

Modeling a Securing software system as a Service Model

¹N.Priya, ²S.Pothumani,

^{1,2}, Assistant Professor,

Department of Computer Science and Engineering, BIST, BIHER, Chennai-73.

¹priya.cse@bharathuniv.ac.in, ²pothumani.cse@bharathuniv.ac.in

ABSTRACT

Cloud computing, doubtless, has become the hokum within the IT business these days. watching the potential impact it's on varied business applications further as in our existence, it will actually be same that this troubled technology is here to remain. several of the options that create cloud computing engaging, haven't simply challenged the present security system, however have additionally unconcealed new security problems. This paper provides associate degree perceptive analysis of the present standing on cloud computing security problems supported an in depth survey carried by the author. It additionally makes a trial to explain the protection challenges in software system as a Service (SaaS) model of cloud computing and additionally endeavors to supply future security analysis directions.

KEY WORDS:

Cloud Computing, software system as a Service, Security Challenges

I. INTRODUCTION

A lot has been written and spoken regarding Cloud Computing technology, by IT specialists, business and business leaders and freelance specialists. Whereas some believe it's a troubled trend representing subsequent stage within the evolution of the web, others believe it's plug, because it uses earlier established computing technologies. So, what precisely is cloud computing? From a user perspective, cloud computing provides a way for deed computing services with none would like for deep understanding of the underlying technology being employed. From associate degree structure perspective, cloud computing delivers services for shopper and business wants in an exceedingly

simplified way, providing infinite scale and differentiated quality of service to foster fast innovation and higher cognitive process. in line with Gartner [1-9], cloud computing is outlined as “a variety of computing, wherever massively ascendable IT- enabled capabilities square measure delivered ‘as a service’ to external customers victimization web technologies. in line with the Sercombe [2] and National Institute of Standards & Technology [10-15], pointers for cloud computing, it's four totally different readying models specifically personal, community, public and hybrid further as 3 totally different delivery models that square measure utilised inside a specific readying model. These delivery models square measure the SaaS (Software as a Service), PaaS (Platform as a Service) and IaaS (Infrastructure as a Service). These models type the core of the cloud and that they exhibit sure key characteristics like on demand self-service, broad network access, resource pooling, measured service and fast snap. Our main space of concern during this paper is that the software system as a service (SaaS). model This known branch of cloud computing , could be a delivery model during which applications square measure hosted and managed in an exceedingly service provider's datacenter, obtained on a subscription basis and accessed via a browser over an online association. It essentially deals with licensing of associate degree application to the shoppers to be used as a service on demand. One exemplar of SaaS is that the Salesforce.com CRM application.

This paper focuses on the problems associated with the service delivery model of cloud computing. The paper describes the assorted security problems with cloud computing with relation to its service delivery model SaaS[16-19]. The organization of the paper is as follows: Section a pair of describes the protection problems that square measure display by the software system as a Service (SaaS) delivery model. Section three lists a number of this solutions that part target the protection challenges display by the SaaS.

Section four provides conclusions derived out of the survey undertaken.

II. SECURITY problems IN SAAS

In software system as a Service (SaaS) model, the shopper should rely upon the service supplier for correct security measures. The supplier should make sure that the multiple users don't get to check every other's data. So, it becomes necessary to the user to make sure that right security measures square measure in situ associate degreed additionally troublesome to induce an assurance that the appliance are going to be out there once required [4]. whereas victimization SaaS model, the cloud client can, by definition, be subbing new software system applications for recent ones. Therefore, the main target isn't upon movableness of applications, however on protective or enhancing the protection practicality provided by the bequest application and achieving a productive knowledge migration [20-26] The SaaS software system merchant might host the appliance on his own personal server or deploy it on a cloud computing infrastructure service provided by a third-party supplier (e.g. Amazon, Google, etc.). the utilization of cloud computing in addition to the 'pay-as-you-go' approach helps the appliance service supplier scale back the investment in infrastructure services and permits it to target providing higher services to the shoppers. Enterprises these days read knowledge and business transactions as strategic and guard them with access control and compliance policies. However, within the SaaS model, enterprise knowledge is hold on at the SaaS provider's knowledge center, at the side of the info of different enterprises. Moreover, if the SaaS provider is investing a public cloud computing service, the enterprise knowledge could be hold on at the side of the info of different unrelated SaaS applications. The cloud supplier would possibly, in addition, replicate the info at multiple locations across countries for the needs of maintaining high availableness. Most enterprises square measure acquainted with the normal on- promise model, wherever the info continues to reside inside the enterprise boundary, subject to their policies. Cloud computing suppliers got to solve the common security challenges being baby-faced by ancient communication systems. At identical time, they even have to take care of different problems inherently introduced by the cloud computing paradigm itself.

within the following section, the SaaS security problems are categorised as ancient and new cloud specific security challenges, for sake of convenience. Figure one shows the assorted security problems in SaaS model that square measure mentioned within the paper.

2.1 a. Traditional Security Challenges

Although the protection issues in ancient communication systems additionally apply to the cloud, the utilization of cloud computing introduces new attack vectors that may create attacks either potential or just easier to hold out. a number of the normal security problems that additionally have an effect on the SaaS model are delineated below:

b. Authentication and authorization

The authentication and authorization applications for enterprise environments may have to be modified, to figure with a secure cloud surroundings. Forensics tasks might become rather more troublesome since the investigators might not be ready to access system hardware physically. the planning projected by Pratap Murukutla [27-31] permits user to use one set of credentials. they need projected an answer with de-facto standards of open authorization {in that|during which|within which} there's a trust party auditor which maintains all the credentials and cloud supplier will unambiguously distinguish one user from different. The model projected within the literature [6] verifies user credibleness victimization ballroom dancing verification, that is predicated on positive identification, smartcard and out of band (i.e. robust 2 factors) authentication. additionally, the theme additionally provides mutual authentication, identity management, session key institution, user privacy and security against several common attacks; but the formal security proofing hasn't nonetheless been formalized[32-37].

c. Availability

The availability ensures the reliable and timely access to cloud knowledge or cloud computing resources by the suitable personnel. the supply of cloud service suppliers is additionally an enormous concern, since if the cloud service is disrupted; it affects a lot of customers than within the ancient model. for example[38-41], the recent disruption of the Amazon cloud service within the year 2011, took

down variety of internet sites together with Reddit, Foursquare, and Quora. The SaaS application suppliers square measure needed to make sure that the systems square measure running properly once required and enterprises square measure supplied with services round the clock. This involves creating fine arts changes at the appliance and infrastructural levels to feature measurability and high availableness. Resiliency to hardware/software failures, further on denial of service attacks, must be designed from the bottom up inside the appliance. At identical time, associate degree applicable action set up for business continuity and Disaster Recovery (DR) must be thought-about for any exigencies as per the steerage provided by [42-45]. this can be essential to make sure the security of the enterprise knowledge whereas maintaining negligible period of time for the enterprises. With Amazon [7] for example, the Amazon internet Services (AWS) API finish points square measure hosted on identical Internet-scale, best infrastructure that supports the Amazon retail web site. commonplace Distributed Denial of Service (DDoS) mitigation techniques like synchronous cookies and association limiting square measure used. To any mitigate the result to potential DDoS attacks, Amazon maintains internal information measure that exceeds its provider-supplied web information measure.

d. Data confidentiality

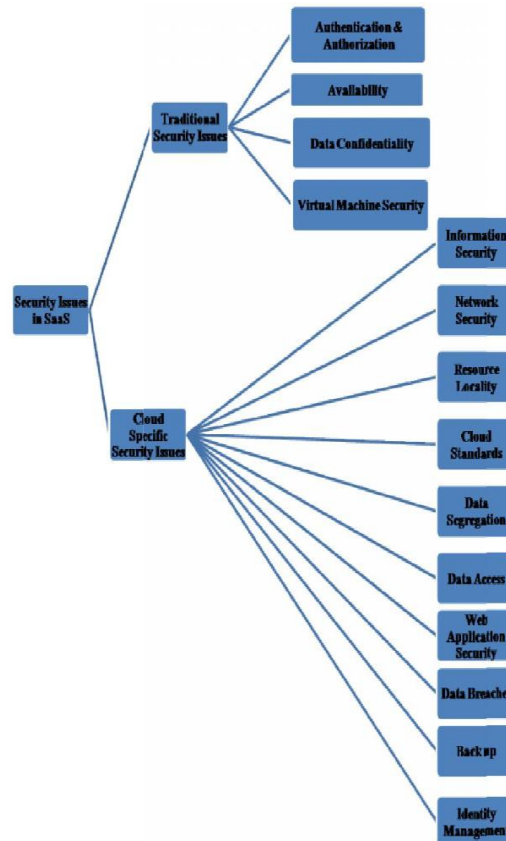
Confidentiality refers to the bar of intentional or unintentional unauthorized speech act of knowledge. Confidentiality in cloud system is expounded to the areas of belongings rights, covert channels, traffic analysis, encryption, and illation [10].

e. Virtual Machine Security

Although the worldwide adoption of virtualization could be a comparatively a recent phenomena, threats to the virtualized infrastructure square measure evolving even as quickly [8]. The hypervisor and virtual machines employed in cloud suppliers may have vulnerabilities, as exemplified by [14]. Such vulnerabilities represent a fair a lot of significant issue in multi-tenant environments, wherever compromise of even one virtual machine will have an effect on all users on identical physical server. Virtualization is one among the most parts of a cloud. however this poses major security risks. Cloud suppliers, therefore, would possibly got to

rethink ancient security concerns from totally different angles.

Figure 1: Security problems in SaaS



2.2 Cloud Specific Security Challenges

a. Information Security

In cloud vendors like Amazon, the Elastic work out Cloud (EC2) directors don't have access to client instances and can't log into the Guest OS. EC2 directors with a business would like square measure needed to use their individual cryptographically robust Secure Shell (SSH) keys to achieve access to a number [8]. All such accesses square measure logged and habitually audited. whereas the info at rest in straightforward Storage Service (S3) isn't encrypted by default, users will encode their knowledge before it's uploaded to Amazon S3, in order that it's not accessed or tampered with by any unauthorized party. Malicious users will exploit

weaknesses within the knowledge security model to achieve unauthorized access to knowledge.

b. Network Security

All knowledge flow over the network must be secured so as to forestall outflow of sensitive info. This involves the utilization of robust network traffic cryptography techniques like Secure Socket Layer (SSL) and also the Transport Layer Security (TLS) for security.

In case of Amazon internet Services (AWS), the network layer provides important protection against ancient network security problems, like MITM (Man-In-The-Middle) attacks, informatics spoofing, port scanning, packet sniffing, etc. for optimum security, Amazon S3 is accessible via SSL encrypted endpoints. The encrypted finish points square measure accessible from each the web and from inside AmazonEC2, guaranteeing that knowledge is transferred firmly each inside AWS and to and from sources outside of AWS [9]. However, malicious users will exploit weaknesses in network security configuration to smell network packets.

c. Resource Locality

This poses a possible downside once disputes happen, that is typically on the far side the management of cloud suppliers. attributable to compliance and knowledge privacy laws in numerous countries, neighborhood of knowledge is of utmost importance in abundant enterprise design [15]. the eu Union has issued a Directive 95/46/EC to shield the user privacy in any respect prices [16].

The directive prohibits transfers of private knowledge to countries that don't guarantee associate degree adequate level of protection. for instance, the recent Dropbox users got to conform to the "Terms of Service" that grant the suppliers the correct to disclose user info in compliance with laws and enforcement requests [17]. additionally to the problem of native laws, there's additionally the question of beneath whose jurisdiction the info falls, once associate degree investigation happens. A secure SaaS model should be capable of providing dependability to the client on the placement of the info of the patron.

d. Cloud standards

To achieve ability among clouds and to extend their stability and security, cloud commonplaces square measure required across totally different standard developing organizations. for instance, this storage services by a cloud supplier is also incompatible with those of different supplier. e.g. IEEE Cloud Computing commonplace Study cluster [18], ITU Cloud Computing Focus cluster [19], Cloud Security Alliance (CSA), Distributed Management Task Force [20], Storage Networking business Association [21], Open Grid Forum [22], Open Cloud syndicate [23] and Organization for the Advancement of Structured Information Standards [24], and then forth. to push the wide use of cloud computing, these standards bodies got to sit down and work along to ascertain common standards. Possible "Inter-cloud" standards within the following domains square measure required to extend cloud ability and free knowledge movement among clouds:

- specification,
- information,
- Metering and charge,
- Quality of Service,
- Resource provisioning,
- Security, identity management and privacy.

As stated, there square measure several general computing standards that will be reused within the cloud, except for the instant, there square measure to our data no dedicated cloud standards. this could augment the confusion for cloud users [25], and are some things that should be addressed within the future.

e. Data Segregation

Multitenancy is one among the main characteristics of cloud computing. As a results of multi-tenancy, multiple users will store their knowledge victimization the applications provided by SaaS. In such a state of affairs, knowledge of assorted users can reside at identical location. Intrusion of knowledge of 1 user by another becomes potential during this surroundings. This intrusion is done

either by hacking through the loop holes within the application or by injecting shopper code into the SaaS system.

f. Data Access

Data access issue is principally associated with security policies provided to the users whereas accessing the info. in an exceedingly typical state of affairs, atiny low business organisation will use a cloud provided by another supplier for concluding its business processes. This organization can have its own security policies supported that every worker will have access to a specific set of knowledge. the protection policies might entitle some concerns, wherein, a number of the workers don't seem to be given access to specific amount of knowledge [26]. These security policies should be adhered by the cloud to avoid intrusion of knowledge by unauthorized users [27].The SaaS model should be versatile enough to include the precise policies hints by the organization. The model should even be ready to give structure boundary inside the cloud as a result of multiple organization are going to be deploying their business processes inside one cloud surroundings.

g. Web application security

SaaS is software system deployed over the web and/or is deployed to run behind a firewall in native space network or laptop computer. The key characteristics embrace Network-based access to, and management of, commercially out there software system and managing activities from central locations instead of at every customer's web site, enabling customers to access application remotely via the Web. SaaS application development might use numerous sorts of software system parts and frameworks. These tools will scale back time-to-market and also the value of changing a standard on-premise software package or building and deploying a replacement SaaS resolution. Examples embrace components for subscription management, grid computing software system, internet application frameworks and complete SaaS platform product. one among the "must-have" necessities for a SaaS application is that it's to be used and managed over the online [28]. The software system that is provided as a service resides within the cloud while not docking with the particular users. this permits improvising the software system while not

inconveniencing the user. Security holes within the internet applications so produce a vulnerability to the SaaS application [29]. The Open internet Application Security Project [30] has provided the 10 most crucial internet applications security threats.

h. Data breaches

Since knowledge from numerous users and business organizations lie along in an exceedingly cloud surroundings, breaching into the cloud surroundings can doubtless attack the info of all the users. Thus, the cloud becomes a high price target [31]. within the Verizon Business breach report web log it's been explicit that external criminals create the best threat (73 percent), however reach the smallest amount impact (30,000 compromised records), leading to a Virtualization vulnerability [32].

i. Backup

The SaaS merchant must make sure that all sensitive enterprise knowledge is frequently protected to facilitate fast recovery just in case of disasters. additionally the utilization of robust cryptography schemes to shield the backup knowledge is usually recommended to forestall accidental outflow of sensitive information within the case of cloud vendors like Amazon, the info at rest in S3 isn't encrypted by default. The users got to one by one encode their knowledge and backups in order that it can't be accessed or tampered with by unauthorized parties.

j. Identity management and sign-on method

Once a SaaS supplier should savvy to manage United Nations agency has access to what systems inside the enterprise it becomes all the tougher task. In such situations the provisioning and de-provisioning of the users within the cloud becomes terribly crucial.

III. CURRENT SECURITY SOLUTIONS

There square measure many analysis works happening within the space of cloud security. many teams and organization have an interest in developing security solutions and standards for the cloud. The Cloud Security Alliance (CSA) is gathering resolution suppliers, non- profits and people to enter into discussion regarding this and future best practices for info assurance within the

cloud [11]. The Cloud Standards web site collects and coordinates info regarding cloud-related standards beneath development by the teams. The Open internet Application Security Project (OWASP) maintains list of prime vulnerabilities to cloud-based or SaaS models that is updated because the threat landscape changes [30]. The Open Grid Forum publishes documents to containing security and infrastructural specifications and data for grid computing developers and researchers [22]. the most effective security resolution for SaaS applications is to develop a development framework that has powerful security design. Tsai W [33], place forth a four-tier framework for web-based development that although appears attention-grabbing, solely implies a security aspect within the method. In his work, Berre [34] has prompt a road map towards cloud-centric development, and also the X10 language is one among the ways in which to realize higher use of cloud capabilities of large multiprocessing and concurrency [35]. Another approach is resource isolation to make sure security of knowledge throughout process, by analytic the processor caches in virtual machines, and isolating those virtual caches from the hypervisor cache [36]. One straightforward resolution, for GB businesses is to easily use in-house “private clouds” [37]. Pearson highlighted that this lack of transparency is preventing several users from reaping actuality advantages of the cloud [38]. For Identity and access management within the SaaS, [12] has issued associate degree Identity and Access Management steerage that provides an inventory of suggested best practices to assure identities and secure access management. Resource neighborhood and knowledge Segregation square measure the 2 key security challenges on that not abundant info is on the market within the existing literature, that necessitates that this could be any preoccupied for analysis.

Table 1: Current solutions out there for securing SaaS

S.No.	Security Areas	Current /Possible Solutions
1	Authentication and authorization	• Open Authorization [5] • Two Factor Authentication [6] • OAuth [39]
2	Availability	• Data Dispersion [8]
3	Data confidentiality	• Attribute based Proxy • Re-Encryption [40]
4	Virtual Machine Security	• Reconfigurable distributed virtual machine [41] • Survey on Virtual machine Security [42]
5	Information Security	• Information Security Risk Management Framework [43]
6	Network Security	• Network Security for virtual machines [44] • Network Security Sandbox [45]
7	Cloud standards	• IEEE Cloud Computing Standard Study Group [18] • ITU Cloud Computing Focus Group [19], • Cloud Security Alliance (CSA)
8	Data Access	• Multi-user access policies [46]. • Data Access Management [47].
9	Web application security	• Web Application Scanners [48]
10	Data breaches	
11	Backup	• Agentless Method for data Backup and Recovery [49]
12	Identity management and sign-on process	• CSA's Identity and Access Management Guidance [12]

IV. CONCLUSION

Though there square measure varied benefits in employing a cloud-based system, there square measure nonetheless several sensible problems that got to be sorted. Cloud computing could be a troubled technology with profound implications not just for web services however additionally for the IT sector as a full. Still, many outstanding problems exist, significantly associated with service-level agreements (SLA), security and privacy, and power potency. As delineated within the paper, presently security has heap of loose ends that scares away many potential users. till a correct security module isn't in situ, potential users won't be ready to leverage actuality advantages of this technology. This security module ought to cater to all or any the problems arising from all directions of the cloud. Each component within the cloud ought to be analyzed at each the macro associate degreed small level and afterwards an integrated resolution should be designed and deployed within the cloud to draw in and retain the potential shoppers. Until then, cloud surroundings can stay cloudy. In a cloud, wherever there square measure heterogeneous systems having a variation in their quality price, one security system would be too pricey surely applications and if there's less security then the vulnerability issue of some applications like money and military applications can increase. On the opposite aspect, if the cloud incorporates a common security methodology in situ, {it can't} be a high price quality target for hackers due to the very fact that hacking the protection system will create the complete cloud susceptible to attack.

In this paper an outline of cloud computing service delivery model, SaaS at the side of the protection challenges , together with each the normal and cloud specific security challenges ,associated with the model has been given variety of latest challenges that's inherently connected to the new cloud paradigm has additionally been deliberated within the paper. As secure knowledge storage in cloud surroundings could be a important concern that prevents several users from victimization the cloud, a sensible resolution to supply security and privacy for user knowledge, once it's placed in an exceedingly public cloud, was additionally mentioned during this paper. the necessity for any work on numerous security mechanisms has

additionally been highlighted, so as to supply clear services that may be trustworthy by all users.

V. REFERENCES

1. Hameed Hussain, J., Sharavanan, R., Floor cleaning machine by remote control, AInternational Journal of Pure and Applied Mathematics, V-116, I-14 Special Issue, PP-461-464, 2017
2. Hameed Hussain, J., Srinivasan, V., Extraction of polythene waste from domestic waste, International Journal of Pure and Applied Mathematics, V-116, I-14 Special Issue, PP-427-431, 2017
3. Hameed Hussain, J., Thirumavalavan, S., Flow analysis of copper tube for solar trough collector without joint, International Journal of Pure and Applied Mathematics, V-116, I-14 Special Issue, PP-541-544, 2017
4. Hanirex, D.K., Kaliyamurthie, K.P., Mining the financial multi-relationship with accurate models, Middle - East Journal of Scientific Research, V-19, I-6, PP-795-798, 2014
5. Hemapriya, M., Meikandaan, T.P., Repair of damaged reinforced concrete beam by externally bonded with CFRP sheets, International Journal of Pure and Applied Mathematics, V-116, I-13 Special Issue, PP-473-479, 2017
6. Hemapriya, M., Meikandaan, T.P., Experimental study on changes in properties of cement concrete using steel slag and fly ash, International Journal of Pure and Applied Mathematics, V-116, I-13 Special Issue, PP-369-375, 2017
7. Hemapriya, M., Meikandaan, T.P., Experimental study on structural

- repair and strengthening of RC beams with FRP laminates, International Journal of Pure and Applied Mathematics, V-116, I-13 Special Issue, PP-355-361, 2017
8. Hemapriya, M., Meikandaan, T.P., Effect of high range water reducers on sorptivity and water permeability of concrete, International Journal of Pure and Applied Mathematics, V-116, I-13 Special Issue, PP-377-381, 2017
 9. Hemapriya, M., Meikandaan, T.P., Strength and workability characteristics of super plasticized concrete, International Journal of Pure and Applied Mathematics, V-116, I-13 Special Issue, PP-345-353, 2017
 10. Hemapriya, M., Meikandaan, T.P., Potency and workability behavior of quality plasticized structural material, International Journal of Pure and Applied Mathematics, V-116, I-13 Special Issue, PP-363-367, 2017
 11. Hussain, J.H., Manavalan, S., Optimization of properties of jatropa methyl Ester (JME) from jatropa oil, International Journal of Pure and Applied Mathematics, V-116, I-18 Special Issue, PP-481-484, 2017
 12. Hussain, J.H., Manavalan, S., Optimization and comparison of properties of neem and jatropa biodiesels, International Journal of Pure and Applied Mathematics, V-116, I-17 Special Issue, PP-79-82, 2017
 13. Hussain, J.H., Meenakshi, C.M., Simulation and analysis of heavy vehicles composite leaf spring, International Journal of Pure and Applied Mathematics, V-116, I-17 Special Issue, PP-135-140, 2017
 14. Hussain, J.H., Nimal, R.J.G.R., Review: Investigation on mechanical properties of different metal matrix composites in diffusion bonding method by using metal interlayers, International Journal of Pure and Applied Mathematics, V-116, I-18 Special Issue, PP-459-464, 2017
 15. Jagadeeswari, P., Subashini, G., Basic results of probability, International Journal of Pure and Applied Mathematics, V-116, I-17 Special Issue, PP-275-276, 2017
 16. Janani, V.D., Kavitha, S., Conceptual level similarity measure based review spam detection adversarial spam detection using the randomized hough transform-support vector machine, International Journal of Pure and Applied Mathematics, V-116, I-9 Special Issue, PP-197-201, 2017
 17. Jasmin, M., Beulah Hemalatha, S., Security for industrial communication system using encryption / decryption modules, International Journal of Pure and Applied Mathematics, V-116, I-15 Special Issue, PP-563-567, 2017
 18. Jasmin, M., Beulah Hemalatha, S., VLSI-based frequency spectrum analyzer for low area chip design by using yasmirub method, International Journal of Pure and Applied Mathematics, V-116, I-15 Special Issue, PP-557-560, 2017
 19. Jasmin, M., Beulah Hemalatha, S., RFID security and privacy enhancement, International Journal of Pure and Applied Mathematics, V-116, I-15 Special Issue, PP-535-538, 2017

20. Jasmin, M., Beulah Hemalatha, S., Digital phase locked loop, International Journal of Pure and Applied Mathematics, V-116, I-15 Special Issue, PP-569-574, 2017
21. Jeyalakshmi, G., Arulselvi, S., Community oriented configurations for WSN, International Journal of Pure and Applied Mathematics, V-116, I-15 Special Issue, PP-529-533, 2017
22. Jeyalakshmi, G., Arulselvi, S., Investigating file systems, International Journal of Pure and Applied Mathematics, V-116, I-15 Special Issue, PP-517-521, 2017
23. Jeyalakshmi, G., Arulselvi, S., Methodology for the development of lambda calculus, International Journal of Pure and Applied Mathematics, V-116, I-15 Special Issue, PP-511-515, 2017
24. Jeyalakshmi, G., Arulselvi, S., Remote procedure calls in access points, International Journal of Pure and Applied Mathematics, V-116, I-15 Special Issue, PP-523-526, 2017
25. Jeyanthi Rebecca, L., Anbuselvi, S., Sharmila, S., Medok, P., Sarkar, D., Effect of marine waste on plant growth, Der Pharmacia Lettre, V-7, I-10, PP-299-301, 2015
26. Kaliyamurthi, K.P., Parameswari, D., Udayakumar, R., Malicious packet loss during routing misbehavior-identification, Middle - East Journal of Scientific Research, V-20, I-11, PP-1413-1416, 2014
27. Kanagavalli, G., Sangeetha, M., Intelligent traffic light system for reduced fuel consumption, International Journal of Pure and Applied Mathematics, V-116, I-15 Special Issue, PP-491-494, 2017
28. Kanagavalli, G., Sangeetha, M., GPS based blind pedestrian positioning and voice response system, International Journal of Pure and Applied Mathematics, V-116, I-15 Special Issue, PP-479-484, 2017
29. Kanagavalli, G., Sangeetha, M., Detection of retinal abnormality by contrast enhancement method using curvelet transform, International Journal of Pure and Applied Mathematics, V-116, I-15 Special Issue, PP-497-502, 2017
30. Kanagavalli, G., Sangeetha, M., Design of low power VLSI circuits for precharge logic, International Journal of Pure and Applied Mathematics, V-116, I-15 Special Issue, PP-505-509, 2017
31. Kanniga, E., Selvamaramathnam, K., Sundararajan, M., Kandigital bike operating system, Middle - East Journal of Scientific Research, V-20, I-6, PP-685-688, 2014
32. Karthik, B., Arulselvi, Noise removal using mixtures of projected gaussian scale mixtures, Middle - East Journal of Scientific Research, V-20, I-12, PP-2335-2340, 2014
33. Karthik, B., Arulselvi, Selvaraj, A., Test data compression architecture for low power vlsi testing, Middle - East Journal of Scientific Research, V-20, I-12, PP-2331-2334, 2014
34. Karthikeyan, R., Michael, G., Kumaravel, A., A housing selection method for design, implementation & evaluation for web based recommended systems, International Journal of Pure and Applied Mathematics, V-116, I-8 Special Issue, PP-23-27, 2017
35. Khanaa, V., Thooyamani, K.P., Using lookup table circulating fluidised bed combustion boiler by

- the method of sensor output linearization, Middle - East Journal of Scientific Research, V-16, I-12, PP-1801-1806, 2013
36. Khanaa, V., Thooyamani, K.P., Face routing protocol using genetic algorithm in, Middle - East Journal of Scientific Research, V-16, I-12, PP-1863-1867, 2013
 37. Khanaa, V., Thooyamani, K.P., Udayakumar, R., Two factor authentication using mobile phones, World Applied Sciences Journal, V-29, I-14, PP-208-213, 2014
 38. Khanaa, V., Thooyamani, K.P., Udayakumar, R., Next major wave of it inovation, World Applied Sciences Journal, V-29, I-14, PP-218-220, 2014
 39. Khanaa, V., Thooyamani, K.P., Udayakumar, R., Traffic policing approach for wireless video conference traffic, World Applied Sciences Journal, V-29, I-14, PP-200-207, 2014
 40. Khanaa, V., Thooyamani, K.P., Udayakumar, R., Patient monitoring in gene ontology with words computing using SOM, World Applied Sciences Journal, V-29, I-14, PP-195-199, 2014
 41. Khanaa, V., Thooyamani, K.P., Udayakumar, R., Load balancing in structured PEER to PEER systems, World Applied Sciences Journal, V-29, I-14, PP-186-189, 2014
 42. Khanaa, V., Thooyamani, K.P., Udayakumar, R., Impact of route stability under random based mobility model in MANET, World Applied Sciences Journal, V-29, I-14, PP-274-278, 2014
 43. Khanaa, V., Thooyamani, K.P., Udayakumar, R., Modelling Cloud Storage, World Applied Sciences Journal, V-29, I-14, PP-190-194, 2014
 44. Khanaa, V., Thooyamani, K.P., Udayakumar, R., Elliptic curve cryptography using in multicast network, World Applied Sciences Journal, V-29, I-14, PP-264-269, 2014
 45. Khanaa, V., Thooyamani, K.P., Udayakumar, R., SRW/U as a lingua franca in managing the diversified information resources, World Applied Sciences Journal, V-29, I-14, PP-279-284, 2014

