ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 11, November 2019

An Analytical Implementation of Securing Cloud Data in Encryption Form Mechanism

Dr. Shaik Abdul Subhahan[1] Nazir Shaik[2] Dr. K.G.S. Venkatesan[3] V.M. Jothiprakash[4] R. Veera Reddy[5]

Associate Professor, Dept. of C.S.E, ISL Engg. College, (Affil. to JNTUH), Hyderabad, Telangana, India[1]

Research Scholar, Dept. of C.S.E, S.R.K. University, Bhopal, (M.P), India[2]

Professor, Dept. of CSE, Megha Institute of Engg. & Tech. for Women, (Affil. to JNTUH), Telangana, India[3]

Asst. Professor, Easwari Engg. College (SRM Group, Affili. to Anna Univ), Chennai, Tamil Nadu, India[4]

Asst. Professor, Dept. of CSE, Megha Institute of Engg. & Tech. for Women, (Affil. to JNTUH), Telangana, India[5]

ABSTRACT: In this paper presents, news reveal a strong offender that breaks information confidentiality by getting cryptological keys, by means that of coercion or backdoors in cryptological software system. Once the cryptography secret is exposed, the sole viable live to preserve information confidentiality is to limit the attacker's access to the cipher text. this might be achieved, as an example, by spreading cipher text blocks across servers in multiple body domains so presumptuous that the somebody cannot compromise all of them. still, if information is encrypted with existing schemes, associate somebody equipped with the cryptography key, will still compromise one server and decode the cipher text blocks hold on in that. during this paper, we have a tendency to study information confidentiality against associate somebody that is aware of the cryptography key and has access to an outsized fraction of the cipher text blocks. to the current finish, we have a tendency to propose Bastion, a unique and economical theme that guarantees information confidentiality although the cryptography secret is leaked and therefore the somebody has access to the majority cipher text blocks. we have a tendency to analyze the safety of Bastion, and that we value its performance by means that of a epitome implementation. we have a tendency to additionally discuss sensible insights with reference to the combination of Bastion in industrial distributed storage systems. Our analysis results counsel that Bastion is well-suited for integration in existing systems since it incurs but 8 % overhead compared to existing semantically secure cryptography modes.

KEYWORDS: Cloud Computing, Cryptography.

I. INTRODUCTION

The world recently witnessed a massive surveillance program aimed at breaking users' privacy. Perpetrators were not hindered by the various security measures deployed within the targeted services. For instance, although these services relied on encryption mechanisms to guarantee data confidentiality, the necessary keying material was acquired by means of backdoors, bribe, or coercion. If the encryption key is exposed, the only viable means to guarantee confidentiality is to limit the adversary's access to the cipher text, e.g., by spreading it across multiple administrative domains, in the hope that the adversary cannot compromise all of them [8]. However, even if the data is encrypted and dispersed across different administrative domains, an adversary equipped with the appropriate keying material can compromise a server in one domain and decrypt cipher text blocks stored therein. In this paper, we study data confidentiality against an adversary which knows the encryption key and has access to a large fraction of the cipher text blocks. The adversary can acquire the key either by exploiting flaws or backdoors in the key-generation software or by compromising the devices that store the keys (e.g., at the user-side or in the cloud). As far as we are aware, this

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 11, November 2019

adversary invalidates the security of most cryptographic solutions, including those that protect encryption keys by means of secret-sharing (since these keys can be leaked as soon as they are generated) [16]. To counter such an adversary, we propose Bastion, a novel and efficient scheme which ensures that plaintext data cannot be recovered as long as the adversary has access to at most all but two cipher text blocks, even when the encryption key is exposed. Bastion achieves this by combining the use of standard encryption functions with an efficient linear transform. In this sense, Bastion shares similarities with the notion of all-or-nothing transform. An AONT is not an encryption by itself, but can be used as a pre-processing step before encrypting the data with a block cipher. This encryption paradigm—called AON encryption was mainly intended to slow down brute-force attacks on the encryption key. However, AON encryption can also preserve data confidentiality in case the encryption key is exposed, as long as the adversary has access to at most all but one cipher text blocks. Existing AON encryption schemes, however, require at least two rounds of block cipher encryptions on the data: one preprocessing round to create the AONT, followed by another round for the actual encryption. Notice that these rounds are sequential, and cannot be parallelized. This results in considerable often unacceptable overhead to encrypt and decrypt large files. On the other hand, Bastion requires only one round of encryption which makes it well-suited to be integrated in existing dispersed storage systems. We evaluate the performance of Bastion in comparison with a number of existing encryption schemes. Our results show that Bastion only incurs a negligible performance deterioration (less than 5%) when compared to symmetric encryption schemes, and considerably improves the performance of existing AON encryption schemes . We also discuss practical insights with respect to the possible integration of Bastion in commercial dispersed storage systems [27].

Our contributions in this paper can be summarized as follows:

• We propose Bastion, an efficient scheme which ensures data confidentiality against an adversary that knows the encryption key and has access to a large fraction of the cipher text blocks.
• We analyze the security of Bastion, and we show that it prevents leakage of any plaintext block as long as the adversary has access to the encryption key and to all but two cipher text blocks [34].
• We evaluate the performance of Bastion analytically and empirically in comparison to a number of existing encryption techniques. Our results show that Bastion considerably improves (by more than 50%) the performance of existing AON encryption schemes, and only incurs a negligible overhead when compared to existing semantically secure encryption modes (e.g., the CTR encryption mode).
• We discuss practical insights with respect to the deployment of Bastion within existing storage systems, such as the Hydrators grid storage system [23].

II. RELATED WORKS

1. A. Beimel, "Secret-Sharing Schemes: A Survey," - A secret-sharing scheme is a method by which a dealer distributes shares to parties such that only authorized subsets of parties can reconstruct the secret. Secret-sharing schemes are important tools in cryptography and they are used as a building box in many secure protocols, e.g., general protocol for multiparty computation, Byzantine agreement, threshold cryptography, access control, attribute-based encryption, and generalized oblivious transfer. In this survey, we will describe the most important constructions of secret-sharing schemes, explaining the connections between secret-sharing schemes and monotone formulae and monotone span programs. The main problem with known secret-sharing schemes is the large share size: it is exponential in the number of parties. We conjecture that this is unavoidable. We will discuss the known lower bounds on the share size. These lower bounds are fairly weak and there is a big gap between the lower and upper bounds [6]. For linear secret-sharing schemes, which is a class of schemes based on linear algebra that contains most known schemes, super-polynomial lower bounds on the share size are known. We will describe the proofs of these lower bounds. We will also present two results connecting secret-sharing schemes for a Hamiltonian access structure to the NP vs. coNP problem and to a major open problem in cryptography – constructing oblivious-transfer protocols from one-way functions [6].

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 11, November 2019

2. M. K. Aguilera, R. Janakiraman, and L. Xu, "Using Erasure Codes Efficiently for Storage in a Distributed System,"- Erasure codes provide space-optimal data redundancy to protect against data loss. A common use is to reliably store data in a distributed system, where erasure-coded data are kept in different nodes to tolerate node failures without losing data. In this paper, we propose a new approach to maintain ensure-encoded data in a distributed system. The approach allows the use of space efficient k-of-n erasure codes where n and k are large and the overhead n-k is small. Concurrent updates and accesses to data are highly optimized: in common cases, they require no locks, no two-phase commits, and no logs of old versions of data. We evaluate our approach using an implementation and simulations for larger systems [2].

3. W. Aiello, M. Bellare, G. D. Crescenzo, and R. Venkatesan, "Security amplification by composition: The case of doublyiterated, ideal ciphers," - One concern in using cloud storage is that the sensitive data should be confidential We investigate, in the Shannon model, the security of constructions corresponding to double and (two-key) triple DES. That is, we consider Fk1 (Fk2 ()) and Fk1 (F 1 k2 (Fk1 ())) with the component functions being ideal ciphers. This models the resistance of these constructions to \generic" attacks like meet in the middle attacks. sense. We compute a bound on the probability of breaking the double cipher as a function of the number of computations of the base cipher made, and the number of examples of the composed cipher seen, and show that the success probability is the square of that for a single key cipher. meet in the middle is the best possible generic attack against the double cipher. local revocable group signature and identity-based broadcast encryption with constant size cipher text and private keys. To realize our concept, we equip the broadcast encryption with the dynamic cipher text update feature, and give formal security guarantee against adaptive chosen-cipher text decryption and update attacks [3].

4. A.Desai, "The security of all-or-nothing encryption: Protecting against exhaustive key search," - We investigate the all-or-nothing encryption paradigm which was introduced by Rivest as a new mode of operation for block ciphers. The paradigm involves composing an all-or-nothing transform (AONT) with an ordinary encryption mode. The goal is to have secure encryption modes with the additional property that exhaustive key-search attacks on them are slowed down by a factor equal to the number of blocks in the cipher text. We give a new notion concerned with the privacy of keys that provably captures this key-search resistance property. We suggest a new characterization of AONTs and establish that the resulting all-or-nothing encryption paradigm yields secure encryption modes that also meet this notion of key privacy. A consequence of our new characterization is that we get more efficient ways of instantiating the all-or-nothing encryption paradigm. We describe a simple block-cipher-based AONT and prove it secure in the Shannon Model of a block cipher. We also give attacks against alternate paradigms that were believed to have the above key search resistance property [12].

5. M. Dürmuth and D. M. Freeman, "Deniable encryption with negligible detection probability**,"** - Deniable encryption, introduced in 1997 by Canetti, Dwork, Naor, and Ostrovsky, guarantees that the sender or the receiver of a secret message is able to "fake" the message encrypted in a specific cipher text in the presence of a coercin gadversary, without the adversary detecting that he was not given the real message. To date, constructions are only known either for weakened variants with separate "honest" and "dishonest" encryption algorithms, or for single-algorithm schemes with non-negligible detection probability. We propose the first sender-deniable public key encryption system with a single encryption algorithm and negligible detection probability. We describe a generic interactive construction based on a public key bit encryption scheme that has certain properties, and we give two examples of encryption schemes with these properties, one based on the quadratic residuosity assumption and the other on trapdoor permutations [24].

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 11, November 2019

III. EXISTING SYSTEM

- Seroussi et al. proposed to make use of the information from users' public profiles and topics extracted from user generated content into a matrix factorization model for new users' rating prediction [9].
- Zhang et al. propose a semi-supervised ensemble learning algorithm.
- Schein proposed a method by combining content and collaborative data under a single probabilistic framework.
- Lin et al. addressed the cold-start problem for App recommendation by using the social information.

DISADVANTAGES OF EXISTING SYSTEM :

- They only focus on brand or category-level purchase preference based on a trained classifier, which cannot be directly applied to our cross-site cold start product recommendation task [12].
- They do not consider how to transfer heterogeneous information from social media websites into a form that is ready for use on the e-commerce side, which is the key to address the cross-site cold-start recommendation problem.

IV. PROPOSED SYSTEM

- In this paper, we study an interesting problem of recommending products from ecommerce websites to users at social networking sites who do not have historical purchase records [15].
- In our problem setting here, only the users' social networking information is available and it is a challenging task to transform the social networking information into latent user features which can be effectively used for product recommendation. To address this challenge, we propose to use the linked users across social networking sites and ecommerce websites (users who have social networking accounts and have made purchases on e-commerce websites) as a bridge to map users' social networking features to latent features for product recommendation [13].
- In specific, we propose learning both users' and products' feature representations (called user embeddings and product embeddings, respectively) from data collected from ecommerce websites using recurrent neural networks and then apply a modified gradient boosting trees method to transform users' social networking features into user embeddings [5].
- We then develop a feature-based matrix factorization approach which can leverage the learnt user embeddings for cold start product recommendation.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 11, November 2019

ADVANTAGES OF PROPOSED SYSTEM:

- Our proposed framework is indeed effective in addressing the cross-site cold-start product recommendation problem.
- We believe that our study will have profound impact on both research and industry communities.
- We formulate a novel problem of recommending products from an e-commerce website to social networking users in "cold-start" situations [31].
- We propose to apply the recurrent neural networks for learning correlated feature representations for both users and products from data collected from an e-commerce website.
- We propose and instantiate a feature-based matrix factorization approach by incorporating user and product features for cold-start product recommendation [36].

V. IMPLEMENTATION

1. Data Owner :

In Data Owner module, Initially Data Owner must have to register their detail and admin will approve the registration by sending signature key and private key through email. After successful login he/she have to verify their login by entering signature and private key. Then data Owner can upload files into cloud server with Polynomial key generation. He/she can view the files that are uploaded in cloud by entering the secret file key [51].

2. Data User :

In Data User module, Initially Data Users must have to register their detail and admin will approve the registration by sending signature key and private key through email. After successful login he/she have to verify their login by entering signature and private key. Data Users can search all the files upload by data owners. He/she can send search request to admin then admin will send the search key. After entering the search key he/she can view the file [49].

3. Admin :

In Admin module, Admin can view all the Data owners and data user's details. Admin will approve the users and send the signature key and private key to the data owners and data users. Also admin will send the search request key to the users. Admin can able see the files in cloud uploaded by the data owners [55].

VI. CONCLUSION

We tend to self-addressed the matter of securing knowledge outsourced to the cloud against Associate in Nursing resister that has access to the encoding key. For that purpose, we tend to introduced a unique security definition that captures knowledge confidentiality against the new resister. We tend to then planned Bastion, a theme that ensures the confidentiality of encrypted knowledge even once the resister has the encoding key, and every one however 2 cipher text blocks. Bastion is most fitted for settings wherever the cipher text blocks ar hold

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 11, November 2019

on in multi-cloud storage systems. In these settings, the resister would wish to accumulate the encoding key, and to compromise all servers, so as to recover any single block of plaintext. we tend to analyzed the safety of Bastion and evaluated its performance in realistic settings. Bastion significantly improves (by quite 65%) the performance of existing primitives which provide comparable security beneath key exposure, and solely incurs a negligible overhead (less than 9%) when put next to existing semantically secure encoding modes (e.g., the CTR encoding mode). Finally, we tend to showed however Bastion are often much integrated inside existing distributed storage systems.

VII. ACKNOWLEDGEMENT

The author would like to thank the ***Founder & Chairman*** of ***I.S.L Engineering College***, Hyderabad, Telangana, for their motivation and constant encouragement, over the years our college has been become synonymous with quality education, infrastructure and practice. "When a Women is a graduate every home will be a University" & beyond providing a sound education, our chairman is to provide our students a holistic learning experience for life. The author would like to specially thank **Dr. Ar. Arunachalam, Head of Dept.,** School of Computing, **Dr. M.G.R. Educational & Research Institute & Dr. K.P. Kalyiemurthie, Dean** School of Computing**, Bharath University, Chennai** for his guidance and for critical review of this manuscript and for his valuable input and fruitful discussions in completing the work and the Faculty Members of Department of Computer Science & Engineering. Also, he takes privilege in extending gratitude to his **parents and family members** who rendered their support throughout this Research work.

REFERENCES

1. M. Abd-El-Malek, G. R. Ganger, G. R. Goodson, M. K. Reiter, and J. J. Wylie, "Fault-Scalable Byzantine Fault-Tolerant Services," in ACM Symposium on Operating Systems Principles (SOSP), 2005, pp. 59–74.
2. M. K. Aguilera, R. Janakiraman, and L. Xu, "Using Erasure Codes Efficiently for Storage in a Distributed System," in International Conference on Dependable Systems and Networks (DSN), 2005, pp. 336–345.
3. W. Aiello, M. Bellare, G. D. Crescenzo, and R. Venkatesan, "Security amplification by composition: The case of doublyiterated, ideal ciphers," in Advances in Cryptology (CRYPTO), 1998, pp. 390–407.
4. C. Basescu, C. Cachin, I. Eyal, R. Haas, and M. Vukolic, "Robust Data Sharing with Key-value Stores," in ACM SIGACTSIGOPS Symposium on Principles of Distributed Computing (PODC), 2011, pp. 221–222.
   A. Beimel, "Secret-sharing schemes: A survey," in International Workshop on Coding and Cryptology (IWCC), 2011, pp. 11–46.
   B. Bessani, M. Correia, B. Quaresma, F. André, and P. Sousa, "DepSky: Dependable and Secure Storage in a Cloud-of clouds," in Sixth Conference on Computer Systems (EuroSys), 2011, pp. 31–46.
5. G. R. Blakley and C. Meadows, "Security of ramp schemes," in Advances in Cryptology (CRYPTO), 1984, pp. 242–268.
6. BOYKO, "ON THE SECURITY PROPERTIES OF OAEP AS AN ALLOR-NOTHING TRANSFORM," IN ADVANCES IN CRYPTOLOGY (CRYPTO), 1999, PP. 503–518.
7. R. Canetti, C. Dwork, M. Naor, and R. Ostrovsky, "Deniable Encryption," in Proceedings of CRYPTO, 1997.
8. M. Brust, C. Ribeiro, and J. Filho, "Border effects in the simulation of ad hoc and sensor networks," in Computer Modelling and Simulation, 2009. UKSIM '09. 11th International Conference on, March 2009, PP. 180–185.
9. 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.
10. M. Matsumoto and T. Nishimura, "Mersenne twister: A 623-dimensionally equidistributed uniform pseudo-random number generator," ACM Trans. Model. Comput. Simul., vol. 8, no. 1, PP. 3–30, Jan. 1998.
11. 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.
12. G. Bianchi, "Performance analysis of the IEEE 802.11 distributed coordination function," IEEE J. Sel. Areas Commun., Vol. 18, No. 3, PP. 535–547, Mar. 2000.
13. R. Blakley and C. Meadows, "Security of ramp schemes," in Advances in Cryptology (CRYPTO), 1984, pp. 242–268.
14. BOYKO, "ON THE SECURITY PROPERTIES OF OAEP AS AN ALLOR-NOTHING TRANSFORM," IN ADVANCES IN CRYPTOLOGY (CRYPTO), 1999, PP. 503–518.
15. K.G.S. Venkatesan, "Comparison of CDMA & GSM Mobile Technology", Middle-East Journal of Scientific Research, 13 (12), PP. 1590 – 1594, 2013.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 11, November 2019

16. 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.
17. J. P. Coon, C. P. Dettmann, and O. Georgiou, "Full connectivity: Corners, edges and faces," Journal of Statistical Physics, Vol. 147, No. 4, PP. 758– 778, 2012.
18. 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.
19. 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.
    A. Eslami, M. Nekoui, H. Pishro-Nik, and F. Fekri, "Results on finite wireless sensor networks: Connectivity and coverage," ACM Trans. Sen. Netw., vol. 9, no. 4, pp. 51:1–51:22, Jul. 2013.
20. 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.
21. 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.
22. K.G.S. Venkatesan, "Comparison of CDMA & GSM Mobile Technology", Middle-East Journal of Scientific Research, 13 (12), PP. 1590 – 1594, 2013.
23. S. A. de Chaves, R. B. Uriarte, C. B. Westphall, "Toward an Architecture for Monitoring Private Clouds", IEEE Communications Magazine, Vol. 49, no. 2, pp. 130-137, 2011.
24. S. Clayman, A. Galis, C. Chapman, et al., "Monitoring Service Clouds in the Future Internet". Future Internet Assembly, pp. 115-126, 2010.
25. L. A. Laranjeira and G. N. Rodrigues, "Extending the reliability of wireless sensor networks through informed periodic redeployment." in SERE. IEEE, 2012, pp. 167–176.
26. 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.
27. 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
28. K.G.S. Venkatesan, "Comparison of CDMA & GSM Mobile Technology", Middle-East Journal of Scientific Research, 13 (12), PP. 1590 – 1594, 2013.
29. 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.
30. K.G.S. Venkatesan. Kishore, Mukthar Hussain, "SAT : A Security Architecture in wireless mesh networks", International Journal of Advanced Research in computer science & software Engg., Vol. 3, Issue 3, PP. 325 – 331, April – 2013.
31. Annapurna Vemparala, K.G.S. Venkatesan, "A Reputation based scheme for routing misbehavior detection in MANET"S ", International Journal of computer science & Management Research, Vol. 2, Issue 6, June - 2013.
32. 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.
33. 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.
34. K.G.S. Venkatesan, AR. Arunachalam, S. Vijayalakshmi, V. Vinotha, "Implementation of optimized cost, Load & service monitoring for grid computing", International Journal of Innovative Research in computer & comm. Engineering, Vol. 3, Issue 2, PP. 864 – 870, February - 2015.
35. R. Karthikeyan, K.G.S. Venkatesan, M.L. Ambikha, S. Asha, "Assist Autism spectrum, Data Acquisition method using Spatio-temporal Model", International Journal of Innovative Research in computer & communication Engineering, Vol. 3, Issue 2, PP. 871 – 877, February - 2015
36. 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.
37. K.G.S. Venkatesan. Dr. V. Khanaa, "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.
38. 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.
39. 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.
40. K.G.S. Venkatesan, Dr. V. Khanaa, 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.
41. K.G.S. Venkatesan, Dr. V. Khanaa, S.B. Amarnath Reddy, "Network Monitoring using Test Packet Generation", IJSCONLINE, PP. 1-12, March – 2015.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 11, November 2019

42. BOYKO, "ON THE SECURITY PROPERTIES OF OAEP AS AN ALLOR-NOTHING TRANSFORM," IN ADVANCES IN CRYPTOLOGY (CRYPTO), 1999, PP. 503–518.
43. R. Blakley and C. Meadows, "Security of ramp schemes," in Advances in Cryptology (CRYPTO), 1984, pp. 242–268.
44. W. Aiello, M. Bellare, G. D. Crescenzo, and R. Venkatesan, "Security amplification by composition: The case of doublyiterated, ideal ciphers," in Advances in Cryptology (CRYPTO), 1998, pp. 390–407.
45. K.G.S. Venkatesan, Dr. V. Khanaa, 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. K.G.S. Venkatesan, Dr. V. Khanaa, Anish Kumar Anbakarasan, Ilampiria Nagarajan , "Safety and Moral Affairs in cyber space : An IT Firm's prospects", International Journal of Innovative Research in computer & communication Engineering, Vol. 3, Issue 7, PP. 6742 – 6751, July - 2015.
47. 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.
48. 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.
49. 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.
50. K.G.S. Venkatesan, "Comparison of CDMA & GSM Mobile Technology", Middle-East Journal of Scientific Research, 13 (12), PP. 1590 – 1594, 2013.
51. Annapurna Vemparala, K.G.S. Venkatesan, "A Reputation based scheme for routing misbehavior detection in MANET"S ", International Journal of computer science & Mangement Research, Vol. 2, Issue 6, June - 2013.
52. 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.
53. 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.
54. K.G.S. Venkatesan, "Comparison of CDMA & GSM Mobile Technology", Middle-East Journal of Scientific Research, 13 (12), PP. 1590 – 1594, 2013.
55. H. Kim, H. Lee, W. Kim, Y. Kim, "A Trust Evaluation Model for QoS Guarantee in Cloud Systems", International Journal of Grid and Distributed Computing, vol.3, no.1, pp. 1-10, 2010.
56. W. Aiello, M. Bellare, G. D. Crescenzo, and R. Venkatesan, "Security amplification by composition: The case of doublyiterated, ideal ciphers," in Advances in Cryptology (CRYPTO), 1998, pp. 390–407.