data retention. The second challenge would be the block-chain is designed to record transaction data, which in comparison to medical data would be small in size and linear in nature, while the counterpart would be large in size and relational and might need to be searched rather than traced back as can be done in the transaction data.

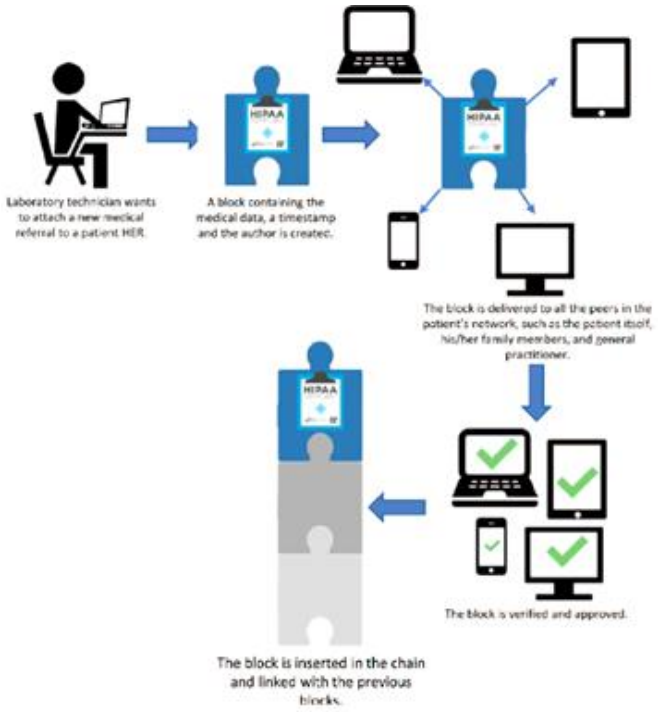

Fig . 6. *A conceptual block-chain-based EMR ecosystem [27]*

To compromise the challenges, some suggest a theory of off-chain storage of data. The concept of this theory is the keeping of the data outside the block-chain. However, the hashes of the data will be stored inside the block-chains. Thus, the healthcare data is stored off-chain, and it can be removed, corrected, secured. Meanwhile, immutable hashes are stored on-chain.

6 CLOUD PRICING: EFFECTIVE FACTORS

The main factors that affect the cloud price are the different products and the cost of the resources in the cloud computing effect on the customer directly. These factors are descriped as follows [28].

a) Static scheme-prices: each cloud resource has a fixed price, and customers will pay as per usage e.g., pay as you go scheme.

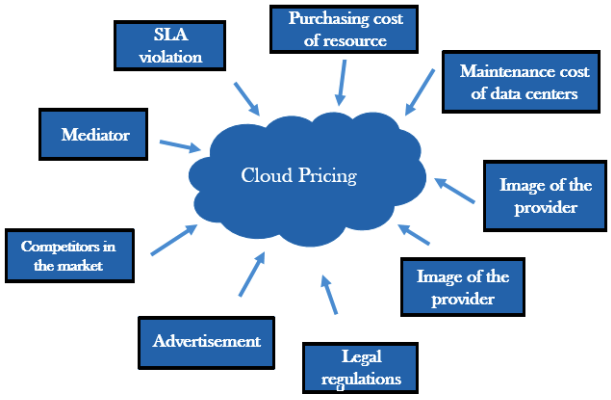

Fig. 7. *Factors affecting cloud pricing.*

b) Dynamic scheme-prices: this category does not have a fixed price for cloud resources e.g. action based pricing such as flight tickets in holiday seasons. Pricing of resource can be predicted in future demand using predictive modeling from the different cloud provider.

c) Amazon has multiple pricing modules for example: pay as you go which means customer can pay only for what his use, pay less per unit by using more which means customer can save more for their projects, pay less when you reserve which means customer can subscribe the computational resources with fewer charges for year or two years, or custom pricing which means the price can be customized for the unique requirements.

d) Microsoft Azure also has its own pricing modules for example: Pay-As-You-Go Subscriptions which means customer supposed to pay for the resources his used for last 30 days, enterprise agreements for large organization that have more than 250 users or devices to use cloud services thus they get enterprise discount for enterprise server, produce and cloud products, or prepaid subscriptions which means customer can prepay for the services for 12 months with 5% discounts.

7 CLOUD SECURITY: ISSUES AND THREATS

In consonance with influential applications of cloud computing, the security is crucial for the confidentiality of data. The customers used cloud computing to keep up many of personal data on their devices. Therefore, the transmission data from their computers to the cloud should have the capability to guard these data. The security issue in cloud computing are; privacy, confidentiality, legal issues, Reliability, Integrity, compliance, and Long term Viability [29]. The safety is the main angst in the computing environment. During the last years, the security has been developed based on surveys in respect of the services provided by cloud computing systems as shown in Fig. 8. The importance of which host level, network level, and application-level are equal in computing systems [30], a big number of security threats can occur at each level as follows.

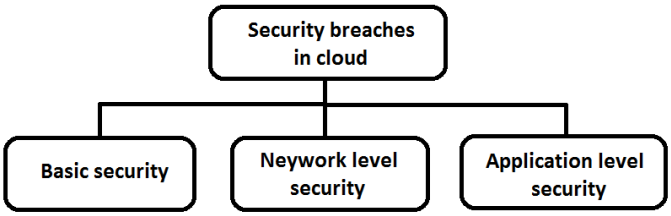

Fig. 8*. Security Breaches in Cloud*

A. Basic security

Nowadays, with the recent modernization of technologies the most consideration in it is safely such as Web technologies of Web 2. The most breaches faced by web application are:

a) The man in the middle attacks (MITM): snooping between customer and server is occurring by an attacker. While both of them believe are directly communicating with each other. But the fact is someone is stealing their data.

b) SQL injection attacks: this happens while the attacker injects SQL commands into the database of the server when an application fails to sanitize untested data. Hence, the attacker harm server database.

B. Network level security

a) Sniffer attacks: this attack launched by applications to capture packets following in the network. Thus, if the data is not encrypted, it will be readable.

b) Reassign number of columns: Place your cursor to the right of the last character of the last affiliation line of an even numbered affiliation (e.g., if there are five affiliations, place your cursor at end of fourth affiliation). Drag the cursor up to highlight all of the above author and affiliation lines. Go to Column icon and select “2 Columns”. If you have an odd number of affiliations, the final affiliation will be centered on the page; all previous will be in two columns.

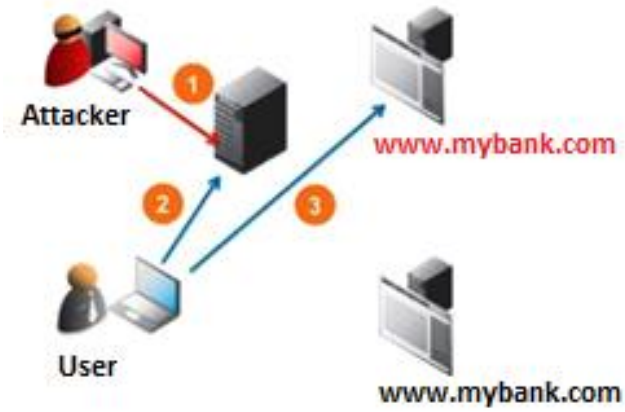

Fig. 9. DNS attacks [32]

C. Application level security

a) Cookie poisoning: it involves modifying the cookie to attain an illegitimate access to an application or to a web page. Figure bellow exhibits this kind of attack.

b) Denial of Service (DOS): in DOS attack, the spy sends a high number of requests to the server to make it busy. Hence, forth with the server became unable to handle all these requests.

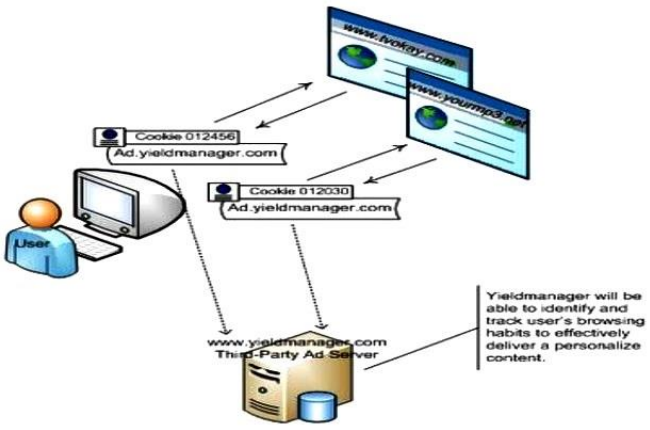

Fig. 10. *Cookie Poisoning [33]*

8 CLOUD COMPUTING ENVIRONMENT

Different studies discuss issues of security in cloud computing can expand. Such as, Quay's Guard is popular software that offered of vulnerability management[31]. However, there have a lot of threats; there has a clout level of security techniques. This section provides some of these techniques.

A. Architecture security

The cloud computing, hosted in data centers means when the user orders a cloud service, this virtual resource migrate to

physical machines in data centers of cloud operator. From here the architecture and functions for secure cloud defined by V. Fusing and A. Sharma [34] to provide security mechanism. The Architecture security includes three main entities the service user, the service provider, and the virtual infrastructure; therefore, the challenges on cloud security cab handle it.

B. **Using Mirage Image Management System**

Among many problems that come from a revolution of cloud computing, one of them is the problem of security management of vertical machine images [35] that encapsulate each application of the cloud and the most important on these images is integrity by cause of the initial state of the VM that determined by some image. The Mirage Image Management System consists of four main components: Image Transformation by Running Filters, Access Control, Image maintenance, and Provenance Tracking.

C. Using Client Based Privacy Manager

Sensitive data processed in the cloud must be having privacy; also, the data leakage should be declined. Client-based privacy manager assists in reducing the risk on it in addition to giving other useful privacy. The essential features of the privacy manager [36] are:

- Preferring setting: this approach is allows the users to handle personal data.
- Data access: a method which allows the users to access their data in the cloud, in order to check the accuracy of their data.
- Obfuscation: the automatic disruption of the fields in data structures before they come out.
- Feedback: this is to display the feedback to users respecting the usage of data.
- Personae: An approach is allowed to choose between various persons when interacting with the cloud.

9 SECURITY ALGORITHMS USED IN CLOUD COMPUTING

Numerous cryptographic algorithms have been developed and used in many different functions. Cryptography is the practice of approaches to secure communication in the existence of third parties. Cryptography's goal is to keep message privacy, confidentiality, data integrity, origin authentication, and Non-repudiation. Encryption algorithms are divided into symmetric-key and asymmetric-key. Modern symmetric-key algorithm sometimes referred to as private-key encryption, for example, DES (Digital Encryption Standard), 3DES (Triple Digital Encryption Standard), AES (Advanced Encryption Standard), and Bluefish. DES usually operates in block mode, in which it encrypts data in 64-bit blocks. The DES algorithm is essentially a sequence of substitutions of data bits united with an encryption key (see Fig. 11). Because the DES algorithm is based on simple Mathematic function, it is not difficult to implement in hardware. DES has a fixed key length. The key is actually 64 bits long, but only 56 bits are used for encryption; the remaining 8 bits are used for parity. The least significant bit of each key byte is used to indicate odd parity. AES is an iterated block cipher, which means that the initial input block and cipher key undergo multiple transformation cycles before producing output. It is based on the more general Rijndael cipher. Rijndael specifies variable block sizes and key sizes, but AES specifically uses keys with a length of 128, 192, or 256 bits to encrypt 128-bit blocks.The asymmetric-key algorithm utilizes a pair of keys for encryption and decryption, private and public key are generated by mathematic relationship. Usually, the public key is distributed to people that expect to receive the encrypted data, and the private key is known and kept only to the person encrypting the data. Examples of asymmetric-key encryption algorithms are DH (Diffie-Hellman) and RSA (Rivest, Shamir, and Adleman).

X. SECURITY ALGORITHMS IMPLEMENTATION FOR AES AND DES.

DES algorithm using net beans IDE with the CloudSim platform is shown in Fig. 11. The DES software code generates a random key for the algorithm and asks to enter the message,

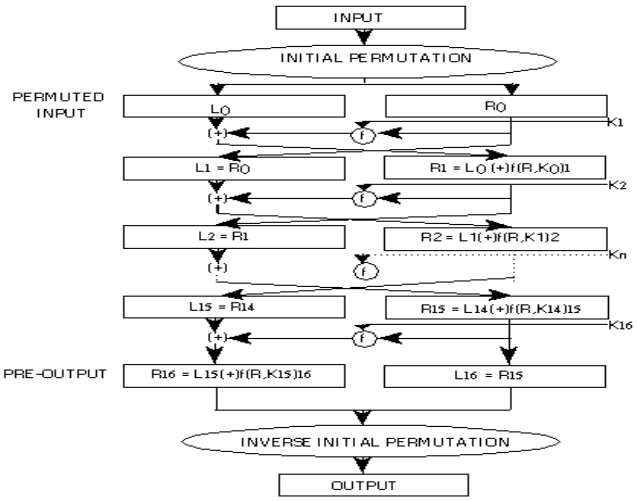

***Fig. 11**. The used code of the DES algorithm*

TABLE I COMPRESSION BETWEEN AES AND DES ALGORITHMS

Comparison	AES	DES
Platform	Cloud computing	Cloud computing
Basic block	AES data block represents into the matrix	DES data block represents into two halves
Principle	AES main Principle Substitution and Permutation	DES works on Feistel Cipher structure.
Key size	128,192,256 bits	56 bits
Scalability	Scalable	Scalable
Number of rounds	10 rounds for 128 bits 12 rounds for 192 bits 16 rounds for 256 bits	16
Computational time	Faster than DES (total time:3 sec.)	Slower than AES (total time: 12 sec.)
Security	AES more secure; since it has a larger secret key	DES more secure; since it has a smaller secret key

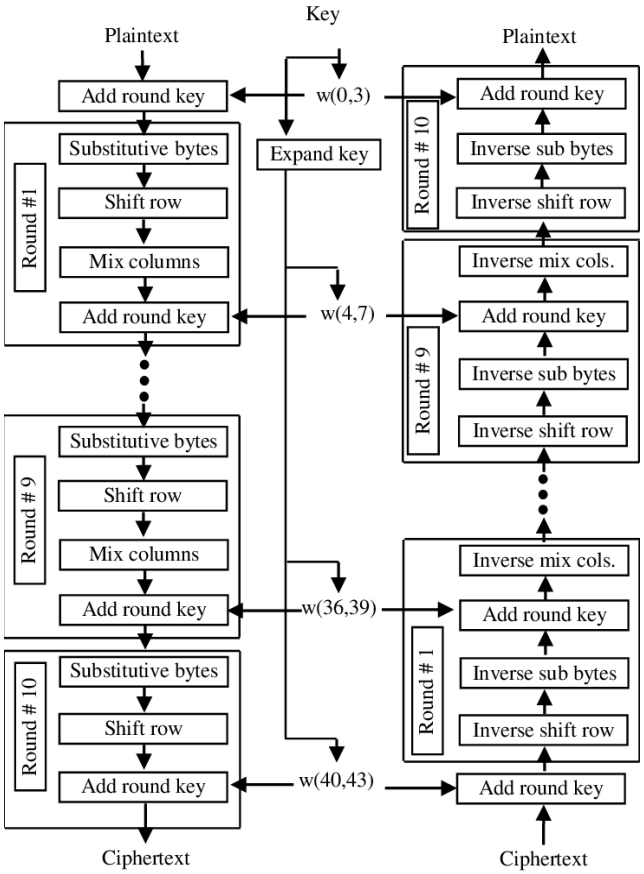

Fig. 12. *The used code of the AES algorithm*

which presents the plain text. After applying the algorithm, the ciphertext will be displayed. AES software code shown in Fig. 12 also generates a random key that used to encrypt the entered message (plaintext). A simple characteristic comparison between AES and DES algorithms can be made as shown in Table I.

REFERENCES

[1] R. Buyya, S. Y. Chee, V. Srikumar, B. James, and B. Ivona, "Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility," Future Generation computer systems 25, vol. 6 ,pp. 599-616, 2009.

[2] G. Brunette, and R. Mogull,"Security guidance for critical areas of focus in cloud computing v2. 1,". Cloud Security Alliance, USA, 1-76, 2009.

[3] P. Mell and T. Grance, "The NIST Definition of Cloud Computing," National Institute of Standards and Technology, Information Technology Laboratory, 2011.

[4] P. Dhir and S. Garg,"Survey on cloud computing and data masking techniques," International Journal of Innovations and Advancement in Computer Science, vol. 6, pp. 2347-8616,2017.

[5] G. Garg, S. Sabharwal, A. Jain. (2016, July),"Basics of cloud computing," International Research Journal of Engineering and Technology, 3 (7),

[6] M Ali, S. Khan, and A. Vasilakos,"Security in cloud computing: Opportunities and challenges," Information Science, pp.357-383, 2015.

[7] K.Hashizume, D.G.Rosado, E.Fernndez-Medina, and E.B. Fernandez," An analysis of security issues for cloud computing," Internet Services Application, vol. 4, pp. 5,2013.

[8] F. Liu, J. Tong, J. Mao, R. Bohn, J. Messina, L. Badger, and D. Leaf, "NIST cloud computing reference architecture," NIST special publication, pp. 1-28, 2011.

[9] M. Alhamad, T. Dillon, and E. Chang " Conceptual SLA framework for cloud computing," In Digital Ecosystems and Technologies (DEST), 4th IEEE International Conference on ,pp. 606-610, 2010.

[10] W. Pauley," Cloud provider transparency: an empirical evaluation," IEEE Security and Privacy, vol. 8 , pp. 32-39, 2010.

[11] C. Pettey, and R. van der Meulen, ' Gartner says cloud consumers need brokerages to unlock the potential of cloud services,' Technical Gartner report, 2009.

[12] J. Lucas-Simarro, I. Aniceto, R. Moreno-Vozmediano, R. Montero, andI. Llorente " A cloud broker architecture for Multicloud environments," Large Scale Network-Centric Distributed Systems, pp. 359-376, 2013.

[13] A. Samba, "Logical data models for cloud computing architectures," IT Professional, vol. 14, pp. 19-26.McMillan, 2012.

[14] S. Orenga-Roglá, and R. Chalmeta,"Social customer relationship management: taking advantage of Web 2.0 and Big Data technologies,". SpringerPlus, vol. 5, pp. 1462, 2016.

[15] D. R. Fordham, and C. W. Hamilton,"Accounting, Information Technology in Small Businesses: An Inquiry," Journal of Information Systems, 2017.

[16] S. Satish, T. N. Manjunath, and R. S. Hegadi," E-Solution for Next Line of Business and Education Using Cloud Computing," In Computing and Communication Technologies (WCCCT), World Congress on, pp. 105-110, 2017, IEEE.

[17] J. W. Rittinghouse, and J. F. Ransome," Cloud computing: implementation, management, and security," CRC press, 2017

[18] A. Ruiz-Zafra, K. Benghazi, M. Noguera, and J. L. Garrido," Zappa:An open mobile platform to build cloud-based m-health systems," In Ambient Intelligence-Software and Applications, Springer, Heidelberg, pp. 87-94, 2013.

[19] K. Gandhi and P. Gandhi,"Cloud Computing Security Issues: An Analysis," INDIACom, pp. 3858-3861, 2016.

[20] US Department of Health and Human Services, "Health insurance reform: security standards," Final rule 45 , 2003.

[21] T. Luarasi, M. Durresi, and A. Durresi " Healthcare based on Cloud Computing," 16th International Conference on Network-Based Information Systems, pp 113-118, 2013,

[22] Guuk university. "What is Cisco ACS?", Internet: https://geek-university.com/ccna-security/what-is-cisco-acs/ (Accessed on 10th June 2019)

[23] F. Tschorsch and B. Scheuermann, "Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies," IEEE Communications Surveys & Tutorials, vol. 18, no. 3, pp. 2084–2123, 2016.

[24] A. Azaria, A. Ekblaw T. Vieira, and A. Lippman,"MedRec: Using Blockchain for Medical Data Access and Permission Management," Proceedings of the 2nd Int'l Conference on Open and Big Data (OBD 16), pp. 25–30, 2016.

[25] J. Zhang, N. Xue, and X. Huang, "A Secure System for Pervasive Social NetworkBased Healthcare," IEEE Access, vol. 4, pp. 9239–9250, 2016.

[26] C. Espocito, A. De Santis, G. Tortora, H. Chang, and K. Kwang, "Blockchain: A Panacea for Healthcare Cloud-Based Data Security and Privacy?," IEEE CS and IEEE ComSoc, pp 31,37 , 2018.

M. Kandqal, M. Gahlawat, and K. Patel, "Role of predictive modiling in cloud services pricing: A survay," IEEE, 7th international conference on cloud computing, pp 249-259, 2017.

[27] B. Rohit and S. Sugata, "Review on Security Subjects in Cloud Computing and Related Mitigation Techniques," In International Journal of Computer Applications, vol. 47, pp 47-66, June 2012.

[28] "Amazon Web Services: Overview of Security Processes", March 2013. pp.1-48.Internet: https://d0.awsstatic.com/whitepapers/Security/AWS_Security_Whitepaper.pdf (Accessed on 26th June 2019)

[29] Infoblox Scott Fulton. "Top 10 DNS attacks likely to infiltrate your network."Internet: https://www.networkworld.com/article.html. (Accessed on 10th August 2019)

[30] P. Garg, S. Goel and A. Sharma,"Security Techniques for Cloud Computing Environment," ICCCA2017, pp. 771-776.

[31] A. B. Jeng, C. C. Tseng, D. F. Tseng, and J. C. Wang, "A Study of CAPTCHA and its Application to User Authentication", Proc. Of 2nd Intl. Conference on Computational Collective Intelligence: Technologies and Applications, 2010.

[32] V. Fusenig and A. Sharma, "Security Architecture for Cloud Networking," International Conference on Computing, Networking and Communications, Cloud Computing and Networking Symposium, pp. 45-49, 2012.

[33] J. Wei, X. Zhang, G. Ammons, V. Bala and Peng Ning,"Managing security of virtual machine images in a cloud environment," the 2009 ACM workshop on Cloud computing security, pp 91-96, November 2009.

[34] M. Mowbray and S. Pearson, "A Client-Based Privacy Manager for Cloud Computing," the Fourth International ICST Conference on Communication System, June 2009.