JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

REVIEW OF TECHNIQUES USED WITHIN LI-FI ALONG WITH THEIR COMPARATIVE ANALYSIS

Sandhya
M.tech Research Scholar
Golden College of Engineering and Technology
Gurdaspur

Mohit Trehan
Assistant Professor
Golden College of Engineering and Technology
Gurdaspur

ABSTRACT

The Traffic Scheduling technique is commonly used in order to facilitate humans through act of technology. Cloud and Internet of Things found its application in this area. As technology provides advantages but it also suffers from some limitations. Faults and failures are commonly let backs of cloud and Iot. The proposed work analyse the technique offered with the help of Traffic Scheduling along with comparative analyse of each. The Traffic Scheduling technique area of application is also presented through the proposed work.

Keywords: Traffic Scheduling, Cloud, Internet of Things, Faults, Failures.

1. INTRODUCTION

Cloud computing and Iot are two different trending technologies used for monitoring traffic. This research highlights some of the applications associated with cloud and Iot in the field of traffic prediction. Cloud computing is ubiquitous computing built on virtualization technologies such as VMs, resources is accessible on-demand [1]. Some essential characteristics of cloud are broad network access, on-demand access of services, shared pool of resources etc. Another revolution to create and store data from different sensors that are connected via internet is internet of things [1]. This enormous amount of data has to be stored, processed and requires some platform. Cloud Computing provide virtual infrastructure for this data. Cloud Computing and Iot are complementary technologies merged together referred as Cloudlet [2]. Some of the key issues in Cloudlet involves energy efficiency, resource allocation, protocol support, IPv6 deployment, location of data storage, security and privacy [3].

Faults are also there in Cloudlet while predicting traffic. A fault is the cause of error and error leads to failure [4]. Different categories of faults in Iot and cloud are crash faults (machine stops functioning), measurement faults (invalid values sent by sensor due to software and hardware failures) [5], transmission faults (network level) and byzantine faults (arbitrary faults, unpredictable behaviour of machines). Sensor faults can also lead to abnormal behaviour. Three type of faults observed in real deployment are SHORT faults, NOISE faults and CONSTANT faults [6]. Four methods used for these fault detection are rule-based methods, estimation methods, time-series analysis-based methods and learning based methods. Similarly at network level we deal with different faults like congestion and link failure.

Resiliency techniques are used at application and infrastructure level. Fault tolerant and resiliency techniques serve effectively for reliability and availability.

1.1 CLOUD COMPUTING

Cloud computing is ubiquitous computing having virtually unlimited storage and processing capabilities and also cost effective means pay according to the usage while predicting traffic. Cloud computing provides three categories of service model: Software as a Service (SaaS) provides different applications available for user on pay-as-you-go basis, Platform as a Service (PaaS) provides platform to all these applications and Infrastructure as a Service (IaaS) provides

computation, storage and resources and also makes the data accessible over internet anywhere. The internet is the primary requirement while predicting traffic with cloud.

Different types of cloud are reported as:

I. Private Cloud: Used, owned, managed by particular organization

II. Public Cloud: For general public

III. Community Cloud: For a particular community that have same ideas ad concerns

IV. Hybrid Cloud: combining two or more different infrastructure

Issues related to each type have its own benefits and drawbacks. CAPEX (Capital Expenses) and OPEX (Operational Expenses) are less.

1.2 INTERNET OF THINGS

The key technologies used in Iot that came before Iot are:

1. **RFID (Radio Frequency Identification):**
RFID system uses radio waves, microwaves or sensors for communication. It consist of one or more readers and several tags, helps in automatic identification of anything. It recognizes high speed moving objects, identify multiple targets simultaneously and has low power consumption and high reliability.

2. **Wireless Sensor Network:**
Iot is represented by sensor networks communicating in multi-hop fashion. Large amount of data obtained is used in multiple fields. Instead of having multiple benefits some of issues related to their communication range, security, storage capacity, processing capabilities are there. These issues are solved by integrating cloud with Iot.

3. **Addressing:**
Unique address is given to large number of objects that are controlled by internet and helps in interconnection of objects. They are uniquely addressed by IPV4 as well as IPV6. IPV6 is not rarely used.

4. **Middleware:**
Main purpose of middleware is service management. It helps in the abstraction of the functionalities and communication capabilities of devices.

Internet of Things (Iot):
Then comes Iot which is interconnection of things in the world-wide network with reliable transmission, accurate control, intelligent processing and other characteristics by RFID, Wireless Sensor Network, addressing and middleware. All daily life things (such as food, paper, clothing, furniture etc.) are involved in Iot. These devices are called as sensors or actuators. It is expected that 24 billion things will be connected by 2020.

1.3 CLOUD AND IOT INTEGRATION (Cloudlet)

Cloud computing and Iot are complementary but their integration gives better platform. Iot get benefit from virtually unlimited capabilities and resources as cloud offers solution for services and application that produces large amount of data. Cloud get benefit by real world things. Cloud is basically based on the concept of virtualization. Now,the scope of cloud become distributed and dynamic that deals with real life things. It gives rise to a new term “Everything as a service”.

1.4 FAULTS, ERROR AND FAILURE

Faults, error and failure are inter-related terms. Faults give rise to errors and then errors lead to failure.

Fault -------- Error -------- Failure

Faults make system state stop. Errors give rise to improper functioning and lead to failure. Failure can be at servers and at network level in the cloud. In Iot, faults can occur at sensors as well as network level.

Different types of faults are surveyed:

1. **CRASH FAULTS:** Makes system totally crash and sensors stop working. These faults arise due to power outage, hard disk crash, high environmental temperature.

2. **MEASUREMENT FAULTS:** These faults are related to the values sent by sensors. Invalid values can be due to hardware or software and by any environmental condition. As an example if there is deviation of antenna of sensor from its place.

3. **TRANSMISSION FAULTS:** Network level faults are transmission faults. Any congestion and packet loss lead to transmission faults. Transmission faults occur when any obstacle stops the radio wave transmission.

4. **BYZANTINE FAULTS:** When behavior of system become unpredictable. These are arbitrary faults. System does not stop its working but it behaves abnormally.

Some of the sensor faults are :

- **SHORT FAULTS:** When there is sharp change in the measurement of two values.
- **NOISE FAULTS:** As short faults affect single sample reading, noise faults affect number of successive readings.
- **CONSTANT FAULTS:** Constant values are either very high or low in comparison to normal value. When sensor gives constant value for large number of successive readings, it is constant faults.

These faults are caused due to damaged sensors, short- circuit, low battery and calibration errors. Combination of noise and constant faults is the result of low battery voltage.

The performance degradation of sensors is also observed by injecting faults artificially. Artificially injection of faults means injecting datasets of varying intensity.

Network level faults are:

- **LINK FAILURE:** It changes the network topology.
- **CONGESTION:** Congestion leads to packet loss. Multiple routes help in congestion reduction.
- Faults have impact on the services offered by cloud Iot. There are some techniques in which system working not get affected during any fault. These are called as fault tolerant techniques. Fault tolerance is the ability of system to perform properly in the presence of faults. It improves the system performance and make the system reliable and available.

2. LIETRATURE SURVEY

To prove the worth of this dissertation work literature survey is conducted. This survey is presented in this section.
Wadhwa and Bala (2016) [7] proposed fault tolerance that can be used to resolve and handle the issues like reliability and availability. Different types of faults and traffic prediction techniques in cloud computing have been discussed. Further, various faults have been analyzed through Nagios monitoring tool.
Guillet et. al. (2016) [8] described work that aims at improving the security of the environment through a design methodology involving formal synthesis techniques. Reconfigurable controller is considered as a mean to provide traffic prediction mechanism.
Cook et. al. (2009) [9] conducted a survey of the technologies that comprise ambient intelligence and of the applications that are dramatically affected by it. In particular, focus is on the research that makes AmI technologies intelligent. The challenges and opportunities that Aml researchers will face in the coming years is also described. Ambient Intelligence is fast establishing as an area where a confluence of topics can converge to help society through technology.
Sajid et. al. (2016) [10] presented this paper as to highlight the security challenges that industrial SCADA systems face in an IoT-cloud environment. Classical SCADA systems are already lacking in proper security measures; however, with the integration of complex new architectures for the future Internet based on the concepts of IoT, cloud computing. The objective of this study was to highlight some important facts about industrial SCADA with an emphasis on threats, vulnerabilities, management and the current practices being followed.

Radhakrishnan (2012) [11] outlines an approach that enables an application to leverage the vast capacity and elasticity of the cloud to mitigate the deleterious effects of resource exhaustion at a node. This paper submits that an algorithm based on flow dynamics may provide a viable solution to the problem of automatic scaling of applications in the cloud.
Wang et. al. (2014) [12] discussed the performance of a cloud based multimedia system using retrying for traffic prediction is studied. We conducted the performance analysis of the media cloud based multimedia system using the retrying fault recovery technique.
Perspective et. al. (2012) [13] introduced an innovative, system level, modular perspective on creating and managing traffic prediction in clouds. We presented an approach toward transparently delivering traffic prediction on the application deployed in virtual machine instance.
Hua et. al. (2016) [14] proposed an efficient remote communication services, called Neptune. Neptune efficiently transmits massive data between long distance data centres via a cost effective filtration scheme. In order to offer efficient remote communication in cloud backups, this paper proposed a cost effective backup framework called Neptune.
Zhu et. al. (2016) [15] described that clouds are becoming an important platform for scientific workflow applications. Therefore traffic prediction in clouds is extremely essential. This paper offer backup facility over the cloud s called Neptune. For cloud backup services are to be designed that include local duplication and network data compression.
Xu and Huang (2016) [16] analysed the errors that occur in the virtualization of cloud computing. We develop a simulation based framework that enables a comprehensive study of traffic prediction. It uses the Xen hypervisor that compare different crash samples that occur due to error. It gives in depth study of soft error propagation.

2.1 Research Gap

In techniques that are explained above in the literature survey has defined different traffic prediction methods while predicting traffic. In these methods the various algorithms like remote computing, Neptune etc. All these methods give traffic prediction methods that are not energy efficient. In our proposed model we gives a strategy that is used to mange fault along with least energy consumption while predicting traffic for prolonged lifetime.

2. COMPARISON OF VARIOUS TECHNIQUES ALONG WITH ADVANTAGES AND DISADVANTAGES

Reference	Advantages	Disadvantages	Technique used
[17]	1. Concurrent task handling is proposed for traffic prediction. 2. Fault tolerance at run time is proposed for traffic prediction.	1. Sensor faults common in cloud are not handled. 2. Energy Efficiency is not considered .	Virtual Actor Model
[18]	1. Cost Effective in nature. 2. DC faults are handled efficiently .	Only voltage fluctuations are considered as a source of faults.	Cost effective Voltage source converter
[19]	1. Probabilistic approach to detect faults in control area network is proposed 2. Cost effective approach is proposed.	Energy efficiency is not considered.	Probabilistic approach
[20]	1. Online Fault handling mechanism is proposed. 2. Fault classification is also handled.	Energy consumption is not considered as parameter.	Online Fault tolerant Model.
[21]	1. Method to handle faults in Analog environment is proposed. 2. The experimental result verifies validity of this approach.	Energy efficiency is an issue not tackled in this environment.	Fault tolerant capability for Analog Circuit.

3. CONCLUSION

The proposed work deals with the study of various techniques along with limitations that are introduced as a result of advancement in technology associated with Traffic Scheduling. The comprehensive survey of existing techniques present today is described through this work. Comparative analysis also indicate best possible technique which can be used in future endeavours.

4. References

[1] K. N. Suchetha and H. S. Guruprasad, "Integration of IOT , Cloud and Big Data GLOBAL JOURNAL OF ENGINEERING SCIENCE AND RESEARCHES," no. October, 2016.

[2] R. Sandhu and S. K. Sood, "SPECIAL ISSUE PAPER A stochastic game net-based model for effective decision-making in smart environments," 2016, doi: 10.1002/cpe.

[3] L. Catarinucci *et al.*, "An IoT-Aware Architecture for Smart Healthcare Systems," *IEEE Internet of Things Journal*, vol. 2, no. 6, pp. 515–526, Dec. 2015, doi: 10.1109/JIOT.2015.2417684.

[4] F. T. Systems and E. Dubrova, "Faults , Errors and Failures Dependability tree Examples of failures • eBay Crash • eBay : giant internet auction house".

[5] M. Zhang, H. Jin, X. Shi, and S. Wu, "VirtCFT : A Transparent VM-Level Fault-Tolerant System for Virtual Clusters," pp. 147–154, 2010, doi: 10.1109/ICPADS.2010.125.

[6] P. Ulbrich, M. Hoffmann, R. Kapitza, D. Lohmann, and W. Schröder-preikschat, "Eliminating Single Points of Failure in Software-Based Redundancy," pp. 49–60, 2012, doi: 10.1109/EDCC.2012.21.

[7] A. Wadhwa and A. Bala, "Preventing Faults : Fault Monitoring and Proactive Fault Tolerance in Cloud Computing," pp. 665–673, doi: 10.1007/978-981-10-0129-1.

[8] S. Guillet, B. Bouchard, and A. Bouzouane, "Safe and Automatic Addition of Fault Tolerance for Smart Homes Dedicated to People with Disabilities," 2016, doi: 10.1007/978-3-319-30184-6.

[9] D. J. Cook, J. C. Augusto, and V. R. Jakkula, "Ambient intelligence : Technologies , applications, and opportunities," *Pervasive and Mobile Computing*, vol. 5, no. 4, pp. 277–298, 2009, doi: 10.1016/j.pmcj.2009.04.001.

[10] A. Sajid, H. Abbas, and K. Saleem, "Cloud-Assisted IoT-Based SCADA Systems Security : A Review of the State of the Art and Future Challenges," vol. 3536, no. c, 2016, doi: 10.1109/ACCESS.2016.2549047.

[11] G. Radhakrishnan, "Adaptive Application Scaling for Improving Fault-Tolerance and Availability in the Cloud," vol. 17, no. 2, pp. 5–14, 2012, doi: 10.1002/bltj.

[12] C. Wang, S. Member, L. Xing, S. Member, and H. Wang, "Performance Analysis of Media Cloud-Based Multimedia systems With Retrying Fault-Tolerance Technique," Vol. 8, no. 1, pp. 313-321, 2014.

[13] A. S. Perspective, R. Jhawar, G. S. Member, and V. Piuri, "Fault Tolerance Management in Cloud Computing :," pp. 1–10, 2012.

[14] Y. Hua, S. Member, X. Liu, and D. Feng, "Cost-Efficient Remote Backup Services for Enterprise Clouds," vol. 3203, no. c, pp. 1–8, 2016, doi: 10.1109/TII.2016.2543258.

[15] X. Zhu, J. Wang, H. Guo, D. Zhu, and T. Laurence, "Fault-Tolerant Scheduling for Real-Time Scientific Workflows with Elastic Resource Provisioning in Virtualized Clouds," vol. 9219, no. c, 2016, doi: 10.1109/TPDS.2016.2543731.

[16] X. Xu and H. H. Huang, "On Soft Error Reliability of Virtualization Infrastructure," vol. 9340, no. c, pp. 1–13, 2016, doi: 10.1109/TC.2016.2560817.

[17] P. A. Bernstein and S. B. Microsoft, "Developing Cloud Services Using the Orleans Virtual Actor Model," pp. 71–75, 2016.

[18] A. Hassanpoor, Y. Häfner, A. Nami, and K. Vinothkumar, "Cost-Effective Solutions for Handling Dc Faults in VSC HVDC Transmission Keywords," no. Mmc.

[19] M. Badril *et al.*, "Error Handling Algorithm and Probabilistic Analysis under Fault for CAN-based Steer-by-Wire System," vol. 3203, no. c, pp. 1–18, 2016, doi: 10.1109/TII.2016.2543232.

[20] K. Shibin, S. Devadze, and A. Jutman, "On-line Fault Classification and Handling in IEEE1687 based Fault Management System for Complex SoCs," pp. 69–74, 2016.

[21] C. Yang, S. Tian, B. Long, and F. Chen, "Methods of Handling the Tolerance and Test-Point Selection Problem for Analog-Circuit Fault Diagnosis," vol. 60, no. 1, pp. 176–185, 2011.