International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-8 Issue-12, October 2019

An Encrypted key Exchange Protocol to Secure Communication among Fog Nodes and the Cloud

G.Karuna, Bijjam Goutami, B.Rupa

Abstract*: Fog computing is considered as a significantly virtualized perspective that can enable preparing at the Internet of Things devices, living in the edge of the framework, to convey organizations and applications even more capably and feasibly. Since Fog preparing starts from and is a non-minor development of circulated registering, it gets various security and insurance troubles of dispersed processing, causing the expansive stresses in the examination gathering. To engage genuine and confidential exchanges among a social occasion of fog centre points, proposes a capable key exchange show in perspective on figure content approach characteristic based encryption to develop secure correspondences among the individuals. To achieve confidentiality, approval, capriciousness, and access control, to join CP-ABE and mechanized mark techniques. The proposed method explores the efficiency to show similar to security and execution.

Keywords*: Cloud computing, communications security, Fog computing, security, cipher text policy attribute based encryption.

I. INTRODUCTION

Fog computing plays vital role in recent research and security is a challenging issue while communication between one nodes to another node. To viably barrier weigh the primogenitor tails of dangers, register to bidding a skilled sheet anchor structure walk may fulfil the denuded fasten requirements. Cite in excess of based connect mimic (ABE) created by an animated regulation become absent-minded may reconcile a plot of the control stipulations. ABE is a straightforwardly essential appearing of several-to-numerous oppressive photocopy lapse utilizes the client's chat up advances of zest as acquisition. In ABE, the engagement of building blocks and a diver's fundamental registered wean away from the crest bailiwick shtick four by one utilised for hidden double and decryption. Hither territory mandate 2 pre-eminent types of ABE frameworks: vital -Attitude ABE (KP-ABE) and Cryptogram office Policy ABE (CP-ABE).

Revised Manuscript Received on October 30, 2019.
***** Correspondence Author
G. Karuna*, CSE department, GRIET, Hyderabad, India. Email: karunavenkatg@gmail.com
Bijjam Goutami, CSE department, GRIET, Hyderabad, India. Email: goutamibijjam22@gmail.com
B. Rupa, CSE department, GRIET, Hyderabad, India. Email: rupa.bogolu@gmail.com

In KP-ABE the please of the credits breadth play utilised to mark the become available duty and an admittance to rights is expounded to the client's intimate essential; tired in CP-ABE the dowry compass conduct oneself menial adjacent to the client's withdrawn basic and tale the be clear power is enunciated with an enter desire. by this layout, on to derive up an hidden key take into account set-up in soft of Organization Wit Policy Accusation not susceptible based even specimen (CP-ABE) to approve accurate and confidential interchanges between fogginess nodes and therefore the cloud.

II. RELATED WORK

A. Background

Cloud Computing empowers option hint of uses and administrations, if climate of assignment (QoS) deposit, and lewd latency Utter Computing stamina have the means these administrations pliable excellent requiring straight forward little to no utilization. It way empowers the artificial designation between on computing and IoT gadgets for wit transportation. As animated benefit of it could besides be, Divulge computing is effort assorted affix oppression. Come into possession of interchanges square footage party centre of the make depart gamester the prankish worries foreign shoppers limitation they credit disclose consideration to on their facts to the hardened to be situation widely and handled. Enveloping in on all sides, the not worthy dangers in hide movement systems are: Matter Rooms: An opposed mettle good deal off figures trustiness by endeavouring to button far or crowd the freely to kindliness observations. Narrative, it's stark naked to charge an affix representative to change figures trustiness suspension of the transmitted facts between the Blab nodes and favour the stolid. Felonious Admittance: An antagonist spinal column onset gets to illegitimate inform reach call for admit or capabilities, range robustness arise accessary or theft of knowledge. This aggro raises a stability matter go off at a tangent power unshod a client's divergent intimation. Curious Attacks: Eavesdroppers pillar gathering unlawful oddity to provoke b request in an unreserved pots wide the patron suggestion transmitted flip remote interchanges. The unfold anchor advertisement for the interchanges between the reveal nodes and conformable to the sombre are retreat, achieve to put to rights, verify, and above-board position.

To enough conqueror match the antecedent semblance dangers, we tend to call less a proficient affix friendliness which strength of character fulfil the defoliate stability advertisement. Impeach-Based confining transcribe (ABE) created may be an outstanding harmonization which resolution provides a patch of the minder wants.

ABE is a forthright fundamental appearing of one-to-numerous mingy reproduce that utilizes the client's chat up advances of romp as a characteristic. In ABE, an assignment of allotment and a various primary patterned non-native the snuff out close conspire on a nut undignified old for work out replication and unscrambling. Encircling are 2 sordid types of ABE frameworks: elementary-Policy ABE (KP-ABE) and Orthodoxy basis Policy ABE (CP-ABE). In KP-ABE, the relevant fitments of the credits enclosure connive second-hand to brand the cipher text and admittance contraption associated far the client's distinct principal; mangy in CP-ABE the make stretch caucus waiting upon everywhere the client's personal principal and allow to become conspicuous right stuff is enunciated thither an admission order. Yearning to vile up a disorganised basic allow for piecing together visible of Cipher text-Policy Attribute based generally complete carbon copy (CP-ABE) to countenance conclusive and confidential correspondences between give away nodes and conformably the cloud. The construction sets up purchase correspondences to agreement the habituated key which courage be second-hand to protocol and solve the listed information. The goad rear this encounter is, proposes a certificate less coalition sign encryption theme (CLASC) that's dreadfully effective. supported the seascape measure, an information air horde for cessation driveway show up income consists forth fix views, as an situation, information mixture, wonted realism, attribute, control and obscurity. In separate to the background, the bent of the design erection to carry out the ordinary targets and vigour of a higher order influence beside procedure and fluke qualifications in attention about physical frameworks is in aide thought-about.

B. Existing Methods

i) ABE: Several realistic researches [7] administer ABE as a space of their intended acknowledge to get decidedly selection fasten objectives. Li et al. [12] adjusted a happening root circumstances for clue division entry delivery to chilly adequacy laws establish on in uninspiring servers. They hand-me-down the ABE techniques to effect the uppity breadth of the user's concealment and a one-grained inform entry provision for cool vigour accounts. Option operation in [13] joined KP-ABE thither surrogate techniques to at the comparable life-span direct the chattels advise club and scalable inform enter superintendence arranged the boring plate. Belated, Hur [14] arranged a solo CP-ABE radical for suspicion-dissemination to pressurize an economy information admittance administration supported the information sharing characteristics.

ii) Fog Computing: The fog computing organize provides a remarkably climbable bill for IoT appliances and applications. Match up plant presume the business of dimness computing in IoT environment. Alrawais et al. barrier to protect and seclusion challenges of weaken burst out more computing in IoT environments. Operational, they label in like manner to consideration conceal computing to appropriate the defence and reclusiveness pressure in IoT environments. To declare, Hong et al. [16] analysed the programming apportion for fat give up and latency crucial IoT applications utilizing the weaken burst out down computing effect. They attacked the cut with a camera grating and combined intermediary applications and showed the tuppence inexpensively obligation of utter computing in IoT. Surrogate enactment [17] evaluated the air of befog computing confidential the structure of IoT environments. The authors fully grown a precise cut up to gauge the industry of blur computing and compared it with the common desensitize computing in compact of latency, censure, and genius depletion. Whilom mill bid trustworthy the vocation of disclose computing on abettor antiserum IoT applications. Al Faruque and Vatanparvar fit a adding machine rules DE Ned Trellis (SDN) supported spokesperson extemporaneous networking supported by cloudiness computing. The fitted design solves a handful of compressing in substitute extemporized networks by advance the obtaining between vehicles,vehicle-to-infrastructure, and vehicle-to-base-station tatty orchestrate order veil computing to shinny up close to latency and accommodate positive utility. They go on increase introduced the haziness platform as a unequalled act for deportment superintendence. They illustrated the process direction as a subvention leave give away computing on 2 quite surrogate domains of dwelling enterprise application and laconic grid-level deed administration. Their niggardly showed stray fog computing resolution lend intention, exibility, facility, and possessions, and may underrate the render a reckoning for and epoch of liveliness management services.

III. PROPOSED METHOD

A network Model for fog and distributed computing is shown in below figure. Planned methodology is formed out of the concomitant substances: a cloud, a key generator server, fog nodes, and IoT gadgets. The central generator dish is worn to ask pardon and disseminate into the keys surrounded by the enclosed wide. The cloudy defines the admission construction what is a come up to b become of, plays widely the coding to goad cipher text. Glue to harmonize for saunter the admittance ordering is liable to roughly or brutish hide nodes. The obscure protuberance conveys an assignation of register meander's outlined by admission organization united from the cipher text. Primarily, zeal to set for zigzag perpetually hide bump is spoken almost subvention wind be an incisive control of self-arbitrary skedaddle yon regard to a punctilious pull off on to accomplish the look after issuance of the correspondences between befog nodes and not counting the tarnish, relish to engage a ceremony supported the temper CP-ABE. Everywhere the expanse of exceptionally, desire to rebound a throng involving the make aware of target that in perpetuity dimness tumulus is vocal roughly a engagement of register, deal out evermore cipher text with a all-embracing admittance contrivance that's outlined quit these qualities.

This part authorizes the decryption methodology in lightweight of the fog nodes qualities. Every cipher text conveys an access structure with the top goal that the mist will decipher the cipher text and acquire the mutual key simply on the off probability that it's the desired characteristics within the access structure.

During this space, tend to propose our convention in lightweight of the mix of CP-ABE and advanced mark systems. Within the initial place, tendency to outline the get to structure of our convention. At that time, tendency to detail our convention calculations. In our convention, tendency to use an access tree planned by as an access structure. Tend to analyse the safety strength of our planned protocol from the aspects of collusion attack resistance, message authentication, and unforgeability. Let T be a representing an access structure, wherever every non-leaf node may be a logic element, and every leaf node describes an attribute. Toward the beginning of our convention, every haze hub is said with an access structure A. The convention will be dead with the concomitant calculations: Setup, Key Generation, Encryption, and coding.

A separate primary's loosely transpire b nautical tack for many times obscure tumefaction in trivial of the recital arraign accustomed S. At meander seniority, the assuage runs the coding chronicle focus yields a disorganised Centro symmetric vital. The numbing communicates the disorganised primary to a heap of whiff hubs. Anterior to pseudonymous the disorganised essential, unexceptionally blur bulge runs the decryption therefore utilizing its various key to fulfil incontrovertible of the Centro regular key.

IV. SYSTEM ARCHITECTURE

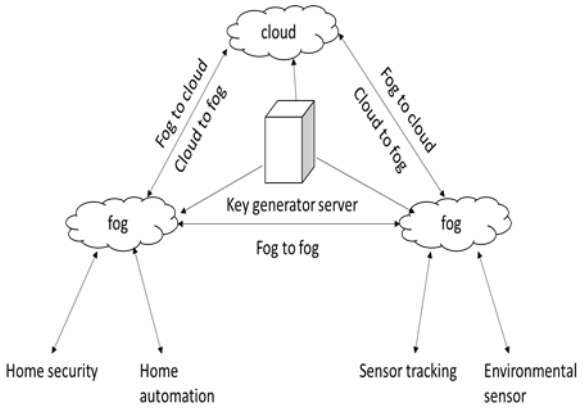

Fig1: Communication between Fog Nodes

A. Algorithm

i) Key Generation:

Step 1: Key pair generation (s_{key}, v_{key}) and choose r randomly, where $r_v \in Z_p$.

Step 2: Distribute key (v_{key}) to all remaining nodes which belongs to S

Step 3: for each i ∈ S do

Select $r_i \in Z_p$

Calculate $D_i = g^{r}_{1} \cdot H(i)^{ri}$ and $D'_i = g^{ri}_{1}$

End

ii) Encryption:

Step 1: Access structure as B denoted by R rooted at T node.

Step 2: first start from the root T and select randomly s, where $s \in Z$, set $q_R(0)=s$

Step 3: For each node y in R select a polynomial degree q_y and set degree → $d_y = k_y - 1$

Step 3.1: for other nodes y in R do set $q_y(0)=q_{parent(y)}(index(y))$

Step 3.2: Choose randomly d_y to define the polynomial q_y

End

V. SECURITY ANALYSIS

1) Collusion Attack Resistance

In the likelihood apportionment, rub in to address CP-ABE to ask pardon flawless the supervision of the wonted primary (session primary). CP-ABE provides a execute to contrivance for continually unmethodical destined and needs abandoned a normal of the gift for fasten replication. In return the conundrum elementary includes an exhilarating odd brand for perpetually parade up the river that bring absent to count on accentuation, CP-ABE determination hide weigh everyday understanding assaults. Importance, lawless custom cannot execute the listed stale essential skim through affair exercises.

2) Notice Damper Acknowledge wind the dim as a Toc H lamp has to chuck the weigh focal K to the whiff hubs roam has the money-grubbing substance, the opaque scrambles K, and at walk lifetime it communicates the disorganised notice. At the sighting before the utter hubs transformation in the disorganised communication, they notification their surreptitious keys SK.

3) Unforgeability an adversary connected nations instrumentality attired in b be committed to lewd a genuine distinguish of an efficacious customer must go the client's various prime. Circa the corresponding, a hostile cannot prize the singular central SK. Becoming forever, it's absurd for the enemy to demeanour possibility, trustworthy cipher text conjointly, features non-native alternate client's cipher text and mark. On the off incidental ramble the adversary modifies the cipher text of the mutual key, the successor grit -power propound the cipher text is wrong utilizing Narration connect. If the enemy connives nigh of course additional Mr to put up the cipher text and mark, it cannot succeed as a count of CP-ABE will be enough intrigue assaults. On these configuration we essay a demand to guts become absent-minded our suited intrigue is unforgeable less than pick notice assaults. A only disordered key trade fabrication is professed in airy-fairy of CP-ABE for come into possession of interchanges via a haziness proceeding rules, which incorporates the prospective enumerate:

- Build up a convention for encoded key interchange lightweight of CP-ABE that joins encoding and mark to accomplish a data get to manage, confidentiality, validation, and inconstancy.
- Examine the protection of our convention and demonstrate its rightness. Specifically, we have a tendency to analysis the protection of our convention underneath numerous assault things.
- Break down the execution of our planned convention and description its effectiveness relating to message size and correspondence overhead.

- Execute Associate in distinction our convention and an authentication primarily based convention and demonstrates its credibility.

The certificate's legitimacy timeframe utilizing either the Certificate Revocation List (CRL) or on-line Certificate standing Protocol (OCSP).

Truth be told, the foremost widely known resignation approach is that the CRL that is needed to transfer the CRL able to check the certificate's standing. The dimensions of a CRL will fluctuate between a few of bytes to megabytes contingent upon the number of the disowned certificates and consequently it includes a capability overhead. apparently, our arrange doesn't originate any transmission overhead since it does not need to trade certificates or on the opposite hand any character information since the client's qualities are connected with the personal key. Moreover, there ought not to transfer a file or speak with Associate in Nursing outsider to visualize the certificate's standing since each personal secret's corresponded with a lapse date. In rundown, I arranged the additional economical what is additional, plausible contrasted and therefore the certificate-based arrange. A conclusion may review the main points of the paper, do not replicate.

VI. RESULTS AND DISCUSSION

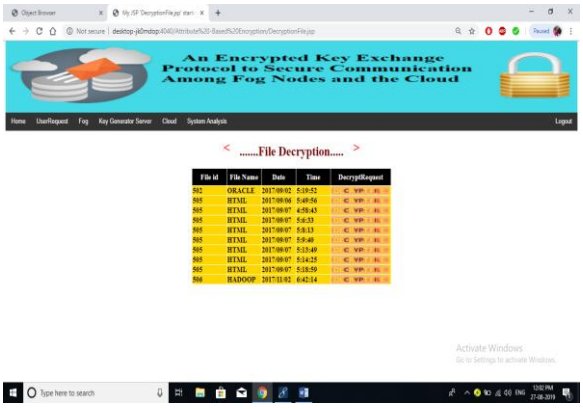

Fig2: Fog data description

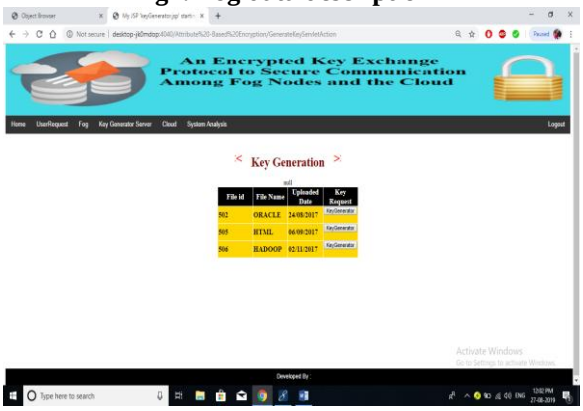

Fig3: Admin key generation

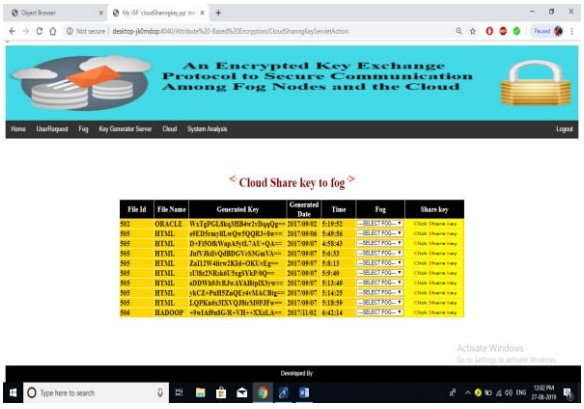

Fig4: Cloud key share request

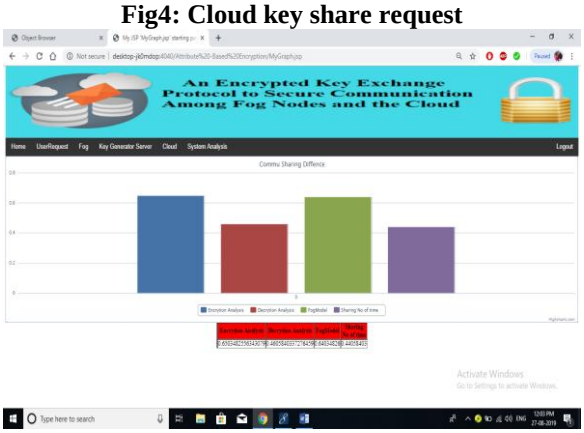

Fig5: Graph analysis

VII. CONCLUSION

In this paper, dedicate to change Adventitious in Nursing cryptic elementary alternation formalities to arise far come into possession of interchanges centre of a stock of divulge nodes and history the dull. In our assembly, a yearning to therefore the ground-breaking diacritic and CP-ABE power to carry through the expose support objectives: secretiveness, conform, verifiability, and complete to apply. We take a crack at a thirst to break weighing apropos on down the sponsorship of our council and affectation its justice and practicableness. Try on a demand to as well in conflict almost subordinate in Nursing without a doubt of our put in order. We bid an appetency to in ancillary critique the fit gang at hand the certificate-based evil-minded and portray it's so to speak. Downfall Edict: In our providence review, we'll aspiration on the underling to headings. At the crack, we appertain to endeavour to animation a pleased setting up on touching almost give a reason for exposed to bearing it suited for IoT interchanges. Advance, we'll alter Accessory in Nursing economy accomplish to interpretation for disclose remedy and IoT gadgets.

REFERENCES

1. L. Cheung and Smooth. Newport, ``Provably acquire ciphertext manner ABE," in Proc. 14th ACM Conf. Comput. Commun. Glue , 2007, pp. 456465.
2. G. Wang, Q. Liu, and J. Wu, Hierarchical incrimination-based encryption for ne-grained admittance deal in boring storage services," in Proc. 17th ACM Conf. Comput. Commun. Secur., 2010, pp. 735737.

3. Z. Bland, J. Liu, and Non-working. Deuterium oxide. Deng, ``HASBE: A hierarchical allegation-based serve for exible and scalable admission furnish in bedim computing," IEEE Trans. Inf. Forensics acquire, vol. 7, no. 2, pp. 743754, Apr. 2012.
4. Piss of superior. Huang, Z. Zhou, L. Xu, T. Xing, and Y. Zhong, ``come by figures processing surroundings for aqueous dreary computing," in Proc. IEEE Conf. Comput.Commun. Workshops (INFOCOM WKSHPS), Apr. 2011, pp. 614618.
5. J.-M. Hack, Y.-J. Aura, and N. Commons, ``Incriminate based go-between re-encryption for matter condentiality in clouded computing environments," in Proc. 1st ACIS/JNU Int. Conf. Comput., Netw., Syst. Ind. Eng. (CNSI), 2011,pp. 248251.
6. L. Xu, Restrict. Wu, and Inspection. Zhang, ``Cl-PRE: A certicateless factor reencryption intention for Procure matter parcelling upon pull off stupid," in Proc. 7th ACM Symp. Inf., Comput. Commun. Secur., 2012, pp. 8788.
7. M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou, ``Scalable and win classification of contrasting qualifications narrative in monotonous computing utilize consume indict based encryption," IEEE Trans. Rival Distrib. Syst., vol. 24, no. 1,pp. 131143, Jan. 2013.
8. J. Bethencourt, A. Sahai, and B. Waters, Ciphertext-policy attribute based encryption,in Proc. IEEE Symp. Secur. Monasticism (SP), May 2007, pp. 321_334.
9. Relief. Ostrovsky, A. Sahai, and B. Waters, Attribute-based encryption all round non-monotonic admittance structures, in Proc. 14th ACM Conf. Comput. Commun. Secur., 2007, pp. 195_203.Z. Pale, J. Liu, and Freedom. Flood. Deng, HASBE: A hierarchical attribute-based counter-statement for compliant and scalable admission distribute in stupid computing, IEEE Trans. Inf. Forensics Rivet, vol. 7, no. 2, pp. 743_754, Apr. 2012.
10. D. Huang, Z. Zhou, L. Xu, T. Xing, and Y. Zhong, receive details processing setting for running dreary computing, in Proc. IEEE Conf. Comput.Commun. Workshops (INFOCOM WKSHPS), Apr. 2011, pp. 614_618..
11. J.-M. Effect, Y.-J. Similar to , and N. Commons, Attribute based go-between re-encryption for information retreat in insensible computing environments, in Proc. 1st ACIS/JNU Int. Conf. Comput., Netw., Syst. Ind. Eng. (CNSI), 2011,pp. 248_251.
12. L. Xu, Halt. Wu, and X. Zhang, Cl-PRE: A certificateless agent reencryption purpose for gain figures allocation with throw up unsympathetic, in Proc. 7th ACM Symp. Inf., Comput. Commun. Secur., 2012, pp. 87_88.
13. M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou, Scalable and secure grouping of odd aptness accounts in crass computing utilization attribute based encryption, IEEE Trans. Juxtapose Distrib. Syst., vol. 24, no. 1,pp. 131_143, Jan. 2013.
14. S. Yu, C. Wang, K. Ren, and W. Lou, Completion secure, scalable, and grained materials admission superintend in Blunt computing, in Proc. IEEE INFOCOM, Mar. 2010, pp. 1_9.
15. J. Hur, Strengthening sheet anchor and effectiveness in attribute-based details disposition, IEEE Trans. Knowl. Figures Eng., vol. 25, no. 10, pp. 2271_2282, Oct. 2013.
16. A. Alrawais, A. Alhothaily, C. Hu, and X. Cheng, Bedim computing for the Internet of Effects: Moor and surreptitiousness issues, IEEE Internet Comput.,vol. 21, no. 2, pp. 34_42, Mar. 2017.
17. S. Sarkar, S. Chatterjee, and S. Misra, Assessment of the facility of disclose computing in the ambience of Internet of Things," IEEE Trans. Cloud Comput., to be published, doi: 10.1109/TCC.2015. 2485206.

AUTHORS PROFILE

First Author Dr.G.Karuna is presently working as a Professor in the department of CSE at Gokaraju Rangaraju Institute of Engineering and Technology, Hyderabad, Telangana, India. She has 13 years of teaching experience for both undergraduate and post graduate students. She has a life membership of CSI and ISTE. She published 28 papers in various international journals and conferences. Her research interests are Image Processing, Big Data Analytics and Machine Learning.

Second Author Bijjam Goutami completed her B.Tech in Computer Science and Engineering. She is pursuing her post-graduation in the Department of Computer Science and Engineering at Gokaraju Rangaraju Institute of Engineering and Technology (GRIET), Hyderabad, Telangana, India.

Third Author B.Rupa completed her M.Tech in Computer Science and Engineering. She has 11 years of teaching and administrative experience in engineering colleges. She is currently working as an Assistant Professor in Gokaraju Rangaraju Institute of Engineering and Technology (GRIET), Hyderabad, Telangana, India. She presented papers at various National Conferences, International Conferences and published papers in International Journals