IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Vol. 6, Issue 12, December 2019

Security Framework for Cloud Computing

Jawaher Alqahtani

Information Systems Department, Faculty of Computing &Information Technology,

King Abdulaziz University, Jeddah, Saudi Arabia

Abstract: Cloud computing is one of the huge things in data innovation and in information technology world. Not at all like other previous computing systems, cloud computing paradigm that give boundless foundation or infrastructure to storage or running client's information/software. Cloud computing is a since quite a while ago envisioned vision of figuring as a utility, where information owner can remotely store their information in the cloud to appreciate on-request profoundly quality application and services from a mutual configurable registering assets. Our paper gives a concise presentation of cloud computing its sorts and security issue and ways to deal with secure the information in the cloud condition. Our proposed framework we expect will be more secure in addition, to addressing forensic computing in cloud computing as one of the most important emerging issues and highlighted security challenges.

Keywords: Attack, Pubic Cloud, Cloud Computing, Security, Evidence

I. INTRODUCTION

This Cloud computing alludes to both the applications delivered as services over the Internet and the equipment(hardware) and frameworks(software system) in the server or data centre that give those services[view of computing]. Cloud computing is as of now rising as a component for high level or professional, and in addition filling in as a storage framework system for assets (resources).Cloud enable clients to pay for whatever assets they utilize, enabling clients to increment or diminishing the amount of assets as required needed [10]. This new computing paradigm is alluded or referred as a cloud computing. In this paper will describe a general structure of cloud computing in which the application and regularly the information itself is stored directly not on your pc but rather a remote server that is associated with the internet. Here focus on the structure of a cloud in which the cloud utilizes the various application, for example, Amazon, Google applications for storing the data [9].

Type Of Cloud Commuting Mode

For secure services in cloud computing there are two kind of model. Initially is the delivery model and another is deployment model.

Delivery model: Delivery model in cloud computing we characterize and define by the three keys that are infrastructure (framework) as a service (IaaS), Software as a service (SaaS), Platform as a service (Paas) see (figure1).

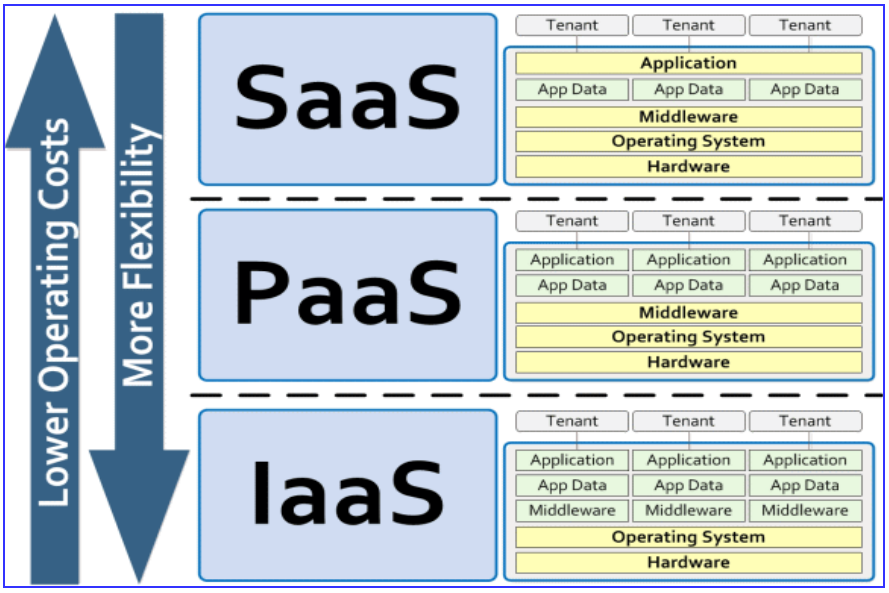

Figure1: Delivery Model

IARJSET
ISSN (Online) 2393-8021
ISSN (Print) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
Vol. 6, Issue 12, December 2019

Infrastructure (framework) as services (Iaas) is the establishment of all the cloud services (bottom layer). It supplies an arrangement of virtualized infrastructural segment, for example, virtual machines. Platform (Stage) as services (Paas) is a centre layer in cloud services. It enables programming environment to access and use extra application building piece or block. Software as an services (Saas) works on the virtualized and pay-per-utilize costing model whereby software applications are rented out to contracted association by specific or specialized saas merchant (vendor) [9].

Deployment model:

- Public Clouds: In public cloud, the services and infrastructure (framework) are given off-site over the Internet. These clouds offer the best level of effectiveness in shared recourses (assets); however, they are less secured and vulnerable rather than private clouds.
- Private Clouds: Differ from public clouds, in the Private Clouds, the services and infrastructure (framework) are kept up and maintained on a private system network. These clouds offer the best level of security and control. However, they require the organization to in any case buy and keep up all the product (software) and infrastructure (framework).
- Hybrid Clouds: Hybrid cloud incorporates a variety of public and private choices with different suppliers or provider.

In basic terms, when you are utilizing cloud computing, you do not have to introduce and install the required application on your framework system. Rather, you utilize the application that keeps running on a remote area/datacentre, which we called the 'Cloud 'see (figure2).

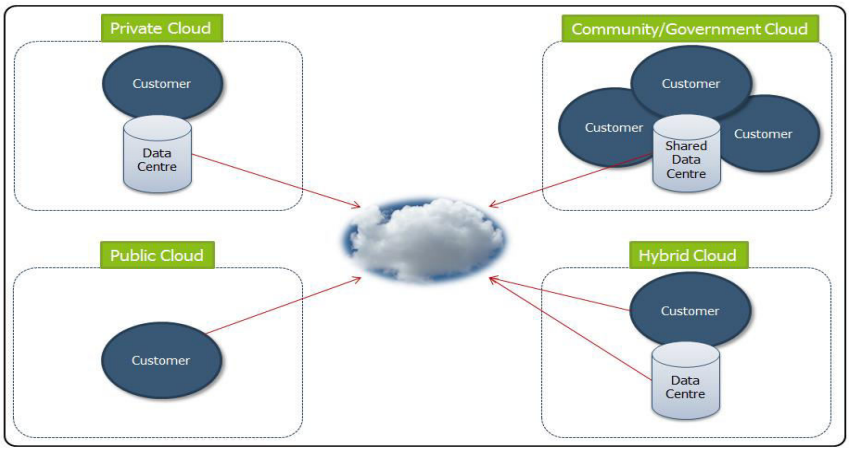

Figure2: Deployment Model

After learning about the cloud and its types, we present the most important challenges facing forensic science in cloud computing:

- Decentralization of server farms

Distributed computing's conveyed design enables information to be made, put away, handled and appropriated more than a few server farms and physical machines which are universally scattered and furthermore conceivably scattered into different topographical areas and purviews. Information is reproduced to different servers to guarantee excess of information.

- Decentralization of server farms

Distributed computing's conveyed design enables information to be made, put away, handled and appropriated more than a few server farms and physical machines which are universally scattered and furthermore conceivably scattered into different topographical areas and purviews. Information is reproduced to different servers to guarantee excess of information.

- Reliance on CSP In a distributed computing condition

The cloud specialist co-op has all the control over the earth and hence controls the wellspring of the evidential information. The way toward safeguarding advanced proof in the cloud very relies upon the help that the examiner gets from the cloud specialist co-op (CSP).

- Metadata/Provenance security

Metadata, otherwise called information provenance, is the historical backdrop of advanced items. Metadata depicts possession and the procedure history (make, adjust and access) of information objects. Metadata is crucial to the accomplishment of measurable examinations with a specific end goal to decide the responsibility for information (who get to the information) and the course of events of evidential information (when information got to). The vulnerability

IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Vol. 6, Issue 12, December 2019

about metadata and metadata accessibility are challenges for examinations in the cloud and who and when inquiries can stay unanswered if the supporting metadata is inaccessible [12].

- Particular logging unstable

Logs are exceptionally valuable evidential information in an examination. Logs incorporate framework logs, arrange logs, firewall logs and switch logs. On the off chance that the cloud specialist co-op (CSP) does not run any logging application then no open door exists to gather particular logging data amid an examination. On the off chance that the CSP runs logging applications, at that point the logs must be reasonable sizes to be helpful and to counteract wiping memory on facilitating servers. At present CSPs are not committed to give all logs and logs are not sensibly secured by the CSPs [13].

II. LITRITURE REVIEW

- **"A survey on security issues in service delivery models of cloud computing (2011)"** Over the most recent years, cloud computing has developed from being a promising business idea to one of the fast developing portions of the IT business .Despite of all buildup encompassing the cloud ,enterprise client are still send their business in the cloud. Security is one of the real issues which restrict the development of cloud computing and complications with information security, privacy and information protection keep on plaguing the market [1].
- **"Quirc: A quantitative impact and risk assessment framework for cloud security (2010)"** Six key Security Objectives (SO) are distinguished for cloud stages, and it is suggested that a large portion of the run of the mill assault vectors and occasions guide to one of these six classes. Wide-band Delphi strategy is proposed as a logical intends to gather the data essential for surveying security dangers. Chance appraisal knowledgebase could be created particular to every industry vertical, which then fill in as contributions for security hazard evaluation of cloud computing stages. QUIRC's key leeway is its completely quantitative and iterative union approach, which empowers partners to nearly survey the relative strength of various cloud merchant offerings and methodologies in a solid way [2].
- **"The management of security in cloud computing (2010)"** cloud computing has raised IT to more up as far as possible by offering the market environment information storage and limit with adaptable versatile registering handling energy to match flexible request and supply, while decreasing capital consumption. However the opportunity cost of the fruitful usage of Cloud computing is to viably deal with the security in the cloud applications. Security awareness and concerns emerge when one starts to run applications past the assigned firewall and towards public domain [3].
- **"Personal cloud computing security framework (2010)"** cloud computing is a developing term nowadays. It display the progress of many existing IT advancements and isolates application and data assets from the fundamental foundation. Personal Cloud is the hybrid deployment model that is combined private cloud and public cloud. Largely, cloud orchestration does not exist today. Web browser provides current cloud service or host installed application directly. As indicated by the ITU-T draft, we should seriously mull over cloud coordination environment in a joint effort with other cloud suppliers. Previous work [4].
- **"Collaboration-based cloud computing security management framework (2011)"** The cloud computing model display to another paradigm change in web based services that delivers professional distributed computing platforms in which computational resources are offered 'as a service'. Despite the fact that the cloud model is intended and designed to receive uncountable rewards for all cloud partners including cloud suppliers (CPs), cloud customers (CCs), and services provider (SPs), the model still has various open issues that affect its validity[5].
- **"Security framework for cloud computing environment: A review (2012)"**

Cloud computing has an extensive variety of properties some of which are as the following:-

- Shared Infrastructure: cloud condition utilizes a powerful software model that permits sharing of physical services, storage and networking capabilities among clients. The cloud foundation infrastructure is to discover the vast majority of the accessible infrastructure over multiple clients .
- Network Access: Cloud services are accessed to over a network system from an extensive variety of devices, for example, PCs, tablets, and cell phones by utilizing measures based APIs .
- Handle Metering: Cloud services provider or partner store data of their customers for managing or handling and enhancement the services and to give revealing or reporting and charging data. Because this, clients are payable for services as per the amount they have really utilized among the charging or billing period[6].
- **"Gartner: Seven cloud-computing security risks (2008)"** authorized client access. Delicate information handled outside the undertaking carries with it an intrinsic level of risk, because in the fact that outsourced services sidestep the "physical, intelligent and work force controls" IT shops apply over in-house programs. Get as much data as you can about the general population who deal with your information. "Request that suppliers supply particular data on the enlisting and oversight of advantaged overseers, and the controls over their access"[7]**.**
- **"Security in cloud computing (2012)"** Strong verification structure: a strong client validation system for cloud computing with multiple security elements, for example, identity management to each user, shared confirmation, session key assertion between the clients and the cloud server, and ease of use (i.e., secret key change stage). The term,

solid two figure means one component „something you know" (secret key) and two calculates „something you have" (smartcard and OOB)[8].

- **"A view of cloud computing (2010)"**Earlier, we distinguished three properties whose blend gives cloud computing its appeal: short-term use (which infers downsizing and in addition up when request drops), no upfront cost, and unbounded limit on request. While it's direct what this implies when connected and apply to computation, it's less evident and clear how to implemented it to persistent storage .The opportunity, which is open research issue, is to make a storage system that would not just meet existing developer desires or expectations as to sturdiness, high accessibility, and the capacity to oversee and question information, butt consolidate them with the cloud features of scaling arbitrarily up and down on request[9]**.**
- **"Security in cloud computing (2010)"** Security dangers on cloud clients are both outside and inside. A considerable lot of the outside dangers are like the dangers that huge server farms have officially confronted. This security concern vendor is separated among the cloud clients, the cloud vendors and the third party vendor required to ensure secure high sensitive software or arrangements. If the application level security is the responsibility of the cloud client, then the supplier is in responsible for the physical security and enforce outside firewall strategies & policies [10]
- **"Survey on Cloud Forensics and Critical Criteria for Cloud Forensic Capability: A Preliminary Analysis (2011)"** the results were presented and the current analysis of the survey "Forensic Cloud and Critical Criteria for Forensic Cloud Capacity" conducted towards digital forensic experts and practitioners.. In the survey results, the majority of respondents agree that the criminal forensic evidence is a digital forensic application in cloud computing is a combination of traditional computer forensics and forensics Small digital device. As a result, researchers say, the forensic architecture of cloud computing environments needs to be developed. In addition, participants reached consensus on the type of tools, procedures, personnel, agreements, policies and guidelines for criminal investigative capacity [11].
- **"Forensics Cloud: An Overview (2011)"** cloud computing has been defined as one of the most transformative technologies in computing history. Cloud organizations, including cloud service providers and customers, are still able to determine a well-defined forensic capability. Without this, they cannot guarantee the robustness and suitability of their services to support investigations into criminal activity. The first steps towards the identification of the new field of forensic medicine in the cloud, the analysis of challenges and opportunities, including the question of jurisdiction and international non-cooperation, were reviewed, while the new environment also provided unique opportunities for constituent standards and policies. Cloud computing is a new battleground for cybercrime, as well as a new ground for a new investigative approach. Forensic cloud is a new area of research, there is still a lot to be done and this paper just marks the way forward [12].
- **"Cloud Computing: The Digital Forensics Challenge(2015)"** The forensic cloud still faces many problems that have not yet been addressed by research to find solutions to the issues. Getting data in the cloud is still the biggest issue with many different problems. Much research is needed to develop procedures and tools that can be used by service providers to extract the data that investigators need in a criminal manner. Service level agreements between cloud clients and cloud service providers can only protect the cloud client to a point if a transparent investigation can not be performed. There is a need for legislation to retrieve timely evidence on the border and third-party surveillance devices to protect the personal rights of the cloud client to protect both cloud customers as well as the investment of the cloud service provider in infrastructure and technology services in the event of an accident. However, this is unlikely to happen soon, given the differences in legislation in many parts of the world. Law enforcement working groups and other cloud parties must address issues and find solutions that can be applied anywhere to stop adversaries from using safe haven countries to commit their crimes in the cloud. Given the current situation, with very few answers to the problems of cross-border legal differences and techniques to ensure that data are obtained in a criminal manner, without prejudice to the custody chain, it can be expected that it will take time to find solutions to the issues highlighted in this paper [13].
- **"Cloud Log Forensics: Foundations, State of the Art, and Future Directions(2012)"** This paper reviews the state of the art of CLF and illuminating the various challenges and issues involved in investigating cloud log data. Recording mode, importance of CLF, and cloud logging are entered as a service. Furthermore, CLF-related case studies are highlighted to highlight the practical implementation of cloud log investigation to analyze malicious behaviors. Defines security requirements for CLFs, vulnerabilities, and challenges to endure with different log portability. We identify and present future challenges and trends to highlight open research areas that have been commissioned to motivate investigators, academics and researchers to investigate them. In the end, cloud record investigators will be the one who uses the tool to analyze cloud records in cloud computing. Therefore, the need for highly standardized CLF tools is extremely important in investigating different cloud records in real time cloud computing [14].
- **" Cloud Log Forensics Metadata Analysis(2013)"** In this paper, researchers note that the increase for information retrieved from the current virtual cloud data system architectures and the quality of questioning it is very difficult for law enforcement agencies to resolve criminal activities in these logical areas. This paper asks a question about the type of information required from hosted operating systems (FM), which is explored by forensic examinations. It also provides an examination of the VM host hypervisor kernel log file system metadata play in cloud

forensic investigations. The researchers analyzed the role of mouse host Hippo Nucleus log file system metadata playing in the forensic investigations cloud. In general, one realizes that some of the information required is impossible to get host systems that are running arbitrary programs, and thus are considered an intractable problem. Against this backdrop, the future of cloud file system designs must be supported by forensics and security, which plays a more central role in the requirements of software engineering and the structure of implementing hosted host operating systems. The ongoing work in the academic and industrial research laboratories authors explore the private cloud design audit log mouth and security tools that can be used to address the range of concerns raised in this paper[15].

III. METHODOLOGY

Cloud computing has become a changing platform for organizations to create their infrastructure and frameworks on. If organizations are to consider using cloud-based systems, they will face the task of reassessing their current security strategy or methodology, and the angles of the cloud aspects to be assessed.

Methodology In this paper:

1. Describe the recent papers published in 2001-2015 on the risks and security issues faced by organizations using cloud computing in their dealings and some proposed or recommended solutions to avoid those risks and then discuss their applicability.
2 - See the most prominent methods proposed, that help to avoid the security risks facing the cloud computing, and how it works.
3 - Proposing a curriculum that combines all the advantages and takes advantage of the capabilities of the previous curricula in solving the challenges and security issues and adding many characteristics and features that make it an integrated approach to enhance the security aspect
4 - Add solutions proposed for the most prominent challenges in the field of forensic medicine in the cloud computing
5. Writing future proposals on the curriculum and presenting the main obstacles faced by the researcher**.**

Part of the steps have been implemented and the other will be applied in future research due to time constraints

IV. CONCLUSION

In this proposed research we review the concept of cloud computing and its components and different types. The research also examined the difference between current cloud computing models and the gaps affecting cloud computing work and effectiveness. One of the most important problems for this type of high-risk technology is security challenges. We highlighted many different security challenges and problems, proposed solutions to the solution as well as providing a proposed framework that enhances the security aspect.

Our proposed framework is expected to be more secure, in addition to addressing criminal computing in cloud computing as one of the most important emerging issues, and emerging security challenges.

REFERENCES

[1]. Subashini, Subashini & Kavitha, Veeraruna (2011). A survey on security issues in service delivery models of cloud computing. Journal of network and computer applications, 34, 1-11.
[2]. Saripalli, Prasad& Walters, Ben(2010). Quirc: A quantitative impact and risk assessment framework for cloud security. Cloud Computing (CLOUD), 2010 IEEE 3rd International Conference on,280-288.
[3]. Ramgovind, Sumant & Eloff, Mariki (2010). The management of security in cloud computing. Information Security for South Africa (ISSA), 2010,1-7.
[4]. Sang-Ho a, Park& Jun-Young , Huh(2010). Personal cloud computing security framework. Services Computing Conference (APSCC), 2010 IEEE Asia-Pacific,671-675.
[5]. Almorsy, Mohemed & Grundy, John(2011). Collaboration-based cloud computing security management framework. Cloud Computing (CLOUD), 2011 IEEE International Conference on,364-371.
[6]. Malik, Ayesha & Nazir, Muhammad(2012). Security framework for cloud computing environment: A review. Journal of Emerging Trends in Computing and Information Sciences,390-394
[7]. Brodkin, Jon(2008). Gartner: Seven cloud-computing security risks, Infoworld,1-3.
[8]. Sharma, Sanjana & Soni, Sonika(2012). Security in cloud computing. National Conference on Security Issues in Network Technologies
[9]. Armbrust, Michael &Fox, Armando(2010). A view of cloud computing. Communications of the ACM,50-58.
[10]. Zunnurhain, Kazi & Vrbsky, Susan(2011). Security in cloud computing. Proceedings of the 2011 International Conf on Security \& Managemt.
[11]. P. Gladyshev, A. Marrington, "Digital Forensics and Cyber Crime", *First International Conference ICDF2C 2013*, 2009.
[12]. P. Gladyshev, A. Marrington, "Digital Forensics and Cyber Crime", *First International Conference ICDF2C 2013*, 2009.
[13]. G. Meyer and A. Stander, "Cloud Computing: The Digital Forensics Challenge", in Proceedings of Informing Science & IT Education Conference, 2015, pp. 285-299.
[14]. Khan S, Gani A, Abdul Wahab AW, Shiraz M, Bagiwa MA, Khan SU, Buyya RK, Zomaya AY, Cloud Log Forensics: Foundations, State-of-the-art, and Future Directions, ACM Computing Surveys. 2016b. (In Press).
[15]. Thorpe, I. Ray, T. Grandison, and A. Barbir. 2012a. Cloud log forensics metadata analysis. In Proceedings of the IEEE Computer Software and Applications Conference Workshops (COMPSACW). 194-199.