RESEARCH ARTICLE OPEN ACCESS

Analytics of Market Place Report and Accuracy Using Big-Data Applications

[1]P.Karthik

[1]Asst.professor, Dept.of.Computer science, PRIST University East campus, Thanjavur

Abstract:

In this paper, we discuss security issues for cloud computing in business side environment. The important views on security issues in cloud computing that are structural relationship (association) with big data. The Big data usages are a good used to organizations, business, companies and many large and small scale industries. We discuss various possible solutions for the problems in cloud computing security. Cloud computing security is developing at a fast pace which includes personal system security(self), network security, information security, and data privacy. Cloud computing plays a very main role in protecting data, applications and the related infrastructure with the help of policies, technologies, controls, and big data tools**.** Forever, cloud computing, big data and its tools, advantages are likely to represent the most promising new frontiers in the world.

Keywords — **Market, analysis, accuracy.**

Introduction:

The big challenge is Big Data. More specifically, how organizations will average Big Data analytics to maximize these developing information company assets by their yawning interest to large resources and better participate in the market place. While industries have practical incentives to make the most of their ever growing observation space (the data they have access to), they also have a pressing need to embed in these systems enhanced privacy protections. We outline in this paper just such an example how an advanced Big Data sense making technology was, from the ground up, company with security enhancing usages. Some features are so critical to accuracy that the team decided they should be compulsory so deeply served in the business side .

In order to complex data and to identify patterns it is very important to securely store, manage and share large amounts of complex data. Cloud comes with an explicit security challenge, the data owner power not have any control of where the data is placed. The reason behind this control issue is that if one wants to get the benefits of cloud computing, he/she must also utilize the allocation of resources and also the scheduling given by the controls. it is required to create the data in the of untrustworthy processes. Since cloud involves extensive complexity, we trust that slightly than providing a holistic solution to securing the cloud, it would be ideal to make worth able enhancements in securing the cloud that will ultimately provide us with a secure cloud. large volumes of data being generated each day, but at the same time can also create problems related to security, data access, monitoring, high availability and business continuity.

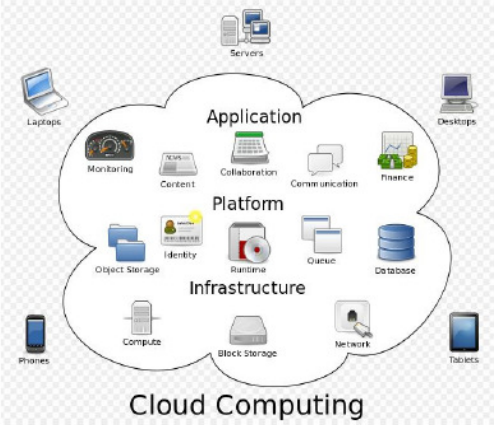
CLOUD COMPUTING:

Cloud Computing is a technology which depends on sharing of computing resources than having local servers or personal devices to handle the

applications. In Cloud Computing, the word "Cloud" means "The Internet", so Cloud Computing means a type of computing in which services are delivered through the Internet. The goal of Cloud Computing is to make use of increasing computing power to execute millions of instructions per second. Cloud Computing uses networks of a large group of servers with specialized connections to distribute data processing among the servers. Instead of installing a software suite for each computer, this technology requires to install single software in each computer that allows users to log into a Web-based service and which also hosts all the programs required by the user. There's a significant workload shift, in a cloud computing system. Local computers no longer have to take the entire burden when it comes to running applications. Cloud computing technology is being used to minimize the usage cost of computing resources The cloud network, consisting of a network of computers, handles the load instead. The cost of software and hardware on the user end decreases. The only thing that must be done at the user's end is to run the cloud interface software to connect to the cloud. Cloud Computing consists of a front end and back end. The front end includes the user's computer and software required to access the cloud network. Back end consists of various computers, servers and database systems that create the cloud. The user can access applications in the cloud network from anywhere by connecting to the cloud using the Internet. Some of the real time applications which use Cloud Computing are Gmail, Google Calendar, Google Docs and Drop box etc.,

Big data applications

The big data application refers to the large scale distributed applications which usually work with large data sets. Data exploration and analysis turned into a difficult problem in many sectors in the span of big data. With large and complex data, computation becomes difficult to be handled by the traditional data processing applications which triggers the development of big data applications Google's map reduce framework and apache are the defects software systems for big data applications, in which these applications generates a huge amount of intermediate data. Manufacturing and Bioinformatics are the two major areas of big data applications. Big data provide an infrastructure for transparency in manufacturing industry, which has the ability to unravel uncertainties such as inconsistent component performance and availability. In these big data applications, a conceptual framework of predictive manufacturing begins with data acquisition where there is a possibility to acquire different types of sensory data such as pressure, vibration, acoustics, voltage, current, and controller data. The combination of sensory data and historical data constructs the big data in manufacturing. This generated big data from the above combination acts as the input into predictive tools and preventive strategies such as prognostics and health management. Another important application for is Bioinformatics which covers the next generation sequencing and other biological domains. Bioinformatics which requires a large scale data analysis, uses Cloud computing gets the parallel distributed computing framework together with computer clusters and web interfaces. International



There are some common characteristics of big data, such as

a) Big data integrates both structured and unstructured data.

b) Addresses speed and scalability, mobility and security, flexibility and stability.

c) In big data the realization time to information is critical to extract value from various data

sources, including mobile devices, radio frequency identification, the web and a growing list of automated sensory technologies. The combination results in the exploration of these four areas:

a) Calculate the risks on large portfolios

b) Detect, prevent, and re-audit financial fraud

c) Improve delinquent collections

d)Execute high value marketing campaigns

Need of security in big data

For marketing and research, many of the businesses uses big data, but may not have the fundamental assets particularly from a security perspective. If a security breach occurs to big data, it would result in even more serious legal repercussions and reputational damage than at present. In this new era, many companies are using the technology to store and analyze pet bytes of data about their company, business and their customers. As a result, information classification becomes even more critical. For making big data secure, techniques such as encryption, logging, honey pot detection must be necessary. In many organizations, the deployment of big data for fraud detection is very attractive and useful. The challenge of detecting and preventing advanced threats and malicious intruders, must be solved using big data style analysis. These techniques help in detecting the threats in the early stages using more sophisticated pattern analysis and analyzing multiple data sources. Not only security but also data privacy challenges existing industries and federal organizations. With the increase in the use of big data in business, many companies are wrestling with privacy issues. Data privacy is a liability, thus companies must be on privacy defensive. But unlike security, privacy should be considered as an asset, therefore it becomes a selling point for both customers and other stakeholders. There should be a balance between data privacy and national security.

CHALLENGES AND ISSUES:

Cloud computing comes with number of security issues because it very large and many technologies including networks, databases, virtualization, resource planning, transaction management, load balancing, concurrency control and memory management. And security issues of these systems and technologies are applicable to cloud computing. it is very important for the network which interconnects the systems in a cloud to be privacy. And virtualization in cloud computing results in several security concerns. For example, mapping of the virtual machines to the physical machines has to be performed very securely

- The challenges level involve:
- Network connection level
- Encryption process
- Information store level

Cloud computing segment a large amount of processing involve acceptance still the maintenance big data services. The whole

organization used to all big data computerized work so issues involve many possible what are they:

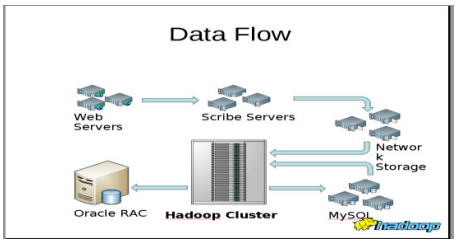
1.different types of technologies:

Cloud consist which many interact data base process that using technologies is very stuff more than person used to that system so security is weakness so any update to new technologies not possible to regular access

2.security tool and key:
Traditional tool is developed is every year so can not apply directly to this distribute cloud computing tools

3.authorized person:
In the person absence that time access to other unauthenticated can actively company records , modify or delete user data it's very difficult find one the problem the internal user can do access to without getting wedged.

4. approved rights:
In this problem admin rights can access any data. But uncontrolled access to any data very danger in critical user data.



The proposed access to this stage:
In this time meet various security in cloud based environment. The solution encourage specify lot of use security measurement in the cloud system:

Format and maintenance:
Document in which All the application software and new software should be updated to make the system more secure.

2. Data Encryption

Since the data is present in the machines in a cluster, a hacker can steal all the critical information. Therefore, all the data stored should be encrypted. Different encryption keys should be used on different machines and the key information should be stored centrally behind strong firewalls. This way, even if a hacker is able to get the data, he cannot extract meaningful information from it and misuse it. User data will be stored securely in an encrypted manner.

3.Operator Logging
All the map reduce jobs which modify the data should be logged. Also, the information of users, which are responsible for those jobs should be logged. These logs should be audited regularly to find if any, malicious operations are performed or any malicious user is manipulating the data in the nodes.

4. **Authentication access:**

Whenever a node joins a cluster, it should be authenticated. In case of a malicious node, it should not be allowed to join the cluster. Authentication techniques like Kerberos can be used to validate the authorized nodes from malicious ones.

Conclusion:
Cloud environment is widely used in industry and research aspects; therefore security is an important aspect for organizations running on these cloud environments. Using proposed approaches, cloud environments can be secured for complex business operations and their future process how to manage large company and cost data mining system service then big data support to very curial

service for database access and secure communication process .

Reference:

[1] J. Bennett and S. Lanning. The netix prize. In
Proceedings of KDD Cup and Workshop, volume 2007,
page 35, 2007.
[2] G. Chittaranjan, J. Blom, and D. Gatica-Perez.
Mining large-scale smartphone data for personality
studies. Personal and Ubiquitous Computing,
published online Dec. 2011.
[3] T. Do and D. Gatica-Perez. Contextual conditional
models for smartphone-based human mobility
prediction. In Proc. ACM Int. Conf. on Ubiquitous
Computing, Pittsburgh, Sep. 2012.
[4] N. Eagle, A. Pentland, and D. Lazer. Inferring
friendship network structure by using mobile phone
data. Proceedings of the National Academy of
Sciences, 106(36):15274{15278, 2009.
[5] M. C. Gonzalez, C. A. Hidalgo, and A.-L. Barabasi.
Understanding individual human mobility patterns.
Nature, 453(7196):779{782, June 2008.