International Journal of Future Generation Communication and Networking
Vol. 13, No. 4, (2020), pp. 1564–1573

Perspective view of Cloud Computing Architecture with Internet Technologies for Real Time Applications

T.Pradeep[#1] Dr.D.Hari Prasad[#2]

[#1]*Assistant Professor, Department of Computer Applications, Sri Ramakrishna College of Arts and Science*
[#2]*Professor and Head, Department of Computer Applications, Sri Ramakrishna College of Arts and Science*
tpradeep@srcas.ac.in dhp@srcas.ac.in

Abstract

This paper describes the concept of cloud computing and the key characteristics possessed by it. It also explains the stack of three services provided and the technologies behind it which includes virtualization as prominent. This also outlines the deployment models and security features provided by it. Cloud computing is a technology to share the data and resources used among various organizations, but the security and privacy are most important aspects of cloud computing. The main responsibility of cloud service provider is the quality of service. Many of the cloud computing security frameworks have faced many challenges in security that has not yet been addressed well. The data accessed and shared through many devices from the cloud environment are not secure because they are likely to have various attacks like Identity Access Management (IAM), hijacking an account or a service either by internal/external intruders. In this paper, we proposed a model-driven approach enables of security requirements at the modelling layer and facilitates a transformation based on security configuration patterns.

Keywords: *Service Models, Deployment Models, Cloud Technologies*

1. INTRODUCTION

Cloud computing, commonly called as 'cloud' has been a buzz word of today's IT industries. But there is no complete understanding of this word and the exact benefits achieved by implementing this technology. But this 5th generation of computing is gaining momentum in many companies as big IT corporate such as IBM, Amazon ,Microsoft are pushing this new technique in great pace, which has started around in early 1990's. According to the National Institute of Standards and Technology (NIST) cloud computing is defined as a model for enabling ubiquitous network access to a shared pool of configurable computing resources. The main technology that paved the way for this methodology is the INTERNET, without which sharing of resources, accessing data from remote location, globalisation of information is impossible.

Commonly, cloud computing is pay-per-use worldview to empower fitting on-request arrange access to a mutual pool of configurable registering assets for example systems, servers, applications, and so forth., that can be quickly provisioned and discharged with the ideal administration exertion or specialist co-op interface. Numerous associations can remodel to cloud computing for social event its solicitations as customers and friends can utilize applications with no framework and access their private archives at any PC with Internet get to [1]. For the most part, distributed computing includes three distinct administrations, for example, Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS). Every equipment framework segments are virtualized into virtual elements. Virtualization implies a procedure that encourages execution of various Operating Systems (OSs) together on one

ISSN: 2233-7857 IJFGCN

Physical Machine (PM). These OSs are detached from one another and from the center physical framework utilizing a Virtual Machine (VM) [2].Cloud computing has numerous difficulties at expanding the quantity of clients since the interest of assets assignment and usage are expanded quickly. Accordingly, Load Balancing (LB) between assets is the most significant test [3]. For the most part, LB is the way toward doling out and reassigning the remaining burden among every accessible asset that amplifies the throughput, asset utilization and vitality sparing while at the same time diminishing the expense and reaction time. Astounding LB systems may give the Service Level Agreement (SLA) and customer experience. In this way, the development of powerful calculations and procedures for LB is a primary part of distributed computing frameworks. Various explores have been done in the zone of LB and assignment planning for cloud frameworks [4-5].

In the modern decades, worldwide presentation is transforming into a novel hypothesis at field of processing called osmotic figuring following the compound osmotic conduct hypothesis. Osmotic processing is basically used to accomplish adjusted organization in profoundly dispersed frameworks. In cloud computing frameworks, assimilation figuring is created to give adjusted VMs that are moved in the cloud frameworks [6-7]. In LB frameworks, however a few bio-enlivened calculations like Ant Colony Optimization (ACO), and so on., may check their effectiveness, the greater part of them need accomplishing better results in all qualities. Accordingly, a crossover meta-heuristics technique was proposed by joining the osmotic trademark and bio-roused LB calculations [8]. The osmotic trademark was utilized to empower a programmed arrangement of VMs that are relocated by means of cloud frameworks. Likewise, the constraints of traditional bio-motivated calculations were settled by hybridizing the Artificial Bee Colony (ABC) and ACO in the cloud computing.

Cloud computing is a relatively new business model for outsourced services. However, the technology behind cloud computing is not entirely new. Virtualization, data outsourcing, and remote computation have been developed over the last 20 years, and cloud computing provides a streamlined way of provisioning and delivering such services to customers. In this regard, cloud computing has often been criticized as representing just a new trend, rather than an innovative computing technology. As such, it is often best described as a business paradigm or computing model rather than any specific technology. A cloud consumer adopting a cloud-based solution needs to follow these steps:

1. Describe the service or application for which a cloud-based solution may be leveraged
2. Identify all functional capabilities that must be implemented for this service
3. Identify the security and privacy requirements and the security controls needed to secure the service or application.

The trust relation between cloud customers (CCs) and cloud service providers (CSPs) has to be established before CCs move their information systems to the cloud. This requires an in-depth understanding of associated risks. Moreover, regulations related to data protection, financial reporting, etc. involve certain requirements that should be complied with when outsourcing business processes to third parties, like CSPs. User authentication and authorization among cloud actors is a critical element of cloud architecture. Without knowing who is logging into the cloud-based information system, and who is accessing what data, cloud actors are not able to protect the data housed by a cloud ecosystem. Understanding who the users are, what data they are trying to access, where the data are stored, and how are users trying to get to these data—these are critical pieces of information that help cloud consumers determine an appropriate cloud architecture and deployment model.

2. WHY CLOUD

ISSN: 2233-7857 IJFGCN

This part describes the need for cloud technology, As the internet sprang up, the amount of data increased day by day and many new methodologies were needed to increase the speed of access and to manipulate (store and retrieve) the data efficiently. The Operating Systems subject has clearly stated a point that the efficiency of the processors and other hardware components are not utilised completely. Hence different techniques such as Time Sharing, Batch Processing are been implemented. Even though these techniques use the resources efficiently, still there is a void in the concept. Apart from this today everything has been networked and the IT industries want to serve their customers at any place. This makes the concern to scale their business to a wide area. Scaling involves many pre planned activities such as to buy the required hardware and software components to deploy their service. This is a very cost consuming process which the business needs to reduce. The reason that is the result of scaling process is maintenance. Once the required resources are been deployed and implemented it has to be maintained to achieve the desired result by the company. Again this is also an high expense for the concern. Along with this thinking from the social and environmental perspective, buying new resources and deprecating significantly increases the amount of e-waste which is an environmental hazard. All these reasons needed something as a result and that is what cloud technology is?

3. SERVICE MODELS

The service models are nothing but the type of services provided by the cloud providers. Based on the needs of the business concerns the services are provided in three types

1 .Infrastructure as a Service

This service shortly called as IaaS provides all the resources that are needed to setup the business infrastructure. It includes various components such as networking, storage, servers, operating systems, virtual machines (VM's). IaaS cloud providers supply these resources on-demand from their large pools of equipment. Eg: AmazonElasticCloud (EC2), Rack space.

2. Platform as a Service

The next level up from IaaS is PaaS where the cloud providers not only take care of the components provided by IaaS but also manages the platform – level components and methods like middleware (IIS, Tomcat, JBoss .) and runtime(.Net framework ,java runtime) will be pre-installed. The customer can just focus on developing and managing application and data related to it. Eg: GoogleAppEngine, Windows Azure Platfrom.

3. Software as a Service

The most common service is the SaaS where all the business activities are run in cloud and all portions are managed by the cloud providers itself>They take care of everything from the application to networking. The firms need not pay for license but use the software's as service whenever needed and pays the vendors accordingly. Eg: Gmail, Google Docs, Office 365 All these applications provide a storage place for our files in the network thus enabling ubiquitous access of resources. Files include documents, images, videos etc.

4. DEPLOYMENT MODELS

The cloud deployment model specifies the type of cloud environment distinguished by the ownership, size and access. There are three types of cloud deployment models each with its own characteristics. They are discussed in the following paragraphs

1.Public Cloud

ISSN: 2233-7857 IJFGCN

Public cloud is the cloud service which is common to all users irrespective of the customers and firms. This service is usually provided by a third party provider and the ownership depends on the third-party who provides this service. Azure platform of windows is a typical example of the public cloud. But the major disadvantage of this model is sensitive data and applications cannot be held in public cloud as the security level is not at its maximum level

2. Private cloud

It is the cloud computing platform that is implemented within the corporate firewalls under the control of IT department .It provides same features as the public cloud but removes a number of objections to cloud computing such as access and control of data. Privacy and confidentiality of information is maintained here. All the access related decisions and problems are rested in the hands of the IT personals.

3. Hybrid cloud

This deployment model is the combination of both Public and private cloud. The organization can maintain its confidential information in the private cloud whereas the common files that are not so confidential can be implemented and accessed from the public cloud. This helps the organization to reduce the cost involved in this process.

5. TECHNOLOGIES BEHIND CLOUD COMPUTING

The previous part of the paper covered what is cloud computing, the need for cloud, types of services provided and the various deployment models. In this part, we discuss about the various pillars which forms the holding of this cloud technology. The technologies that are working behind the cloud computing platforms making computing flexible, reliable and usable are Virtualization, Service-Oriented Architecture, Grid Computing and Utility Computing

1. Virtualization

Virtualization is a technique which allows sharing single physical instance of an application or resource among multiple tenants. It does so by assigning a logical name to a physical resource and providing a pointer to that physical resource when demanded. The virtualization concept is been achieved in many resources such as Server virtualization, Client, network, storage and service virtualization. Each of this type is achieved by using application software's such as hypervisor (virtual machine monitor) and other to achieve virtualization. In this the server virtualization is the heart of cloud computing. This has made the optimized usage of available resources instead of buying a new one.

2. Service-oriented Architecture

The important technology behind the cloud computing is Service-oriented Architecture (SOA).This is a concept which provides every as service. This is possible by using the WSDL (Web services Description Language),UDDI(Universal Description Discovery and integration) and SOAP (Simple Object Access Protocol)messages. In this the business process are being given as web service by a third party providers. The client first searches for the services provided in the UDDI registry and find the service description in the WSDL. Then the needed service is invoked by sending appropriate SOAP messages which is based on XML language resulting in interoperability. Thus this made the accessing of resources by any type of clients say PC or Smart Phone, Laptop etc.

3. Grid computing

Grid is a distributed architecture of large numbers of computers connected to solve a complex problem. The difference between the distributed and grid is that in the former only particular resources are shared among some particular computers in the network but in the latter

ISSN: 2233-7857 IJFGCN

every resource is shared among all the computers thus turning a normal computer network into a powerful supercomputer. With the right user interface, accessing a grid computing system would look no different than accessing a local machine's resources. Thus the efficiency of a computer is increased with enormous processing power and storage capacity. Thus this concept helped in serving the customer's Request in very short period of time.

4. Utility computing

Utility computing is a basically a business model in which one company outsources part or all of its computer support to another company. It doesn't mean it includes only technical advice it includes everything from computer processing power to data storage. Thus this idea has contributed the concept of outsourcing the resource requirements to the third party vendors namely cloud service providers. Thus allowing companies to only pay for the computing resources they need and when it is needed.

6. CHALLENGES FACED IN CLOUD COMPUTING

Though cloud computing has changed the conventional method of accessing the resources (CAPEX model) into OPEX model, it faces challenges in many areas. They are described below.

1. Security & Privacy
Security and Privacy of information is the biggest challenge to cloud computing. Security and privacy issues can be overcome by employing encryption, security hardware and security applications.

2. Portability
This is another challenge to cloud computing that applications should easily be migrated from one cloud provider to another. There should not be vendor lock-in. However, it is not yet made possible because each of the cloud providers uses different standard languages for their platforms.

3. Interoperability
Application on one platform should be able to incorporate services from other platform. It is made possible via web services. But writing such web services is very complex.

4. Computing Performance
To deliver data intensive applications on cloud requires high network bandwidth, which results in high cost. If done at low bandwidth, then it does not meet the required computing performance of cloud application.

5. Buisness Tactics
It is necessary for cloud systems to be reliable and robust because most of the businesses are now becoming dependent on services provided by third-party.

7. ACCESS CONTROL

Traditional access control architectures are based on the assumption that data storage management is located within a trusted domain and the owner has adequate knowledge about the system. However, this assumption is no longer valid in the cloud computing paradigm. Multiple stakeholders are engaged as users within the cloud platform and have different levels of data access permission. As a result, a greater granularity of access control is required to ensure that each stakeholder has access to exactly what they are authorized and to ensure the privacy and confidentiality of the cloud-based services.

ISSN: 2233-7857 IJFGCN

Researchers and experts are mostly concerned about outside attackers when considering the security issues in distributed systems. Therefore, significant efforts have been made to keep the malicious attacker outside of the perimeter. Unfortunately, such efforts cannot always be effective in the cloud computing paradigm. The incident where Google fired engineers for breaking internal privacy policies confirms that attackers may reside within the service framework [1]. Carnegie Mellon University's Computer Emergency Response Team (CERT) defines a malicious insider as "A current of former employee, contractor, or business partner who has or had authorized access to a network and intentionally used that access in a way that negatively affect the confidentially, integrity, or availability of any information or information systems" [2]. Due to insider threats, cloud-based services are in serious risk of intellectual property theft, IT damage, and information leakage. Hence, security vulnerabilities emerging from insider threats should be addressed by policies, technical solutions, and proper detection methods

8 SECURING SERVICES IN THE CLOUD

Service-Oriented Architecture (SOA) is an architectural pattern, while cloud computing is a set of enabling technologies as a potential target platform or technological approach for that architecture. By combining SOA and cloud computing, it becomes possible to reduce the time taken to implement technology, enhance business performance and expose the existing legacy application over the Internet. The role of SOA in cloud computing is important because a successful cloud solution requires an in-depth understanding of the architecture, the services offered and how to leverage them. Cloud computing becomes part of the architectural arsenal to create a successful SOA.

Cloud services benefit the business by taking the best practices and business process focus of SOA. These benefits apply to both cloud service providers and cloud service users. Cloud service providers need to architect solutions by using a service-oriented approach to deliver services with the expected levels of elasticity and scalability. Companies that architect and govern business processes with reusable service-oriented components can more easily identify which components can be successfully moved to public and private clouds. A Service-Oriented Architecture (SOA) is a software architecture for building business applications that implement business processes or services through a set of loosely coupled, black-box components orchestrated to deliver a well-defined level of service.

Service-oriented architectures are based on the idea of exposing software functionality as services to be used by independent parties. Their inherent independence of a specific platform and operating system make them perfectly suitable to connect service consumers and service providers over the Internet and provide a technical foundation for cloud computing [3]. The combination of SOA and cloud computing facilitating the provision of composed application and services that integrate and orchestrate services from different sources pose new challenges to security. Since services and applications are exposed to the Internet and are used in a global context, the management of user identities across organisational borders is a key element to perform access control and to prevent unauthorised access in a decentralised environment.

Open Identity Management Models support the sharing of identity information across several trust domains in a controlled manner. Clients can request identity information from the identity management systems and convey this information in an interoperable format to a requesting party. Besides identity provisioning, confidentiality and integrity of exchanged, stored, and processed information must be ensured. Several specifications emerged to protect information at different layers. For instance, a secure channel can be used to protect exchanged information, while signature and encryption mechanisms applied to a message can also protect stored and processed information. These security requirements are stated in security policies that configure the secure interaction of participants in a service-based system. Policies facilitate the negotiation

ISSN: 2233-7857 IJFGCN

of security requirements between services and service clients to enable interoperability at runtime. This enables a seamless usage of services in the cloud to build composed applications.

However, due to the complexity of the involved specifications, the variety of security mechanisms and the flexibility of service-based systems, such policies are hard to understand and even harder to codify. To overcome these limitations, we foster a model-driven approach that generates security configurations based on system design models annotated with security requirements. To implement the functional and security requirements specified at the modelling layer, our cloud platform has to ensure two aspects: The system with all involved services and web application components must be instantiated in a virtual machine according to the functional requirements and the services must be configured in compliance with the modelled security requirements. As illustrated in Figure 1, our approach consists of three layers. Functional and security requirements, expressed at the modelling layer, are translated to a platform independent model. This model constitutes the foundation to setup the virtual machine, application server, services and composed applications that are provided to the user [4].

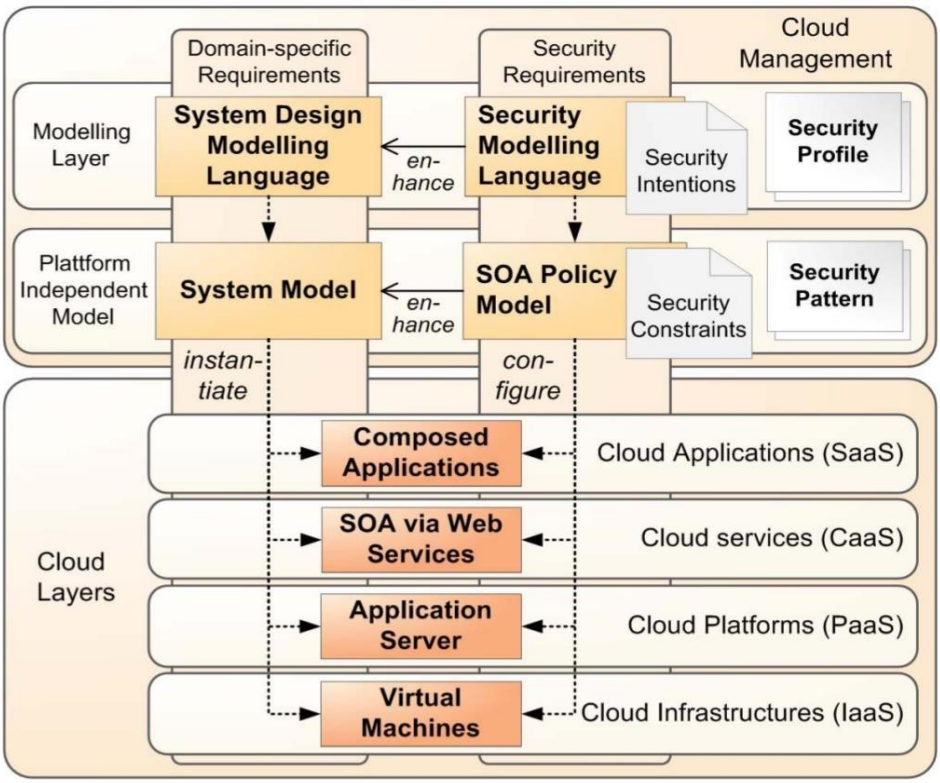

Fig -1: Model-driven Security in SOA

A Model-driven approach transforms security intentions to enforceable security policies. This transformation is based on a set of security configuration patterns that provide security expert knowledge to configure the system. Our model-driven approach requires an automated generation of enforceable security configurations based on the modelled security requirements [5].

9 DATA SECURITY AND PRIVACY IN CLOUD

Security and privacy concerns faced by the cloud consumers require them to evaluate the risk and its management in the cloud environment, then mitigating those risks. Of course, the most critical benefit offered by cloud computing is the reduction of business costs. Most

ISSN: 2233-7857 IJFGCN

businesses have well-established security objectives, strategies, and policies consistent with compliance requirements to protect their intellectual property, and their clients' data. Many security components come into play, but the most four critical components are shown in Figure 2. Data and transmission of data must take place through secured channels. Application and storage security both must be maintained by the cloud service provider.

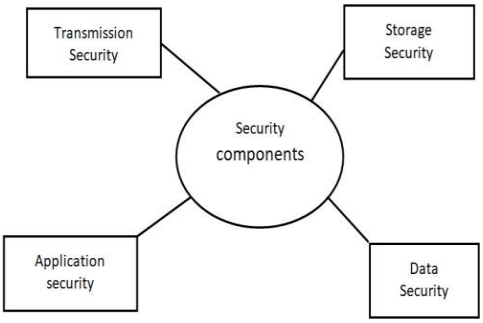

Fig -2: Security Components.

The storage data itself can be encrypted by many cloud service providers using server side encryption (SSE). This will encrypt the data on the cloud storage devices with strong cryptographic algorithms but the encryption keys stay with the cloud provider and are not under the control of the cloud customer. If nothing else is offered, the cloud server administrator should activate SSE per default for the cloud storage used. This encryption gives some basic protection against unauthorized access to the customer data but also means that the security of this solution depends on the cloud provider's ability to restrict access to the storage encryption keys even to other employees.

The cloud service provider should enforce the same or even higher levels of security controls as expected by the cloud customer or as best practice in the industry. There are logical risks of information disclosure or data integrity by having unsecure applications or permission handling functionalities. The application or underlying infrastructure could be open to exploits by hackers. The user permission and role model could be exploited as well by external hackers or internal employees that have too many access rights. In general, the same security measures need to be applied like in any IT system. The complexity arises from the cloud technology model that is based on virtualization and distributed responsibilities between the infrastructure layers. The cloud service provider must take care of physical and logical security that is in his sole responsibility. For example, the cloud service provider may offer encryption, but it is up to the customer to activate and use it. Clear responsibilities for network, operating system, and application security measures are key priorities to achieve such a secure cloud solution.

Cloud computing is yet to standardize the process of service metering. Therefore, service metering is not yet trustworthy to the cloud consumers. The process requires a systematic, verifiable, and reliable framework for cloud computing to be sustainable. Subsequently, the trust relationship of cloud service providers with customers and enterprises will be enhanced, resulting in a wider adoption of cloud-based solutions. Maintaining the privacy of users is of high concern for most organizations. Whether employees, customers, or patients, personally identifiable information is a high-valued target. Many cloud subscribers do not realize that when they contract a provider to perform a service, they are also agreeing to allow that provider to gather and share metadata and usage information about their environment. In some cases, providers even sell or share these data legally based on their privacy statements

ISSN: 2233-7857 IJFGCN

The evolving nature of cloud computing technologies has resulted in nonstandard security implementations and practices. Moreover, the lack of governance for audits creates a challenging environment to verify if the cloud service providers have complied with the standards. As a result, cloud computing security may not yet be ready for audits [6]. Users depend on the service level agreement (SLA) and have to rely on the cloud service provider to keep up their end of the bargain. However, cloud services are best effort services and a service provider may not guarantee the security standards. Therefore, as SLAs play a vital role in ensuring the security of the cloud-based services, governing bodies and security experts should be part of the SLAs and legal aspects, which is not yet seen to be in practice for cloud-based service models [7].

10 Conclusion

Thus the internet has created a new and embarking technology known as cloud which is a much optimized methodology of accessing resources. Even though the benefits are of higher rate there are some major problems to be rectified and the existing system can be enhanced in providing ways to easily shift from one cloud service to another. In future, interoperability which is achieved within the cloud can be taken one step ahead and can be made possible among various cloud providers. This creates a scenario that any type of service can be accessed by any client from anywhere and from any providers. This result is more optimization of the resources.

References

[1] Y. Ren, R. Werner, N. Pazzi, A. Boukerche, "Monitoring patients via a secure and mobile health-care system", IEEE Wirel. Commun. 17, pp. 59–65, 2010.

[2] J. R. Gallego, A. Hernandez-Solana, M. Canales, J. Lafuente, A. Valdovinos, J. Fernandez-Navajas, "Performance analysis of multiplexed medical data transmission for mobile emergency care over the UMTS channel", IEEE Trans. Inf Technol. Biomed. 9, pp. 13–22 2005.

[3] B. Arunachalan, J. Light, I. Watson, "Mobile agent-based messaging mechanism for emergency medical data transmission over cellular networks", 2nd International Conference on Communication Systems Software and Middleware, pp. 1–6, 2007.

[4] B.M. Prakoso,A.R.N. Pristy, M. Arsyad, A.B. Noegroho, A. Sudarsono, A. Zainudin, " Performance analysis of OLSR routing for secure medical data transmission for rural areas with Delay tolerant network", In: 2016 International Symposium on Electronics and Smart Devices (ISESD), pp. 51–56, 2016.

[5] O.H. Salman, M.F.A. Rasid, M.I. Saripan, S.K. Subramaniam, "Multi-sources data fusion framework for remote triage prioritization in telehealth", J. Med. Syst.38, 103, 2014.

[6] M. Werner, C. Pietsch, C. Joetten, C. Sgraja, G. Frank, W. Granzow, et al., 2009. Cellular in-band modem solution for ecall emergency data transmission. In: VTC Spring 2009 – IEEE 69th Vehicular Technology Conference, pp. 1–6, 2009.

[7] M. Aal-Nouman, H. Takruri-Rizka, M. Hope, "Transmission of medical messages of patient using control signal of cellular network", Telematics and Informatics, https://doi.org/10.1016/j.tele.2017.11.008, 2017.

[8] S. A. Hussain et al, "An Efficient Channel Access Scheme for Vehicular Ad Hoc Networks", Mobile Information Systems, Vol.2017, 2017.

[9] B. Yuanguo, "Neighboring vehicle-assisted fast handoff for vehicular fog communications", Special Issue on Fog Computing on Wheel. Springer, 2017.

ISSN: 2233-7857 IJFGCN

[10] S. Midya, "An Efficient Handoff Using RFID Tags. Proc. of Intl. Conf. on Intelligent Communication, Control and Devices", Advances in Intelligent Systems and Computing 47, pp. 779, 2016.

[11] Radio Link Control (RLC) protocol specification, 3GPP Tech. Specification 25.322 v5.4.0 (2003–03), 2002.

[12] S. Misbahuddin, R. Olson, J. A. Zubairi, M. Irfan, S. M. Arif, S. Mansoor, S. Saeed, Z. Irfan, "Client-Server Based Transmission Scheme over GSM Network for MEDTOC with Patient Classification", In: International Conference on Collaboration Technologies and Systems (CTS), pp. 176–179, 2012

[13] H. Huang, T. Gong, N. Ye, R. Wang, Y. Dou, "Private and Secured Medical Data Transmission and Analysis of Wireless Sensing health-care System", IEEE Trans. on Ind. Inf. 13, pp. 1227–1237, 2017.

ISSN: 2233-7857 IJFGCN