ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 11, November 2016

A Dual Encryption is providing a Better Security on the Public Cloud Security Mechanism

K.G.S.Venkatesan[1], N. Madhava Reddy [2], K. Varun Kumar Reddy [3]

Professor, Dept. of C.S.E, GATES Institute of Technology, NH-44, Gooty, A.P, India[1]

Assistant Professor, Dept. of C.S.E., GATES Institute of Technology, NH-44, Gooty, A.P, India[2 3]

ABSTRACT: A Cloud technique improve general strive execution by avoiding merchandiser lock-in victimization clear structure to handle problems with customers. Fogs might handle broad amounts of sales per unit time requiring very little information trades on the everyday however a substitute cloud might perform higher for additional diminutive amounts of sales per unit time together with generous information trades on the standard. For moving nearer the amendment in multi cloud, we have a tendency to propose a twofold coding security framework with AES (Advanced Encryption Standard) and MD5 (Message Digest Five) over the sure outcast and completely different open fogs severally. each of the coding framework is giving a much better update than the safety reason. the information is being encoded with the AES ways and checked at the untouchable aspect, then once the mixed information square measure sent to the various open fogs, sometimes people by and huge cloud isn't having a powerful security, however instead the projected technique (MD5) is proposing a amendment over the safety and giving a much better security section than the changed mixed information from the sure outsider. Once the coding procedure completed information are secured within the specific open cloud. Right once the client endeavor to urge to the set away information, they need to create a sales to the untouchable and therefore the outcast can offer them single mixed information succeeding unscrambling of the second layer of the encoded info. To upgrade the Accuracy analysis, client load, house use to customers wants, together with standard reaction time, typical accomplishment rate and resource security levels.

KEYWORDS: MD5 (Message Digest 5), AES (Advanced Encryption Standard) .

I. INTRODUCTION

The Distributed processing ascends as another figuring perspective which hopes to give reliable, adjusted and QOS Quality of Service guaranteed enrolling dynamic circumstances for end-customers .Distributed get ready, parallel taking care of and system handling together created as disseminated registering. The essential standard of appropriated registering is that customer data is not secure locally yet rather is secured in the server homestead of web stockpiling organizations gave moreover hardware and programming organizations are open to the general populace and business markets [1]. The organizations gave by organization suppliers can be everything, from the base, stage or programming resources. cloud organization is a solid of focal sensitivity toward endeavors and customers, the most delicate data send the customers to cloud organization centers, which relies on upon the trust relationship set up amidst customers and organization suppliers operators, to manufacture the assignment of cloud organizations, a cloud trader should set up and give trust organization capacity to relieve the hassles of their customers. Trust model in perspective of component organization components of a cloud resource from a customer's perspective, trust is a comprehensive document for organization guarantee and there are a couple trust segments in a system [2].

The standard Cloud figuring model where a client uses a singular cloud server ranch Introduces a couple of challenges cloud organization distance can leave countless depending totally on it without access to critical and paid for resources. In like manner relying upon a singular cloud server ranch makes it hard to complete attractive responsiveness and usability to clients scattered the world over. Where handling resources are open as participation utility organization basically like water and power appropriated processing has been portrayed as a kind of parallel and circled system

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 11, November 2016

giving virtualized resources. Fogs license us to concentrate on how buyers are required to use them. Clients are kept cynic to the purposes of enthusiasm of how organizations are given [5]. Thus, customers focus on what really matters to them, consuming an organization. It fundamentally sets the interface between organization suppliers and organization customers. Regardless, In a Multi-Cloud environment, the broad assortment of Cloud organizations and customer specific essentials make it difficult to pick the best structure of services. Proposed framework Advance Encryption Standard (AES) and Message Digest 5 (MD5) is proposing an overhaul over the security and giving a better security part than the exchanged mixed data from the trusted pariah. Once the encryption procedure completed data will be secured in the different open cloud. Right when the customer endeavor to get to the set away data, they have to make a sales to the outcast and the untouchable will give them single mixed data subsequent to interpreting of the second layer of the encoded data[3]. In dispersed figuring, Resource Allocation (RA) is the strategy of designating open advantages for the required cloud applications over the internet. Clouds may handle immeasurable amounts of sales per unit time requiring little data trades on the ordinary yet a substitute cloud may perform better for smaller amounts of requesting per unit time including generous data trades on the typical. Matchmaking resource across over organization manager trust arrangement for various cloud trust organization that can effectively reduce customer load and improve structure endurance on multi-dimensional resource organization directors trust appraisal.

Multi-dimensional organization heads avoiding the effect of individual inclination on weight parcel, and asserting the weight assignment of multi-executives adaptively are vital in trust mix figuring. Really, some past arrangements rely on upon expert feeling to weight trust figures anyway this system needs adaptability and might provoke off base results in trust evaluation [4].

II. LITERATURE SURVEY

In Service operator-aware trust scheme (SOTS) for asset matchmaking over different mists. Through examining the implicit relationship between the clients, the merchant, and the administration assets, this paper proposes a middleware structure of trust administration that can viably lessen client load and enhance framework reliability. Therefore, utilizing SOTS, the agent can effectively and precisely set up the most trusted assets ahead of time, and along these lines give more reliable assets to clients [9].

Utilizing this module, the representative can powerfully sort superior assets by dissecting the noteworthy asset data as far as giving profoundly trusted assets. Trusted asset matchmaking and conveying module. The administration client arranges with the administration dealer on the Service-Level Agreement (SLA).Agent distribute and benefit administrator procurement module to screen the utilization of allotted assets to ensure the SLA with the client [15].

A general estimation and quantitative strategy to survey the security levels of an asset is another intriguing course. Assessment of the proposed plan in a bigger scale different cloud environment is additionally a critical undertaking to be tended to in future exploration.

A multi-cloud strategy improve overall enterprise performance by avoiding vendor lock-in using different infrastructure to meet needs of customers. Clouds might handle large numbers of requests per unit time requiring small data transfers on the average but a different cloud might perform better for smaller numbers of requests per unit time involving large data transfers on the average. Matchmaking a resource across service operator trust scheme for multiple clouds, trust management that can effectively reduce user burden and improve system dependability on multi-dimensional resource service operators [19].

A resource monitoring system based on a eucalyptus platform of this monitoring system is an active agent binding mechanism when a cloud provider registers its virtual machines with the broker each registered resource is commanded to download to monitoring agent . A universal measurement and quantitative method to assess the security levels of a resource is another interesting direction of the proposed scheme in a larger-scale multiple cloud environment is also an important task [25].

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 11, November 2016

To analysis combining the trust scheme with reputation management to address concerns in users feedback. A universal measurement and quantitative method to assess the security levels of a resource is another interesting direction of the proposed scheme in a larger-scale multiple cloud environment is also an important task.

To solve the complexity of application deployment in Cloud infrastructure, virtual appliances, pre-configured, ready-torun applications are emerging as a breakthrough technology. However, an automated approach for deploying network of appliances is required to guarantee minimum deployment cost low latency, and high reliability [29].

***A. VIRTUAL UNIT AND APPLIANCE MODELING*:** We built an aggregated repository of virtual appliance and virtual unit services based on the advertised services by Cloud providers, Services contain information regarding cost, virtual appliance size, and data communication cost inside and outside of Clouds. Latency and reliability calculation:

QoS criteria and the problem of deployment is formulated and tackled by two approaches namely FCBB (Forward-checking-based backtracking) and genetic-based selection. We evaluated the proposed approaches by a real case study using real data collected from 12 Cloud providers, which showed that proposed approaches deliver near-optimal solution. Next, they were tested with different types of requests [22].

Quality of Service (QoS),reliability and cost efficiency by utilizing multiple clouds. Inter-Cloud research is still in its infancy, and the body of knowledge in the area has not been well defined.Inter-Cloud environment for cloud customers is that they can diversify their infrastructure portfolio in terms of both vendors and location. Thus, they could make their businesses more adaptable to vendors' policy and availability changes and easily expandable in new legislative regions [27].

To classified and analyzed the state of the art in Inter-Cloud developments more specifically, To focus on how current Inter-Cloud projects facilitate the brokering of different applications across multiple clouds.

III. EXISTING SYSTEM

Existing Framework proposes an administration administrator mindful trust plan (SOTS) for asset matchmaking over numerous mists. Through examining the implicit relationship between the clients, the merchant, and the administration assets the current strategy is not giving any solid security instrument over the cloud which could spare the put away information splendidly [31]. This trust plan making an accessibility of to coordinating and who are need to get to the information every last individual ought to be coordinated to this if any reason it might be get to the any individual are getting any spillages and any assaults then it having the significant issue is a the hacking issue all clients have status about this information then till it is putting away or not there is no any framework security keys in client then the client having some far fetched assertion to store information in cloud.

Multi-cloud is the corresponding utilization of more than two administrations to minimize danger of far reaching information misfortune or downtime because of a restricted segment disappointment in a distributed computing such a disappointment can happen in equipment programming infrastructure. Trust assessment as a procedure of multi-trait choice making and create and versatile trust assessment data entropy can beat the impediment of conventional trust plans trusted administrators are weighted physically. Our look at investigation yields fascinating perception that can encourage the use of administration administrator trust in vast multi-cloud environment [21].

Trust model taking into account dynamic administration elements of a cloud asset from a client's point of view, trust is a complete record for administration ensure and there are a few trust components in a framework, i.e., security, accessibility, and dependability. As watched that trust is past security, and an extended trust model ought to consolidate security, unwavering quality, and accessibility variables and different elements [5].

A trust-mindful expediting system for multi-cloud situations, cloud specialists can give intermediation and conglomeration capacities to empower suppliers to convey their virtual frameworks over various mists. The eventual fate of distributed computing will be pervaded with the development of cloud dealers going about as middle people between cloud suppliers and clients to arrange and designate assets among various server farms [9].

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 11, November 2016

The dependability of an asset is assessed by the specialist as indicated by numerous administration administrators concerning the security accessibility and unwavering quality of this asset inside of a few determined time windows. The calculated model of the trust mindful asset match making relies on upon the cloud specialist goes about as TTP for clients assess every asset execution amid specific time arranging benefits powerfully and circulating assignments productively. At whatever point another asset needs to offer its administrations it must join the administration system on the customer side a client searching for administration must send an inquiry together with his polices to the trusted representative. The trust assessment intermediary will choose a suitable asset by applying a coordinating calculation. At whatever point an administration asset coordinates the cloud specialist disperse the clients undertaking to the asset through its director [10].

IV. PROPOSED SYSTEM

In Framework it's not give solid security system. We can defeat those propose another methods or calculations for give a decent security and capacity of information. Utilizing procedures are AES and MD5 and when the strategies will be having the more adaptability then the framework getting the complete yield and these are new systems and event of all capacities to keep up every single specialized work. This trust plan making an accessibility of to coordinating a who are need to get to the information every single individual ought to be coordinated to this if any reason it might be get to Match making is in distinguishing proof process extremely alluring and it have low precision by give these systems to push ahead it. These methods give security keys to an every single module or data change process. Cloud administrations by considering their practical and non-utilitarian SLA prerequisites. A key commitment of the proposition is the outline of a multi-Cloud administration representative structure going about as a middle person in the middle of purchasers and various Cloud suppliers to mechanize the administration choice and sending. Contrasting with other condensation calculations, MD5 is easy to execute, and gives a "unique finger impression" or message summary of a message of discretionary length [15].

It performs quick on 32-bit machine is being utilized vigorously from huge organizations, for example, IBM, Cisco Systems, to individual software engineers. MD5 is viewed as a standout amongst the most effective calculations as of now accessible. For drawing nearer the improvement in multi cloud, we propose a double encryption security system with AES and MD5 over the trusted outsider and numerous open mists individually [19]. Both of the encryption procedure is giving a superior improvement to the security reason. The AES is being utilized while the client validated themselves with the trusted outsider and transferring their information to the outsider side; the information is being scrambled with the AES systems and confirmed at the outsider side, then after the encoded information are sent to the different open mists, Usually people in general cloud is not having a solid security, but rather the proposed method Message Direct 5 (MD5) is proposing an improvement over the security and giving a superior security instrument to the transferred scrambled information from the trusted outsider [29]. Once the encryption process finished information will be put away in the diverse open cloud. Continuously information will be an encryption group on account of outsider understanding that information it will going to done a procedure in encryption utilizing first encryption calculation then it will transfer to one more second area then it will procedure to a made with the diverse encryptions like AES and MD5 both will be significant encryption methods; .

ADVANTAGES OF PROPOSED SYSTEM:

- The dual encryption is providing a better security on the public cloud where there is no perfect security available.
- The reliability and efficiency about the storing data will be increase with the enhanced security mechanism.
- Usually public clouds getting data loss most cost consumption using MD5 encryption technique decrease data loss and excess cost consumption.
- Technique will across the Hacking is the major defect to overcome that technique in this technique proposed

V. ARCHITECTURAL DESIGN

In this venture make a taking into account existing framework and proposed make a design that is clarified full subject of task engineering notice underneath to comprehend that chart comprehend complete existing substance in view of this

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 11, November 2016

engineering the primary idea of this undertaking is new systems or calculations for give a decent security and capacity of information. Utilizing methods are AES and MD5 and when the strategies will be having the more adaptability then the framework getting the complete yield and these are new procedures and event A multi-cloud technique enhance general avoiding so as to undertake execution merchant lock-in utilizing diverse base to address issues of customers [25]. For drawing nearer the improvement in multi cloud, we propose a double encryption security system with AES and MD5 over the trusted outsider and various open mists individually. Both of the encryption system is giving a superior upgrade to the security reason. The AES is being utilized while the client confirmed themselves with the trusted outsider and transferring their information to the outsider side; the information is being scrambled with the AES systems and checked at the outsider side, then after the encoded information are sent to the various open mists, Usually general society cloud is not having a solid security, but rather the proposed method Message Direct 5 (MD5) is proposing an upgrade over the security and giving a superior security component to the transferred scrambled information from the trusted outsider. Advance encryption calculation is progressed encoded strategy it assume key part in distributed computing any encryption if any unscrambling reason likewise relying on the any decoding calculation here the development encryption calculation give decoding keys to giving unscrambling moreover.

At the point when information proprietor need to share the information to outsider he ought to have validation that implies the information proprietor need to do enlistment by giving id or login id to the information proprietor. Once after information proprietor is verified information will be sent to outsider [39].

A. DATA ENCRYPTION IN THIRD PARTY AND DATA DOWNLOADING

At the point when the information proprietor shared information to the outsider then information will be scrambled in outsider position. The encryption system is done utilizing AES calculation and the information will be encoded and sent to the cloud through the outsider .that will be affirmation with an affirmation security key 1.

In the wake of finishing the encryption process, reviewer advances the information to various open mists where cloud server is re-scrambling the information with MD5 and putting away the re-encoded information out in the open cloud [40]. Here double encryption procedure was finished by this MD5 calculation and it give re encryption to that information here having the affirmation with a security key 2.

B. DATA RETRIEVAL THE THIRD PARTY

The information proprietor making a solicitation to the inspector for getting to the information which have been put away in the different open cloud, the evaluator accepting the proprietor ask for and giving the scrambled information from the various cloud and information proprietor could get to the information with the decoding information with a security key 2 it adjusts [45].

IV. EVALUATION OF AES AND MD5

A. AES (ADVANCED ENCRYPTION STANDARD) :

AES is a symmetric encryption calculation preparing information in piece of 128 bits. A bit can take the qualities zero and one, as a result a paired digit with two conceivable qualities instead of decimal digits, which can take one of 10 qualities. Affected by a key, a 128-piece square is encoded by changing it uniquely into another piece of the same size. AES is symmetric since the same key is utilized for encryption and the converse change, unscrambling. The main mystery important to keep for security is the key [49]. AES might designed to utilize distinctive key-lengths, the standard characterizes 3 lengths and the subsequent calculations are named AES-128, AES-192 and AES-256 separately to show the length in bits of the key. Each extra piece in the key adequately duplicates the quality of the calculation, when characterized as the time essential for an aggressor to organize an animal power assault, i.e. a comprehensive inquiry of all conceivable key mixes with a specific end goal to locate the right one. It is indispensable that the right technique is connected in the right way for every last circumstance, or the outcome might well be shaky regardless of the possibility that AES accordingly is secure. It is anything but difficult to actualize a framework utilizing AES as its encryption calculation, yet a great deal more expertise and experience is required to do it in the

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 11, November 2016

right path for a given circumstance. Close to a sledge and a saw will make anybody a decent woodworker, will AES make a framework secure independent from anyone else [50].

B. MD5 (MESSAGE DIGEST 5) :

The MD5 calculation is intended to be very quick on 32-bit machines. Moreover, the MD5 calculation does not require any substantial substitution tables; the calculation can be coded very minimalistically. The MD5 calculation is an expansion of the MD4 message-digest calculation. MD5 is marginally slower than MD4, however is more "traditionalist" in configuration. MD5 was composed on the grounds that it was felt that MD4 was maybe being received for utilize more rapidly than legitimized by the current basic audit; in light of the fact that MD4 was intended to be incredibly quick, it is "at the edge" as far as gambling effective cryptanalytic assault. MD5 backs off somewhat, surrendering a little in velocity for a much more noteworthy probability of extreme security. It fuses a few recommendations made by different analysts, and contains extra advancements [54]**.**

MD5 has been utilized in a wide assortment of security applications, and is additionally generally used to check the trustworthiness of files. Comparing to other condensation calculations, MD5 is easy to execute, and gives a "unique finger impression" or message summary of a message of subjective length. It performs quick on 32-bit machine.

MD5 is being utilized intensely from huge partnerships, for example, IBM, Cisco Systems, to individual developers. MD5 is viewed as a standout amongst the most proficient calculations right now accessible. Here the point of preference is both re encryption done. at that point the security level ought to be high [51].

The principle thought is that the intermediary first assesses the recently enrolled asset, in light of its enlisted data. The FSLA system will allow the asset to get clients' registering assignments. In the communications between the client and the asset, the agent will screen its administration administrators, then ascertain its GTD as indicated by the proposed trust plan. Figure GTD in light of intermediary connection with client [55].

It utilizes FSLA (First Service-Last Audit) component. The FSLA component will allow the asset to get client's registering undertakings. In the communication between the client and the asset, the representative will screen its administration administrators, and after that figure its GTD. On the off chance that the dedication QoS is lower than the real GTD that is processed by expedite, the agent will make a strict correctional stride.

Enlivened by an extended trust assessment approach in, in administration service operator trust scheme (SOTS), we characterize trust as a measured conviction by a cloud agent regarding the security, accessibility, and dependability of an asset inside of a few determined time windows [59].

This definition fits in with a methodology in view of trusted thirty party (TTP) . The representative goes about as the TTP, which is made out of numerous enrolled assets. The key developments of SOTS go past those of existing plans as far as the accompanying perspectives:

An efficient trust administration plan for multi-cloud environment, in light of multi-dimensional asset administration administrators. Alcoholics assess the trust of cloud asset in differentiation to customary trust plots that dependably concentrate on one-sided trust components of administration assets. It joins various element into a trust vector to shape an extended trust plan to assess an asset. This trust plan is more reliable with the fundamental traits of a trust relationship, in this manner, it is more in accordance with the desires of cloud clients [60].

A versatile combined registering methodology of element administration administrators, in light of data entropy hypothesis . Lushes models the issue of trust assessment as the procedure of multi-trait choice making, and afterward builds up a versatile trust assessment approach. This versatile combined processing methodology can be defeat the restrictions of customary trust plans, in which the trusted properties are weighted physically or subjectively [62].

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 11, November 2016

C. RESOURSE TRUST DEGREE (RTD) :

The proposed FSLA component RTD is time window-based trusted marker for administration administrators and it ought to be more delicate to new administrators. RTD created in the time window when an association happens between a client and an asset. It figures with a plan of action taking into account client. Administrators and it ought to be more touchy to new administrators. RTD created in the time window when a collaboration happens between a client and an asset. It ascertains with a plan of action in light of client [61].

IV. CONCLUSION

The 2 cryptography instruments those area unit AES and MD5 these two estimations area unit giving the safety. Right once information of affairs send information to untouchable AES can inscribe that information and exchange to the cloud. it'll offer the adjustment security key.MD5 can re scramble the information| MD5 can offer another security to it decoded data .what ever different occasion mean as untouchable is taken USA like may be a sure unfortunate person if it existing of a information knowledge| are unscrambled by a two fold cryptography associated afterward recuperate that information into associate open cloud it'll having terribly key rule of this to create an openness of information of knowledge dynamical it's into encoded data to decoded data. It beat the hackings conjointly and find full security. Propose a twofold cryptography security dispense with AES and MD5 over the sure unfortunate person and completely different open fogs severally. Once the cryptography procedure completed information are secured within the specific open cloud. To upgrade the Accuracy analysis, client load, house utilization to customers wants, as well as typical time interval, standard trip accomplishment rate and resource security levels.

REFERENCES

1. K Xiaoyong Li, Huadong Ma, Feng Zhou and Xiaolin Gui, “Service Operator-aware Trust Scheme for Resource Matchmaking across Multiple”, IEEE Transactions on Parallel and Distributed Systems Volume: 26 Year: 2015, pp.14-24
2. K. Hwang, D. Li, “Trusted Cloud Computing with Secure Resources and Data Coloring”, IEEE Internet Computing, vol. 14, no. 5, 2010, pp. 14-22.
3. N. Dukkipati and N. McKeown. Why Flow-Completion Time is the Right Metric for Congestion Control. ACM SIGCOMM Computer Communication Review, 2006.
4. S. M. Habib, S. Ries, and M. Muhlhauser, “Towards a Trust Management System for Cloud Computing”, Proc. of IEEE TrustCom-11/IEEE ICESS-11/FCST-11, pp. 933-939, 2011.
5. L. S. Brakmo, S. W. O’Malley, and L. L. Peterson. TCP Vegas: New Techniques for Congestion Detection and Avoidance. ACM SIGCOMM Computer Communication Review, 1994.
6. K.G.S. Venkatesan. Dr. V. Khanna, S.B. Amarnath Reddy, “Providing Security for social Networks from Inference Attack”, International Journal of Computer Science Engineering & Scientific Technology, March – 2015.
7. A.R. Arunachalam, K.G.S. Venkatesan, Abdul Basith.K.V., M. Sriram, “Traffic Identification Method Engine : An open platform for Traffic classification “,”, International Journal of Innovative Research in computer & communication Engineering, Vol. 3, Issue 3, PP. 2475 – 2481, March - 2015.
8. S. Ha, I. Rhee, and L. Xu. CUBIC: a New TCP-friendly High- Speed TCP Variant. ACM SIGOPS Operating System Review, 2008.
9. K. Tan, J. Song, Q. Zhang, and M. Sridharan. A Compound TCP Approach for High-Speed and Long Distance Networks. In Proc. IEEE INFOCOM, 2006.
10. L. Xu, K. Harfoush, and I. Rhee. Binary Increase Congestion Control (BIC) for Fast Long-Distance Networks. In INFOCOM 2004.
11. V. N. Padmanabhan and R. H. Katz. TCP Fast Start: A Technique for Speeding Up Web Transfers. In Proc. IEEE Global Internet Conference (GLOBECOM), 1998.
12. K. Winstein and H. Balakrishnan. TCP Ex Machina: Computer generated Congestion Control. In Proc. ACM SIGCOMM, 2013.
13. B. Sundarraj, K.G.S. Venkatesan, M. Sriram, Vimal Chand, “An Iaas cloud system with Federation Threshold”, ”, International Journal of Innovative Research in computer & communication Engineering, Vol. 3, Issue 3, PP. 2593 – 2598, March - 2015.
14. K.G.S. Venkatesan and M. Elamurugaselvam, “Design based object oriented Metrics to measure coupling & cohesion”, International journal of Advanced & Innovative Research, Vol. 2, Issue 5, PP. 778 – 785, 2013.
15. S. Sathish Raja and K.G.S. Venkatesan, “Email spam zombies scrutinizer in email sending network Infrastructures”, International journal of Scientific & Engineering Research, Vol. 4, Issue 4, PP. 366 – 373, April - 2013.
16. K.G.S. Venkatesan, “Comparison of CDMA & GSM Mobile Technology”, Middle-East Journal of Scientific Research, 13 (12), PP. 1590 – 1594, 2013.
17. P. Indira Priya, K.G.S.Venkatesan, “Finding the K-Edge connectivity in MANET using DLTRT, International Journal of Applied Engineering Research, Vol. 9, Issue 22, PP. 5898 – 5904, 2014.
18. Ms. J.Praveena, K.G.S. Venkatesan, “Advanced Auto Adaptive edge-detection algorithm for flame monitoring & fire image processing”, International Journal of Applied Engineering Research, Vol. 9, Issue 22, PP. 5797 – 5802, 2014.
19. K.G.S. Venkatesan. Dr. V. Khanna, “Inclusion of flow management for Automatic & dynamic route discovery system by ARS”, International Journal of Advanced Research in computer science & software Engg., Vol.2, Issue 12, PP. 1 – 9, December – 2012.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 11, November 2016

20. Needhu. C, K.G.S. Venkatesan, "A System for Retrieving Information directly from online social network user Link ", International Journal of Applied Engineering Research, Vol. 9, Issue 22, PP. 6023 – 6028, 2014.
21. K.G.S. Venkatesan, R. Resmi, R. Remya, "Anonymizimg Geographic routing for preserving location privacy using unlinkability and unobservability", International Journal of Advanced Research in computer science & software Engg., Vol. 4, Issue 3, PP. 523 – 528, March – 2014.
22. Selvakumari. P, K.G.S. Venkatesan, "Vehicular communication using Fvmr Technique", International Journal of Applied Engineering Research, Vol. 9, Issue 22, PP. 6133 – 6139, 2014.
23. K.G.S. Venkatesan, G. Julin Leeya, G. Dayalin Leena, "Efficient colour image watermarking using factor Entrenching method", International Journal of Advanced Research in computer science & software Engg., Vol. 4, Issue 3, PP. 529 – 538, March – 2014.
24. Dr. K.P. Kaliyamerthie, K.G.S. Venkatesan, S. Sriram, N. Vijay, Richard Solomon, "Neighborhood based framework, Active Learning", ", International Journal of Innovative Research in computer & communication Engineering, Vol. 3, Issue 3, PP. 2535 – 2542, March - 2015.
25. K.G.S. Venkatesan. Kausik Mondal, Abhishek Kumar, "Enhancement of social network security by Third party application", International Journal of Advanced Research in computer science & software Engg., Vol. 3, Issue 3, PP. 230 – 237, March – 2013.
26. V. N. Padmanabhan and R. H. Katz. TCP Fast Start: A Technique for Speeding Up Web Transfers. In Proc. IEEE Global Internet Conference (GLOBECOM), 1998.
27. K.G.S. Venkatesan, "Planning in FARS by dynamic multipath reconfiguration system failure recovery in wireless mesh network", International Journal of Innovative Research in computer & comm. Engineering, Vol. 2, Issue 8, August - 2014.
28. B. Sundarraj, K.G.S. Venkatesan, Vimal Chand, "A Stochastic Model to Investigate Data center performance & QOS in IaaS cloud computing systems", ", International Journal of Innovative Research in computer & communication Engineering, Vol. 3, Issue 3, PP. 2560 – 2565, March - 2015.
29. Anish Kumar Anbakarasan, Ilampiria Nagarajan, K.G.S. Venkatesan, "Moral Hacking : A way to boost data security by using vulnerability scanning Tools", ", International Journal of Innovative Research in computer & communication Engineering, Vol. 3, Issue 3, PP. 2605 – 2613, March - 2015.
30. K.G.S. Venkatesan and M. Elamurugaselvam, "Using the conceptual cohesion of classes for fault prediction in object-oriented system", International journal of Advanced & Innovative Research, Vol. 2, Issue 4, PP. 75 – 80, April 2013.
31. K.G.S. Venkatesan, "Automatic Detection and control of Malware spread in decentralized peer to peer network", International Journal of Innovative Research in computer & comm. Engineering, Vol. 1, Issue 7, PP. 15157 – 15159, September - 2013.
32. Satthish Raja, S K.G.S. Venkatesan, "Electronic Mail spam zombies purify in email connection", International Journal of Advanced Research in Computer Science Engineering & Information Technology, Vol. 1, Issue 1, PP. 26 – 36, June – 2013.
33. K.G.S. Venkatesan. Dr. V. Khanna, S.B. Amarnath Reddy, "Providing Security for social Networks from Inference Attack", International Journal of Computer Science Engineering & Scientific Technology, March – 2015.
34. A.R. Arunachalam, K.G.S. Venkatesan, Abdul Basith.K.V., M. Sriram, "Traffic Identification Method Engine : An open platform for Traffic classification ",", International Journal of Innovative Research in computer & communication Engineering, Vol. 3, Issue 3, PP. 2475 – 2481, March - 2015.
35. K.G.S. Venkatesan, Dr. Kathir. Viswalingam, N.G. Vijitha, " Associate Adaptable Transactions Information store in the cloud using Distributed storage and meta data manager", International Journal of Innovative Research in computer & communication Engineering, Vol. 3, Issue 3, PP. 1548 – 1555, March - 2015.
36. Abhinav Kumar, Abhijeet Kumar, Dr. C. Nalini, K.G.S. Venkatesan, "QOS – Guaranteed Neighbor selection & distributed packet scheduling algorithm by using MANET wireless networks", ", International Journal of Innovative Research in computer & communication Engineering, Vol. 3, Issue 3, PP. 2466 – 2474, March - 2015.
37. K.G.S. Venkatesan, Dr. V. Khanna, Jay Prakash Thakur, Banbari Kumar, "Mining User profile Exploitation cluster from computer program Logs", International Journal of Innovative Research in computer & communication Engineering, Vol. 3, Issue 3, PP. 1557 – 1561, March - 2015.
38. Ms.J.Praveena, K.G.S.Venkatesan, "Advanced Auto Adaptive edge-detection algorithm for flame monitoring & fire image processing", International Journal of Applied Engineering Research, Vol. 9, Issue 22, PP. 5797 – 5802, 2014.
39. K.G.S.Venkatesan, "Planning in FARS by dynamic multipath reconfiguration system failure recovery in wireless mesh network", International Journal of Innovative Research in computer & comm. Engineering, Vol. 2, Issue 8, August -2014.
40. J. Bethencourt, A. Sahai, and B. Waters. "Cipher text-Policy Attribute-Based Encryption". In Proc. of IEEE Symp. on Security and Privacy, May 2006.
41. Yang Tang, Patrick P. C. Lee, John C. S. Lui, Radia Perlman "Transactions And Dependable And Secure Computing" IEEE , VOL.9 NO.6, 2012
42. Margaret, A, & Henry, J., Journal of business ethics, Computer Ethics: The Role of Personal, Informal, and Formal Codes, 15(4), 425
43. K.G.S. Venkatesan, Dr. V. Khanna, S.B. Amarnath Reddy, "Network Monitoring using Test Packet Generation", IJSCONLINE, PP. 1-12, March – 2015.
44. F. Ye, S. Roy, and H. Wang, "Efficient Data Dissemination in Vehicular Ad Hoc Networks, " in IEEE J. on Sel. Areas in Comm., vol.30, no.4, pp.769-779, May 2012.
45. K.G.S. Venkatesan, Dr. V. Khanna, Dr. A. Chandrasekar, "Reduced path, Sink failures in Autonomous Network Reconfiguration System (ANRS) Techniques", International Journal of Innovative Research in computer & communication Engineering, Vol. 3, Issue 3, PP. 2566 – 2571, March - 2015.
46. L. Ghaderi, D. Towsley, and J. Kurose, "Reliability Gain of Network Coding in Lossy Wireless Networks, " in Proc. IEEE INFOCOM, Phoenix, AZ, Apr. 2008.
47. K.G.S. Venkatesan. Dr. V. Khanaa, K.P. Kaliyamurthie , Multi-Layer Integrational of cluster computing, JIRAS, A Unit of UIIRS, PRINT ISSN : 2320 1932, ONLINE ISSN – 2348 3636, Vol. 2, Issue 1, PP. 188 – 196, January-June 2016.
48. K.G.S. Venkatesan. Dr. V. Khanaa , Construction of Economical coloured Trees for node failures, JIRAS, A Unit of UIIRS, PRINT ISSN : 2320 1932, ONLINE ISSN – 2348 3636, Vol. 2, Issue 2, PP. 152 – 160, JUL-DEC 2016.
49. K.G.S. Venkatesan, Satyavijay Kumar, Rohit Kumar, Energy-Minimum Data gathering operations based on dynamic programming using wireless sensor Network, JIRAS, A Unit of UIIRS, PRINT ISSN : 2320 1932, ONLINE ISSN – 2348 3636, Vol. 2, Issue 2, PP. 169 –

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 11, November 2016

179, JUL-DEC 2016.
50. K.G.S. Venkatesan. Dr. V. Khanaa, Dr. A. Chandrasekar, "Autonomous System (AS) for mesh network by using packet transmission & failure detection", Inter. Journal of Innovative Research in computer & comm. Engineering, Vol. 2, Issue 12, PP. 7289 – 7296, December - 2014.
51. Sathish Raja, K.G.S. Venkatesan, "Electronic Mail spam zombies purify in E-mail connection", International Journal of Advanced Research in computer science Engineering & Information Technology, Vol. 1, Issue 3, pp. 28 - 36, June – 2013.
52. K.G.S. Venkatesan. Dr. V. Khanna, S.B. Amarnath Reddy, "Network Monitoring using Test Packet Generation", IJSCONLINE, PP. 1-12, March – 2015.
53. C. Fragouli, J. Widmer, and J. Le Boudec, "Efficient Broadcasting Using Network Coding, " in IEEE/ACM Trans. on Netw., vol.16, no.2, pp.450-463, Apr. 2008.
54. Sathish Raja, K.G.S. Venkatesan, "Electronic Mail spam zombies purify in E-mail connection", International Journal of Advanced Research in computer science Engineering & Information Technology, Vol. 1, Issue 3, pp. 28 - 36, June – 2013.
55. K.G.S. Venkatesan. Dr. V. Khanaa, Implementation of GOLEM based mostly Mobile Learning Application as a versatile Learning Media, International Journal of Pharmacy & Technology, ISSN : 0975 – 766X, Vol. 8, Issue No. 3, pp. 17280 - 17288, Sep-2016.
56. K.G.S. Venkatesan. Dr. V. Khanaa, On the Construction of SMPS, International Journal of Pharmacy & Technology, ISSN : 0975 – 766X, Vol. 8, Issue No. 3, pp. 17397 -17403, Sep-2016.
57. K.G.S. Venkatesan. Dr. V. Khanaa, Contrasting Flip-Flop Gates & Agents, International Journal of Pharmacy & Technology, ISSN : 0975 – 766X, Vol. 8, Issue No. 3, pp. 17410 -17414, Sep-2016.
58. K.G.S. Venkatesan. Dr. V. Khanaa, Decoupling the Location-Identity split from active Networks in the Turning Machine, International Journal of Pharmacy & Technology, ISSN : 0975 – 766X, Vol. 8, Issue No. 3, pp. 17415 -17419, Sep-2016.
59. K.G.S. Venkatesan. Dr. V. Khanaa, Partitional Agglomeration calculations attempts & Territorially enhance an exact Foundation, International Journal of Pharmacy & Technology, ISSN : 0975 – 766X, Vol. 8, Issue No. 3, pp. 18514 -18520, Sep-2016.
60. K.G.S. Venkatesan. Dr. V. Khanaa, Reliable communication in MANET to communicate in Ad-hoc Network, International Journal of Pharmacy & Technology, ISSN : 0975 – 766X, Vol. 8, Issue No. 3, pp. 17770 -17775, Sep-2016.
61. C. Fragouli, J. Widmer, and J. Le Boudec, "Efficient Broadcasting Using Network Coding, " in IEEE/ACM Trans. on Netw., vol.16, no.2, pp.450-463, Apr. 2008.