International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-8, Issue-1, May 2019

Data Management in the Clouds and Related Challenges and Issues

E. Saikiran, Anubharti, Md. Ateeq-ur-Rahman

Abstract*: Cloud computing, an ever changing computing type through which users have access to configurable on-demand functionality through Web-based technology, has the ability to provide IT services faster and cheaper but also provides new data management possibilities. The auditing framework in the cloud computing environment is necessary to process a load-balanced model for examining the significant risk of Cloud Service Provider services. This paper has defined various aspects of the layout of an auditing frame work, together with all other components are widely considered to be safe and secure for access control and store data on CCE. In the cloud computing environment, the audit framework is required to process different cloud models to evaluate the risk of cloud services. In this paper, we introduced several areas of audit framework development, including all elements designed to access or store CCE information to address safety issues.

***Index Terms*: Cloud computing; Data Management; infrastructure components; analysis framework**

I. INTRODUCTION

Recently there has been a substantial increase in the popularity of cloud computing systems, pay-as-you-go charges and several customers with the same physical infrastructure [1]. The cloud computer environment provides endless computer economic resources and users with delusion. Users can boost or decrease their consumption of resources depending on their energy needs. All clusters, grids and cloud technology are designed to allow for a fast and efficient aggregation of resources and a single system approach of a large quantity of computer resources from a fully virtualized system [2, 3]. Cloud technology also offers computer services for utilities as computer services. A business model is characterized in the utility computer for the provision of computer services on request. In this model, users pay service providers based on their service usage. Conventional facilities such as water, electricity, gas and telephony are also provided to users. Cloud computing is a new phenomenon that satisfies rapidly growing IT and computing requirements. This is quite beneficial for users and organizations, as it can keep prices down and help to solve disruptive IT systems [4]. The Cloud is becoming more and more prominent in several regions such as banking, e-commerce, retail, academics, etc., due to its many benefits. The possibility of IT companies ' capital expenditures is also reduced by cloud computing [5]. Across the other hand, cloud vendors can probably afford and organize cloud available resources in terms of profit.

In Section 2, we describe the interesting details of various data management plans and the organization of this paper. The work proposed in Section 3. The Results and discussion in Section 4. Finally, we concluded the paper in Section 5.

II. BACKGROUNDWORK

In this section, we aim to determine which information leadership applications are best adapted for cloud computation implementation. For instance, during season-or-involved or unpredictable increases in item supply sold by an electricity retail business, or during an exponential development stage of a social networking site, extra computing resources can be allotted on the fly to manage enhanced demand in just a few minutes.For over two decades the database research community has been held back by interoperable and exact data management. As perdatabase systems the principalgeneralresolution to report data not only on a single machine but also global serialization [2]. The damaging effects on overall quality caused by partial inadequacies and overhead synchronization did not support this concept over a few machines. Almost all of these structures have therefore never been widely used in industry.Thequeries permitting strict latency and availability, encompass irregular working loads, function on cluster computer architectures and stack claims in database system territories. Many applications go to the cloud with the wide availability of the framework "cloud computing." The resource elasticity and payout for the model have violated the infrastructure obstacle for new applications.

In combination with an increased production for data storage while assuring 24/7 accessibility and different guidelines for accuracy, these applications ' sporadic load features present challenges and opportunities for cloud data management. Since cloud computing is predicated on networked assets, all listed cyber threats face these assets. And as data from several clients can be focused on the networks of one cloud provider, hackers tend to be attracted to these extremely wealthy domains more likely. Table 1 summarizes some of the common cyber-security technologies classified by their type of security control. Long-term endeavors are vital, such as standard development, cybersecurity research and technological solutions and transition of key findings into common items. Although in areas such as protocol safety, product safety and operational directives there are many other standards for cyber security technology, standards want to be established that guide the use of cyber security technologies and procedures.

Revised Manuscript Received on 30 May 2019.

***** Correspondence Author

E. Saikiran*, Research Scholar SRU and Working as Assistant Professor, Department of Computer Science and Engineering, SRITW, Warangal Urban, Telangana, India,.

Dr. Anubharti, Dean of Engineering SRU, Alwar, India.

Dr Md. Ateeq-ur-Rahman, Professor and Principal, Shadan College of Engineering and Technology ,Hyderabad, Telangana, India

Several areas of research are being developed by the federal government organizationforcyber-security technologies [4-6]. Table 2 identified some of the key needs of cyber-security research.

Table 1. Common technologies

Category	Technology
Access control: Boundary protection Authentication Authorization	Firewalls
Content management	Screens the unsuitable content web and communication applications, with the exception of spam, prohibited file types and intellectual property.
Biometrics	Uses human characteristics, such as fingerprints, irises, and voices to establish the identity of the user.
Smart tokens	Establish identity of users through an integrated circuit chip in a portable device such as a smart card or time synchronized token.
User rights and privileges	Allow or prevent access to data and systems and actions of users based on policies of an organization.

Table 2. Research in cyber-security

Research area	Description
Composing secure systems from insecure components	Building the complex heterogeneous systems that maintain security while recovering from failures.
Security for network embedded systems	Detect, understand, and respond to anomalies in large, distributed control networks that are prevalent in electricity, oil and natural gas, and water sectors.
Security metrics and evaluation	Metrics that express the costs, benefits, and impacts of security controls from multiple perspectives: economic, organizational, technical, and risk.
Socioeconomic impact of security	Legal, policy, and economic implications of cyber-security technologies and their possible uses, structure and dynamics of the cyber-security marketplace, role of standards and best practices, implications of policies intended to direct responses to cyber-attacks.
Vulnerability identification and	Techniques and tools to analyze code, devices, and systems in dynamic and large-scale environments analysis.

III. PROPOSED MODEL

These schemes described previously benefit different phases of cloud data management.

Cloud Data Management Solutions

Cloud data–Cloud data can be very large (for example, text-based or scientific applications), unorganized or non-structured, and usually adjoining only (with rare updates) cloud users and applications developers.

• New File Systems: GFS, HDFS

• New DBMS: Amazon Simple DB, Google Base, Google big table, Yahoo Pnuts, etc.

• New parallel programming: Google Map Reduce (and its various variations) something like an aggregate structure may help to select the technologies to protect critical infrastructure.

A global framework should include:

(1) Determination of business security requirements;

(2) Performance of risk evaluation;

(3) Establishment of a safety policy;

(4) Implementation of solutions including people, processes and technology to mitigate identified security risks.

Considering the cloud data storage scenario as outlined in Figure.1, we have proposed the Cloud audit framework consisting of four entities:

(i)Cloud Users as their primary role is to use resources of cloud depend on user request for storage purpose.

ii) The broker job is to always maintain strong association among several layers of virtual devices. Also maintain business services providers has the responsibility of managing user applications.

iii) The Cloud Service Provider (CSP) provides metering, service-level policy, license administration and authentication control ingredients for infrastructure.

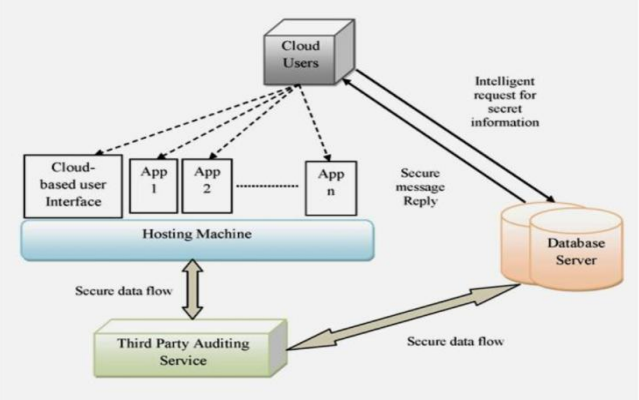

Fig.1: Cloud Data Storage Scenario

Figure.2 represents the workflow in relation to the current individual elements of the audit model as characterized below in the description and communication of the components:

Service Broker: Cloud users wishing to use or deploy their application must sign up on the broker server to promote services such as registration, requesting, monitored and managing. To keep the service broker on the log server and to provide an audit service with the user log. Cloud Brokers offers a single access point for the management of various cloud facilities for company and technical reasons. The two main characteristics of the cloud broker are the capacity to provide various cloud suppliers with a single coherent interface and the direct visibility of the broker to which the business provides services in the context.

Identification Management Service (IMS): The main objective of identification management in cloud computing is to administer private identification information to correctly control access to computer assets, applications, data and facilities. The leadership of identity is the only region of IT safety that provides real advantages over and above the danger of safety violations. Identity leadership enables avoid violations of safety and serves an important part in assisting any business obey with IT safety rules. The advantages of maintaining our economic information secure from unlawful access can be enormous.

Authentication and Access Management Service: Authentication and access management services (AAMS) Efficient management and proper process management are the responsibility of the detection and authentication management service. The User Management Service is related to rules, policies and management of lifecycle identification. Data management and supply services are accountable for the distribution of data identification into the authorization of IT resources.

Hosting service: The hosting service includes several cloud service provider components. These aredesigned for connecting together between users of cloud resources as wellthe brokers for providing services. Once all authentication and identity is completed, the user application is dispatched on the host machine and VMM or hypervisor is requested to get the needed resources from the IaaS (Infrastructure as a Service) layer. The infrastructure layer then assigns the resources for the particular application and instantly provides the user with physical and virtual resources. This workflow requires identity management, which makes it easy for your host to identify problems associated with correct requests, for the recognition of virtual machine ID and data center ID. Since verifying identifiers, the host proves the validation of the resource allocation.

Audit service: The audit service provides a Policy Database, a Strategy Review Engine, an Event Processing service and two-module query managers, such as query access managers and query regulations. The Policy Database main goal is toprovidethe wanted policies for keeping data more secure on the cloud and safety in line with customer needs and proposed legislation, regulations and laws. The strategic rules engine identifies a strategic plan for the all type of rules and regulations by the governing bodies by following standards of the cloud services.

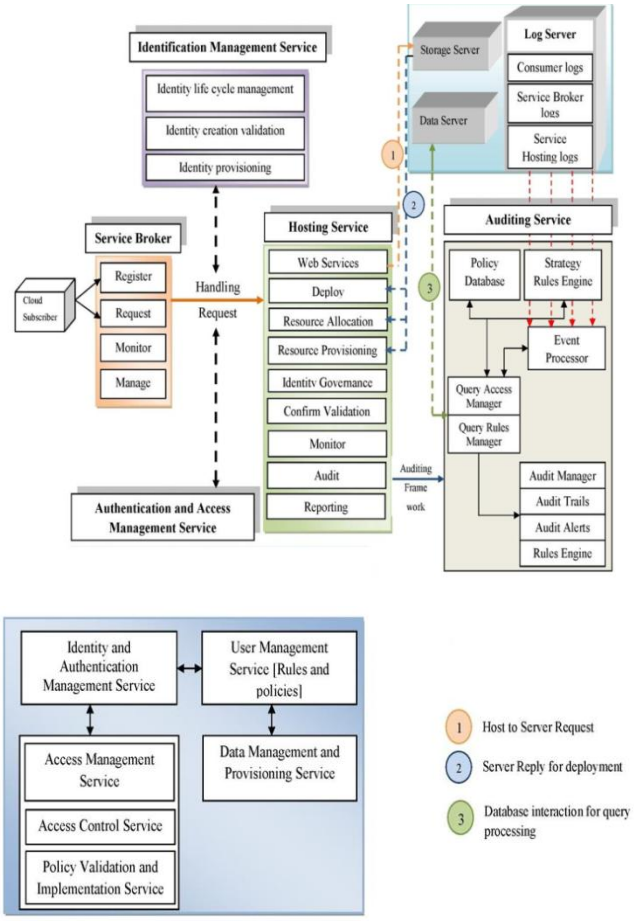

Fig.2: Auditing framework for cloud computing environment

IV. RESULTS AND DISCUSSION

The below displayed results are simulated under Java JDK and My SQL server.

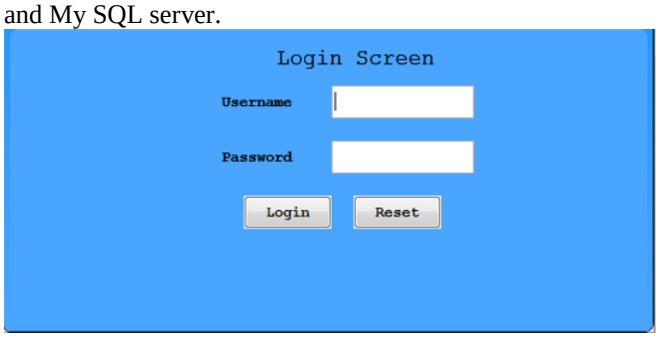

Fig.3: Login as admin environment

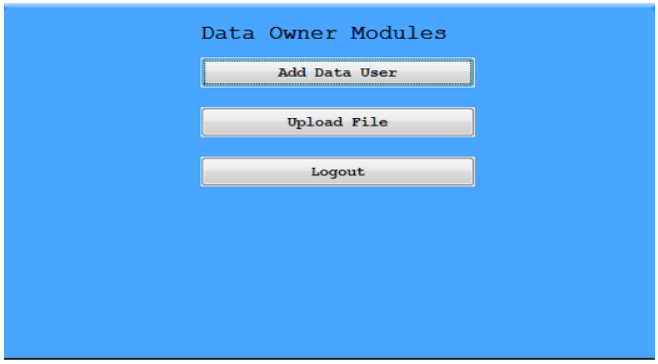

Fig.4: Data owner modules screen

Fig.5: Register as master

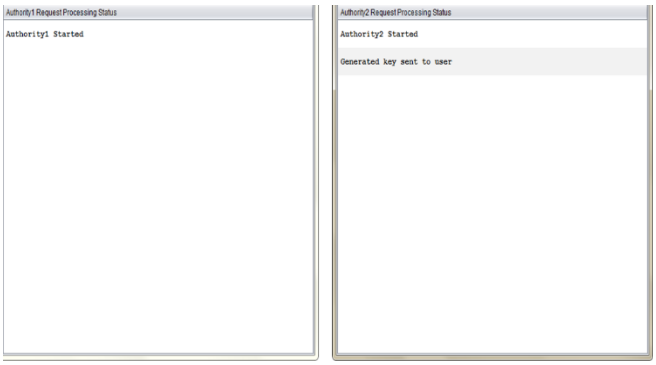

Fig.6: Authority1 generate the key for user. Authority2 send the generate key to user.

V. CONCLUSION

Again the way private companies are transferred in the age of information has changed cloud computing. But with the outbreak of data in a global networked environment, countries have become more and more interconnected, and safeguarding a crucial country facilities for all levels of government is an enormous task. The primary reasons behind the achievement of the utility cloud paradigm are elasticity, the payment of the payment model and the extensive use of commodities to exploit economy of scale. Developers experience a very hard problem: isolation and atomicity through thorough data partition engineering.

REFERENCES

1. Kim, W., "Cloud Computing: Today and Tomorrow", Journal of Object Technology. Vol. 8. No.1, pp. 65-72, February, 2009.
2. Marios, D., Dikaiakos, G.P., Dimitrios, K., Mehra, P., Athena, V., "Cloud Computing Distributed Internet Computing for IT and Scientific Research", Journal of IEEE Internet Computing, Vol. 13, Issue. 5, pp. 10-13, 2009.
3. Costanzo, A. D., De Assuncao, M.D., Buyya, R., "Harnessing Cloud Technologies for a Virtualized Distributed Computing Infrastructure", Journal of IEEE Internet Computing, Volume 13, Issue.5, pp. 24-33, 2009.
4. Chen, X. J., Zhang, J., Li, J., Li, X., "Resource virtualization methodology for on demand allocation in cloud computing systems", SOCA, Vol. 7, Issue 2, pp. 77-100,June 2013.
5. Adams, K., Agesen, O., "A Comparison of Software and Hardware Techniques for x86Virtualization", in Proc.ASPLOS"06, Oct. 21–25, pp. 2-13, 2006.
6. Villegas, D., Antoniou, A., Sadjadi, S. M., Iosup, A., "An Analysis of Provisioning and Allocation Policies for Infrastructure-as-a-Service Clouds", in Proc.12th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing, pp. 612-619, 2012.004.