A Secure Cloud-Based Heterogeneous Network using A Novel Routing Protocol For Smart Military Applications

M Hemanth Chakravarthy, Pethuru Raj, A. Suresh, E A Neeba, S Sasikala

***Abstract:** Having understood the strategic significance of the flourishing cloud idea, enterprises across the globe are keenly strategizing and executing to embark on the cloud journey with all the clarity and confidence. There are product vendors bringing forth additional capabilities to easily and quickly setup and sustain competent cloud environments, which are being positioned as the one-stop IT solution for worldwide business organizations. The business domains such as governments, retail stores, healthcare providers, telecommunication service providers, supply chain and logistics, utilities, homeland security, etc. are keenly embracing the cloud idea to be ahead of their competitors in their operations, outputs and offerings. However, there are some critical challenges and concerns being associated with the cloud paradigm. The widely quoted non-functional requirements (NFRs) and the quality of service (QoS) attributes such as security, performance, reliability, modifiability, and availability have to be fulfilled by cloud software, platform and infrastructures in order to boost the confidence level of business executives and institutions. There are mission-critical and emergency services, which are finding their residence in cloud environments (private, public and hybrid). Their requirements are quite unique and hence researchers across the globe are striving hard and stretching further to bring forth innovative, disruptive and transformation technology solutions to fulfill the various needs.This paper proposes a cloud-based network architecture that contributes a consistent and ubiquitous Internet connection. The mesh topology is recommended here to ensure that the connectivity is available all the time without any fail and slowdown. The security of data when it gets transmitted over channels, persisted in data stores, and used by applications, has to be ensured in order to boost the confidence of data owners and users. Hence, this paper proposes a secure cloud-based heterogeneous network using a novel routing protocol.*

***Index terms** — Cloud, Security, Emergency Services, Heterogeneous Network, Military Network, Elliptical Curve Cryptography (ECC), Hybrid Elliptical Curve Cryptography (HECC).*

Revised Manuscript Received on April 06, 2019.

M Hemanth Chakravarthy, Application Development Team Lead, Accenture Technology, Perungalathur, Chennai-63, TamilNadu, India.

Pethuru Raj, Chief Architect and Vice President, Site Reliability Engineering (SRE) Division Reliance Jio Infocomm. Ltd. (RJIL), SARGOD Imperial, 23, Residency Road Bangalore 560025, India.

A.Suresh, Professor & Head, Department of Computer Science and Engineering, Nehru Institute of Engineering and Technology, T.M.Palayam, Coimbatore, 641105, TamilNadu, India.

E A Neeba, Assistant Professor, Department of Information Technology, Rajagiri School of Engineering & Technology, Rajagiri Valley, Kakkanad, Kochi – 682039, Kerala, India.

S Sasikala, Professor, Department of Computer Science and Engineering,
Paavai Engineering College, Namakkal, TamilNadu, India.

I. INTRODUCTION

As articulated above, there are several business-critical and emergency services, which are being taken to cloud environments. Cloud infrastructures are the most optimized and organized IT infrastructures, which are centralized, consolidated, virtualized and increasingly containerized. The cloud-enablement aspect is capable of bringing forth a number of unique innovations for institutions, individuals and innovators. In the recent past, due to the faster maturity and stability of cloud centers, the well-known emergency services such as homeland security (military services), mainland and inland security (police services), healthcare providers (hospitals and clinics), fire service, etc. are being hosted and managed in cloud environments. The secondary emergency service providers include aviation, border security, etc. These services are becoming indispensable for our daily lives.

The technologies and tools used by military services had been developed long time back and hence are not considered as modern and modular applications. The macro-level military application architecture is given below. The military networks are highly complicated and confused.

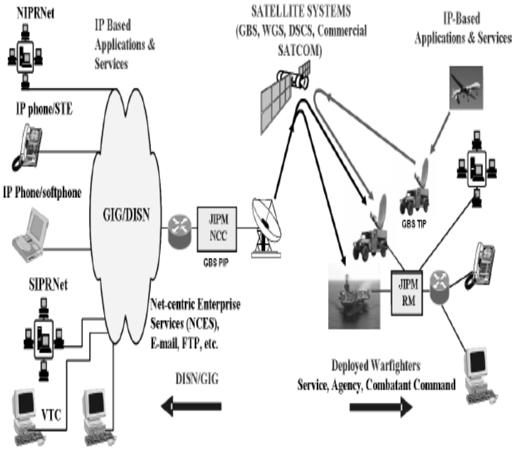
NIPRNet
IP Based Applications & Services
SATELLITE SYSTEMS (GBS, WGS, DSCS, Commercial SATCOM)
IP-Based Applications & Services
IP phone/STE
IP Phone/softphone
GIG/DISN
JIPM NCC
GBS PIP
GBS TIP
SIPRNet
JIPM RM
Net-centric Enterprise Services (NCES), E-mail, FTP, etc.
DISN/GIG
Deployed Warfighters Service, Agency, Combatant Command
VTC

Figure 1. A Sample Representation of Military Networks

- Maximum Obtainability – Unlike the currently available telecommunication (wired as well as wireless) networks, the military networks ought to be highly available. The availability, reliability and resiliency of military networks have to be guaranteed at any cost. They have to be highly fault-tolerant.
- Dependability – The information has to reach the desired end-points

without any hitch and hurdle.

- Amenities – The military networks have to be flexible enough to be integrated with other network such as Intranets and the Internet

From the above-mentioned requirements, it is clearly understood that the most important obligations of military services may be registered as 1) connectivity and obtainability of all communication mechanisms in all circumstances even after war occurrences 2) accessibility to internet and intranet facilities 3) dependable and appropriate transmission. The rest are certain investigating ventures which are presently carried out in order to make the subsequent group of the Internet, on account of the Global Environment for Network (GENI), which is supported financially by the U.S. National Science Foundation (NSF).

The foremost objective of these projects is to establish a connection between the satellites and the internet, in order to obtain utility by satisfying past experiments. This paperwork determined this issue, and established the network architecture which could encompass every key mechanisms of networks with the network connection, known as anywhere and anytime network (to accomplish the physical / hardware requirements), a protocol called smart for improved dependable transmission (to accomplish the software requirements).

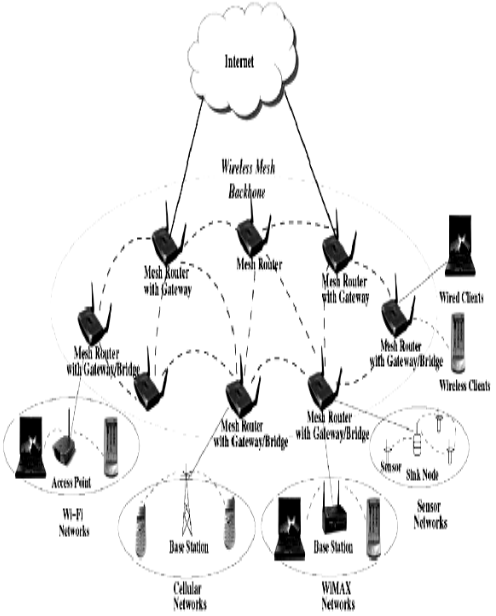

Figure 2. Heterogeneous Network using Mesh Routers as gateways

In section II, the paper explains the cloud based heterogeneous network architecture that contains of all the foremost communication devices and its interoperability with internet. In section III, the paper suggested protocol for dependable transmission to create the proposed heterogeneous network. In section IV & V, the paperwork defines the structure model, implementation as well as the result and performance analysis.

II. PROPOSED CLOUD BASED NETWORK ARCHITECTURE

In the past, the network structure was not built in the way that it could be used with a wide flexibility. But our proposed varied network construction deals with the integration of various network, called cloud computing. In cloud computing, many nodes which may be wired or wireless can integrate without compromising any characteristics. Fast expansion in this technology will also enlarge stern protection concern, since protection has an invariable concern, but this technology has several benefits such as lowering the cost, sufficient to maintain a wide service capture. The Network Interface Card (NIC) plays a key role here since it can outfit the systems such as the laptop, desktop computers, Mobile phone etc. Due to this outfit we can connect straight with the wireless mesh routers, which serve as the pathway for heterogeneous network.

It is attaining a noteworthy contemplation as a probable pathway for the Internet service providers (ISP), and the remaining to compress tough and consistent broadband service contact in a path which require low up-front reserves. The self-organization and self-configuration capacity of the cloud arranges each and every node at a particular instance as required. The more the nodes implemented, the consistency for the client will be increased. The conservative wireless router is used as the routing capability for the gateway working. Mesh router which could consist of some extra routing works can also be used which serves best for mesh networks.

In addition to increasing the suppleness of mesh-networks, a mesh router is typically outfitted among various cellular borders constructed on similar or dissimilar cellular contact equipments. Arbitrarily, MAC protocol in a mesh router is improved and has a good adaptability in a multiple hops mesh environment. These are all constructed in a hardware platform.

The routers of the mesh network can be constructed depending on devoted computers, e.g., embedded systems. This seems to be very dense, as shown in Fig.2. This can also be constructed depending on the laptops and desktop computers. The clients of the mesh network have essential functionality for the networks, and they can also work as a router. Moreover, the nodes could not be survived in the gateway functionalities. Moreover, the clients typically have an individual wireless interface. The end result is that the hardware and the software platform for the clients can be very simple when compared with the mesh routers. The clients will have various devices like laptop, desktop PC, PDA, RFID reader than that of the routers.

A typical infrastructure for connecting a variety of communication devices and to provide ***always-on-line anywhere anytime capability*** is shown in fig 2. This architecture has the capacity to bond wired, wireless, cellular and sensory equipment such as RFID and very simple to use. This could also survive for long since during the war the wired and wireless equipments may get damaged but these sensory equipments hold their responsibility and do their work. It also provides suppleness by incorporating through gateways and also connects the network through traditional equipment.

Organizing a WMN is very easy since every necessary component are by now obtainable in the form certain protocols like ad hoc network routing, IEEE 802.11 MAC, wired equivalent privacy (WEP) security, etc. Many investigation labs [1] [2] have understood about impending these expertise and proffer mesh networking solution. Home Mesh [3], In-Home IPTV [4] are certain WMN dependent relevancies. Moreover, to connect with the internet hard work of some researchers are required. For instance, the accessible MAC and routing protocols used in WMN do not have essential flexibility and the output falls when the nodes count is increased [6].

III. PROPOSED SECURED CLOUD BASED HETEROGENEOUS NETWORKS

A. Ant colony based mobile agent:

This particular procedure is very essential and affordable too. This particular algorithm has the finest solution by developing the simulated ants. Naturally the ant's action is based on searching for food and moves to places and discovers new paths. Whereas these simulated ants look for the solution space. The motion of these ants depends on the cologne which is deposited and the ants follow that way. Once the cologne gets vanished the system does not remember the old information and negotiate the rapid junction to trifling solution. This certain number of paths permit us to search for a huge number of solutions. This algorithm is very successful to various optimization techniques namely traveling salesman problem [8], routing [9], [10]. Certain proof for this pathway of Ant Colony optimization technique is established at [11]. In our paper, we used ant-like mobile agent for the gathering of data. The ant representatives budge in the network at random positions and scrutinize huge amount of nodes. Moreover, this will also gather some information regarding the network and contribute to its nodes. This process can be useful to speed up the optimization process by providing plenty of up to date information.

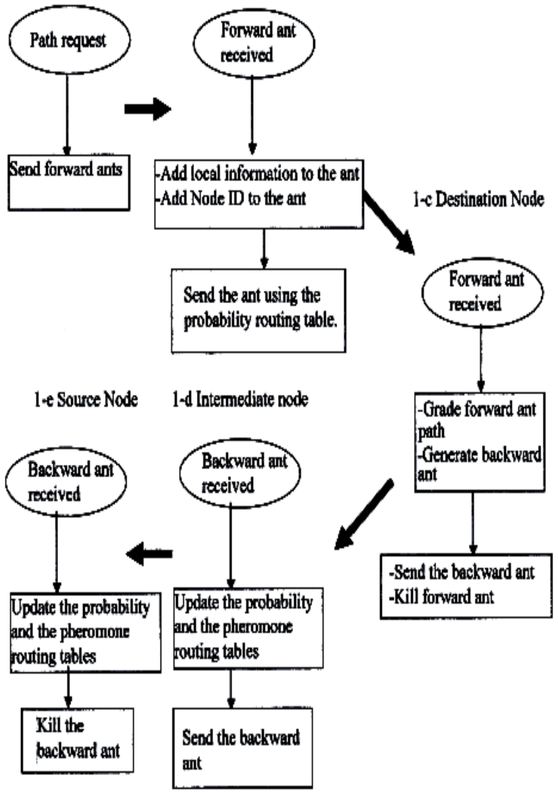

Figure 3. Second Level performance diagram of Ant colony based data collection

The routing table can be built by the formula given below: the neighbor j is selected by the destination D and node i and it is

$$prob(D,i,j)=\left\{\frac{Fun(TD,i,j,\eta)----if\,,j\in N}{\sum Fun(TD,i,j,\eta)---if\,,j\notin N}\right. \qquad -------$$

(1)

Here TD denotes the cologne value which corresponds to acquaintance j at node i and 0<TD<1 is the local empirical value of node j. $0 < \eta < 1$, represents the acquaintance's certain information like energy which remains, power required, delay process etc. Fun(TD, i, j, η) is a function in TD and η (when TD and η are maximum this value is maximum). N denotes the set of all possible acquaintances node demarcated by the ant's information as well as the direction-finding restrictions. The cologne value of every entrance in the table can be adjusted to equivalent terms which provides not biased hunt for the finest path. If certain information regarding the finest route is accessible then the cologne terms of the entrance could be fixed to the nearest value which fastens this algorithm.

B. HECC based Cloud Security

The proposed HECC is shown below:

- In the field of ECC, the prime case is denoted as 'p' and the binary case is denoted by 'm' and 'f' pair. The constants 'a' and 'b' are said as the elliptic curve in the equation.

- For current cryptographic purposes, the points of the plane curve over a known field should convince the below equation (2)

$$y^2 = x^3 + ax + b \qquad (2)$$

and also with a illustrious point at infinity.

- The cyclic subgroup is termed by its generator G. Many discrete logarithmic based protocol has been tailored to elliptic curves which reinstates the cluster $(Z_p)^x$ with an elliptic curve and this can be any of the five methods given below:
    1) the elliptic curve Diffie–Hellman (ECDH) key agreement scheme depends on the Diffie–Hellman scheme,
    2) the Elliptic Curve Integrated Encryption Scheme (ECIES) can also be said as Elliptic Curve Augmented Encryption Scheme,
    3) the Elliptic Curve Digital Signature Algorithm (ECDSA) depends on the Digital Signature Algorithm,
    4) the ECMQV key agreement scheme is based on the MQV key agreement scheme,
    5) the ECQV inherent the certificate scheme.
- For cryptographic purpose the order of G which is a small positive number n where nG is equal to infinity, is usually prime. As n denotes amount of a subcategory of $E(F_p)$, this depends on the Lagrange's theorem where the h is said to be an integer. The h is uttered in equation (2)

$$h = \frac{|E(F_p)|}{n} \qquad (2)$$

Where, h should be minimum (h≤4) and if possible, h is equal to one. Let’s sum up: in the prime case the domain parameters are (p, a, b, G, n, h) and in the binary case they are (m, f, a, b, G, n, h). curvature and implement a universal point-counting algorithm, for example, Schoof's algorithm, choose an arbitrary curve from a folk that permit effortless reckoning the amount of points. This could provide disparity among the finite-field cryptography (e.g., DSA) that needs 3072-bit public keys and 256-bit private keys, and integer factorization cryptography (e.g., RSA) that needs 3072-bit amount of n, from that the private key must be huge but the public key may be small to lodge well-organized encryption, particularly in the place where slighter processors are disturbed. HECC method is productively been worn in [13]. This method affords the most favorable refuge and the best among the accessible systems [15].

IV. RESULT AND PERFORMANCE ANALYSIS

The proposed cloud based secured military architecture is the arrangement of various networks together with the amount of unit worn. In our design, these values are RTT values from TCP communications, average packet loss and average response time of probable route. Hence, it is simulated using network simulator. The table 2 and table 3 showing the throughput and response time of existing and proposed military systems. The figure 4 represents the packet loss of existing military systems and proposed cloud based military systems.

Simulation-Parameters	Values-Obtained
Simulated-area	200 × 200 m2
Propagation	Two ray ground
MAC-type	802.11
Antenna	Omni-Antenna
Queue	Drop Tail/Priority
Queue-Limit	50
Amount of node	10 to 500
Packet-Type	CBR
Packet-size	220 Bits

Table 1 Simulation Parameters

Throughput in KB		
No of Nodes	**Existing System**	**Proposed System**
10	6	6
25	7	7
50	8	9
100	9	10
200	11	12
500	14	15

Table 2 Throughput of existing and proposed systems

Response Time in ms		
No of Nodes	**Existing System**	**Proposed System**
10	110	102
25	107	92
50	104	82
100	102	78
200	112	99
500	128	111

Table 3 Response Time of existing and proposed systems

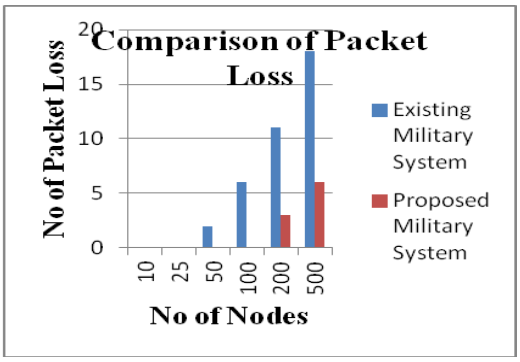

Figure 4 Packet Loss of existing and proposed military systems

V. CONCLUSION

From the results inscribed above, it is observed that there is no packet loss even at 100 nodes are transferring data at the time as the proposed military system has cloud resources. And the packet loss on above 100 nodes is also less than 25% of existing military systems. Similarly, the response time of proposed military system is faster than the existing military systems. The data receiving capability of the proposed and existing system are recorded in terms of throughput. The throughput of the proposed military system is always higher than the existing military systems. Hence, it is concluded that the proposed cloud-based secured and smart military system is more optimal than the existing military systems.

This work lays a stimulating foundation for cloud security researchers to unearth advanced security solutions and approaches for ensuring unbreakable and impenetrable security for essential and mission-critical services, which are increasingly deployed and delivered through cloud centers, which are coming up across the globe to meet up the growing needs of governments, business enterprises and commoners.

REFERENCES

1. BWN lab wireless mesh networks research project. Available from: <http://www.ece.gatech.edu /research /labs /bwn /mesh />.
2. Aguayo, Bicket, Biswas, De Couto, Morris, MIT Roofnet Implementation. Available from: <http: //pdos.lcs.mit.edu /roofnet /design />.
3. Ting He, S.-H. Gary Chan, and Chi-Fai Wong, "HomeMesh: A Low-Cost Indoor Wireless Mesh for Home Networking", IEEE Communications Magazine, December 2008
4. Emad Shihab, Lin Cai, Fengdan Wan, and Aaron Gulliver, "Wireless Mesh Networks for In-Home IPTV Distribution", IEEE Transaction on Network, January/February 2008.
5. Roberto Riggio, Daniele Miorandi, and Imrich Chlamtac, "Hardware and Software Solutions for Wireless Mesh Network Test beds", IEEE Communications Magazine, June 2008
6. Najah A. Abu Ali, Abd-Elhamid M. Taha, Hossam S. Hassanein, and Hussein T. Mouftah "IEEE 802.16 Mesh Schedulers:Issues and Design Challenges", IEEE Transaction on Network, January/February 2008
7. Schoonderwoerd R., Holland O., Bruten J., 'Ant like agents for load balancing in telecommunication networks', In proceedings of the first int. conf. on autonomous agents, pp209-216, New York, ACM Press 1997
8. Haibin Duan, Xiufen Yu, "Hybrid Ant Colony Optimization Using Memetic Algorithm for Traveling Salesman Problem", Proceedings of the IEEE Symposium on Approximate Dynamic Programming and Reinforcement Learning, P92-95, 2007
9. Subramanian D., Druschel P., and Chen J., 'Ants and reinforcement learning: A case study in routing in dynamic networks', In proceedings of the 15th int. joint conf. on artificial intelligence, pp823-838, San Francisco, Morgan Kaufmann, 1997
10. Kwang Mong Sim and Weng Hong Sun, "Ant Colony Optimization for Routing and Load-Balancing: Survey and New Directions", IEEE Transactions on Systems, Man, and Cybernetics, VOL. 33, NO. 5, P560-572, 2003
11. Manuel Lopez-Ibanez, Christian Blum, "Beam ACO for the traveling sales man problem with time windows", Computers & Operations Research 37 (2010) 1570–1583
12. Hemanth Chakravarthy, M. and E. Kannan 2014. "A review on secured cloud computing environment". J. Comput. Sci., 11 (8): 1224-1228.
13. Hemanth Chakravarthy, M. and E. Kannan 2014. "Hybrid Elliptic Curve Cryptography For Secured Cloud" International Journal of Applied Engineering Research Volume 9, Number 24,pp. 29329-29337.
14. Hemanth Chakravarthy, M. and E. Kannan "Ant colony-based authentication system for cloud computing "Research Journal of Applied Sciences, Engineering and Technology, 11(2): 144-149,2015
15. Hemanth Chakravarthy, M. and E. Kannan "Hybrid elliptic curve cryptography using ant colony-based authentication system for cloud computing" Journal of Engineering and applied Sciences Vol 10, No. 16, pp 7273-7279, 2015.

AUTHORS PROFILE

Dr.M.Hemanth Chakravarthy,,currently working as Application Development Lead in Accenture Services. He obtained his M.E (Software Engineering) from GIET, Rajahmundry (JNTU, Kakinada). He Completed his Ph.D in the Department of Computer Science and Engineering at Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Chennai-62, Tamilnadu, India. He has been in Software Industry for the past 10 years and has expertise in Salesforce, Software Testing and Java. He has primarily worked in Sales, Services and Marketing Clouds and has expertise in Roles, Profiles, Hierarchies, Workflows, Rules and Validations along with Chatter and Triggers. He has also Extensively worked on integration systems with legacy applications to SFDC His area of research is Cloud Computing. He has published 5 research articles in International Journals and 2 papers presented in international Conferences. He has attended various Training Programmes, Workshops and FDPs related to his area of interest.

Dr. Pethuru Raj, has been working as the chief architect in the Site Reliability Engineering (SRE) Center of Excellence, Reliance Infocomm Ltd. (RIL), Bangalore. He previously worked as a cloud infrastructure architect in the IBM Global Cloud Center of Excellence (CoE), IBM India Bangalore for four years. Prior to that, He had a long stint as TOGAF-certified enterprise architecture (EA) consultant in Wipro Consulting Services (WCS) Division. He also worked as a lead architect in the corporate research (CR) division of Robert Bosch, Bangalore. In total, He have gained more than 17 years of IT industry experience and 8 years of research experience. He obtained his PhD through CSIR-sponsored PhD degree in Anna University, Chennai and continued the UGC-sponsored postdoctoral research in the department of Computer Science and Automation, Indian Institute of Science, Bangalore. Thereafter, He was granted a couple of international research fellowships (JSPS and JST) to work as a research scientist for 3.5 years in two leading Japanese universities. Regarding the publications, He have published more than 30 research papers in peer-reviewed journals such as IEEE, ACM, Springer-Verlag, Inderscience, etc. He have authored 7 books thus far and He focus on some of the emerging technologies such as IoT, Cognitive Analytics, Blockchain, Digital Twin, Docker-enabled Containerization, Data Science, Microservices Architecture, etc. He have contributed 25 book chapters thus far for various technology books edited by highly acclaimed and accomplished professors and professionals. The CRC Press, USA had also released his first book titled as "Cloud Enterprise Architecture" in the year 2012 and you can find the book details in the page http://www.crcpress.com/product/isbn/9781466502321 He has edited and authored a book on the title" Cloud Infrastructures for Big Data Analytics" published by IGI International USA in March 2014. A new book on the title" Smarter Cities: the Enabling Technologies and Tools" by CRC Press, USA, is to hit the market in the month of June 2015. He has collaborating with a few authors to publish a book on the title "High-Performance Big Data Analytics" to be published by Springer-Verlag in the year 2015.

Dr. A. Suresh B.E., M.Tech., Ph.D works as the Professor & Head, Department of the Computer Science and Engineering in Nehru Institute of Engineering & Technology, Coimbatore, Tamil Nadu, India. He has been nearly two decades of experience in teaching and his areas of specializations are Data Mining, Artificial Intelligence, Image Processing, Multimedia and System Software. He has one patent. He has published 75 papers in International journals. He has published more than 40 papers in National and International Conferences. He has served as a reviewer for Springer, Elsevier, and Inderscience journals. He is a member of ISTE, IACSIT, IAENG, MCSTA, MCSI, and Global Member of Internet Society (ISOC). He has organized several National

Workshop, Conferences and Technical Events. He is regularly invited to deliver lectures in various programmes for imparting skills in research methodology to students and research scholars. He has published three books, in the name of Data structures & Algorithms, Computer Programming and Problem Solving and **Python** Programming in DD Publications, Excel Publications and Sri Maruthi Publisher, Chennai, respectively.

Dr. E. A. Neeba, currently working as an Assistant Professor in the Department of Information Technology at Rajagiri School of Engineering & Technology, Kochi, Kerala, which is affiliated to the A.P.J Abdul Kalam Technological University, Kerala. She received her doctoral degree from Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Chennai, Tamil Nadu. She completed her Masters in Computer Science & Engineering from SRM Institute of Science and Technology, Chennai. Her research interests include Analysis of data, Data Mining and Big Data, knowledge representation, and ontology, both from the theoretical perspective and their application to natural language understanding, reasoning, information visualization, and interoperability. Having a rich industrial experience of around 10 years prior to joining academia, and also she has publications in around 10 SCI/ SCIE/Scopus indexed international journals and a few national journals. An active participant in various conferences and workshops on data mining, she is currently involved in several projects in this field. She was entrusted with leadership positions such as the Accreditation coordinator for the college, and Head of the Quality Cell, besides organizing various national and international events.

Dr. S. Sasikala, currently working as a Professor in Department of Computer Science and Engineering, Paavai Engineering College, Namakkal, TamilNadu, India. She received doctorate in faculty of Information and Communication Engineering from Anna University India, 2016. She has published more than 18 Journal and Conference papers in the area of Data mining and Big Data Analytics with Elsevier Science Direct, Springer and IEEE publishers. She has published two International Scientific books in KDD and Data mining and Data warehousing. She is serving as an Editorial Board Member and Reviewer for many reputed journals like IEEE, ELSEVIER and SPRINGER. She has 16+ years experience in teaching and Research. Prior to joining Paavai Engineering College, she served at K.L.N.College of Information Technology Madurai, Velammal College of Engineering and Technology Madurai, P.S.N.A Engineering college Dindigul and Sethu Institute of technology Madurai. Her research interests include Data Mining, Internet of Things, Machine Learning Paradigms and Optimizations.