A Secure and Efficient Multi Authority Encryption Scheme in Cross Domain Data Sharing

L. Godlin Atlas, Arjun K.P., Sreenarayanan N.M., N. Thillaiarasu

Abstract*: Attribute Based Encryption (ABE) in light of the fact that the rule locals to make sure about the patient data set aside on a semi-trusted. In ABE plot, each patient is regularly recognized by name which fuses the patient attributes. At the reason when Patient re-proper the delicate data for sharing on cloud system on cloud structures. Taking care of the patient records on suspicious limit makes secure transfer of data to be a test issue. To remain tricky customer data mystery against suspicious cloud structure. the current system when in doubt apply cryptographic techniques by revealing data unscrambling keys just to affirmed customer. the basic troubles for cryptographic technique fuse at a proportional time achieving structure flexibility and fine-grained data get the opportunity to manage, gainful key or customer the load up, data security, computational overhead then forward. To manage these issues, promptly applied and maintaining access approaches snared in to attributes and sanctioning the information owner to designate most count genuine assignments to customer disavowal to untrusted server without uncovering data substance to around then. We achieve this target by introducing multi authority characteristic based encryption. Our proposed plot in like manner has momentous features of customer get the chance to benefit characterization, dynamic modification of access game plans or archive properties and customer puzzle key duty, supports capable on-demand customer or trademark denial and break-glass access under emergency circumstances.

Keywords: Cloud processing, Personal wellbeing records, information security, fine-grained get to control, characteristic based encryption, numerous authority ABE, client repudiation, untrusted capacity.

I. INTRODUCTION

Disseminated figuring, the since very while back held dream about preparing as an utility, can change a tremendous bit of the IT business, making programming a lot of progressively appealing as a help and shaping the route during which IT gear is arranged and made. Late approaches in IT have unimaginably energized inaccessible data accumulating and sharing. Advanced applications, for instance, online casual networks and online records give incredibly worthwhile ways to deal with persons to store and offer distinctive data including singular contour, electronic reports then beyond online servers. Conveyed figuring, saw in light of the fact that the more extended term IT designing, and even pledges to supply limitless and flexible limit resource (and other handling resources) as a help of cloud customers during an actually monetarily smart way [3]. But still at its starting period, Cloud Computing has quite recently drawn uncommon thought, and its preferences have pulled in an extending number of customers to redistribute their local server homesteads to cloud servers.

Data security could likewise be a fundamental problem for inaccessible data accumulating. On another hand, presentation of conscious data, for instance, prosperity records, set aside on inaccessible data servers must be deliberately guaranteed before customers have opportunity to use the information organizations. Fine-grained data get the chance to oversee segments often ought to be recognized to ensure appropriate presentation of unstable data among various customers. yet, in remote data accumulating customers don't really have their data. Conscious data pro associations are essentially certain to be outside the customers' trust region, and are not allowed to comprehend capability with customers' sensitive information set aside on their servers. Things being what they're, customers can't rely upon remote data servers to approve get the opportunity to oversee courses of action like customary access control [2] during which reference screens got the chance to be totally trusted. Customer executed data get the opportunity to oversee is during this way significantly needed for remote data accumulating. Even more for the principal part, such a drag also exists in any untrusted amassing, e.g., scattered data storing in Wireless Sensor Networks (WSNs), that accumulating devices that are either guaranteed by deceptive provider(s) or significantly weak against memory break attacks, These stresses start from the way that cloud servers are ordinarily worked by business providers which are probably going to be outside of the trusted in zone of the customers. In untrusted limit data servers aren't allowed to encourage acquainted with the substance of fragile data, nor would they have the option to be trusted to maintain data get to courses of action. to remain data mystery to data servers the information owner encodes data before move.

Revised Manuscript Received on April 25, 2020.
* Correspondence Author

L.Godlin Atlas*, SCSE, Galgotias University, Greater Noida, India. Email: godlin88@gmail.com

Arjun. K.P, SCSE, Galgotias University, Greater Noida, India. Email: arjunkppc@gmail.com

Sreenarayanan N.M., SCSE, Galgotias University, Greater Noida, India. Email: sree.narayanan1@gmail.com

N.Thillai Arasu., SCSE, Galgotias University, Greater Noida, India. Email: thillai888@gmail.com

Retrieval Number: D8439049420/2020©BEIESP
DOI: 10.35940/ijeat.D8439.049420
Journal Website: www.ijeat.org

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication
© Copyright: All rights reserved.

Customers get to is yielded by having the information unscrambling key(s) under the MA-ABE plot. Multi Authority Attribute Based Encryption is open key cryptography for one-to-various correspondences. It allows the sender to make sense of for each force k a lot of qualities saw by that position and assortment dk(decryption key) with the objective that the message are frequently unscrambled remarkably by a customer who has at any rate dk of the given properties from each position. At the point when this kind of property-based access control plot give security protection on data. Customer can confer their data on cloud to security using multi authority characteristic based encryption.

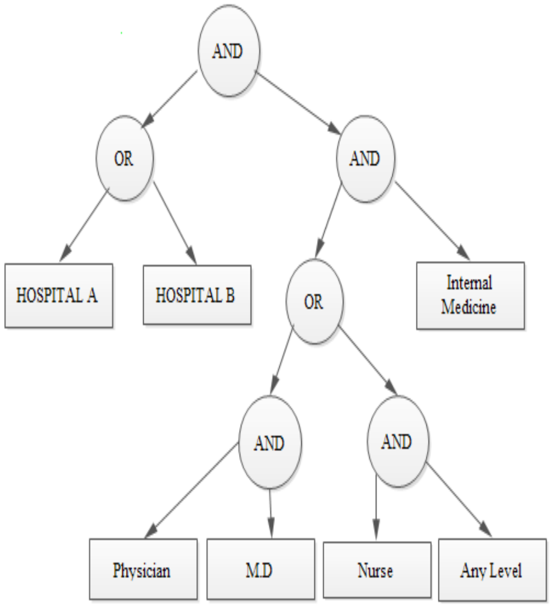


Fig.1. PHR Framework

II. RELATED WORKS

In Role Based Access Control (RBAC) system each customer get to rights are settled excited to his/her occupations. Take an instance of crisis center, its numerous noteworthy occupations, for 1111111111111instance, master, agent, tireless etc. This procedure licenses authority to decide the entire experiences with respect to the patient regardless, it doesn't allow laborers to decide the entire bits of knowledge concerning the patient. For delegate sensitive information is concealed. In RBAC calm records are taken care of on various regions. To beat this, Patient Controlled Encryption (PCE) is introduced. It allows the patient to explicitly share their records among pros and restorative administrations providers. Here, constant is totally capable of sharing and key age. Subsequently, security setback is occurred. Different leveled Identity Based Encryption (HIBE) is used to disengage the information from novel data which contain complex information. HIBE grants the length of the figure substance to be restricted and permits the creation of escrow spread that limit the degree of the key escrow. The flexibility of the structures are cultivated a new encryption algorithm which is unrefined for one-to-various trades. In the new encryption scheme, data are linked to characteristics for a public key fragment is described. The encode or accomplices the course of action of the message by moving by looking at open key portions. Each customer is dispensed a passageway ordinarily described as a passage tree over data characteristics, which means center points of the entryway nodes are limit entryways and nodes are connected with quality. Client secret keys described to reflect the entryway structure in this way the customer can translate a figure content if and just if the information attributes satisfy his passageway structure. For fine grained get the chance to oversee the new encryption techniques are used. In CP-ABE private keys are set apart with a lot of characteristics and subsequently the ciphertext are connected with get to structures that control which customer can interpret the ciphertext. Additionally, CP-ABE is impenetrable to game plan attacks from unapproved customers. of those wonderful effects which does encryption incredibly sensible for compactable data get the opportunity to oversee on untrusted limit.

III. EXISTING SYSTEM

In the present system, the technique uses revocable ABE estimation. For each patient, the Patient Health Records (PHR) data got the chance to be mixed so it's versatile with the measure of customers drawing nearer. Also, since there are various owners (calm) during a PHR structure and every owner would scramble his/her PHR records using a substitute course of action of cryptographic key, it's fundamental to downsize the key dissemination complexity in such multi-owner settings. Existing cryptographic approved access control plans are for the principal part proposed for the single-owner circumstances. By using this methodology mixed data are regularly kept private whether or not the cut-off point is in server. Past Encryption structures are pre owned credits to depict the encoded messages consolidated systems with customer's keys; while promptly are used to delineate a customer's affirmations, and a social affair scrambling data chooses a path for who can decipher. Subsequently this procedure is hypothetically closer to standard access control methodologies, for instance, Access control-based method encryption. This will, just acknowledge the setup in which encrypted texts are connected with other sets, while customer riddle values are connected with various attributes. These systems that adopt into thought complicated strategies will have different applications.

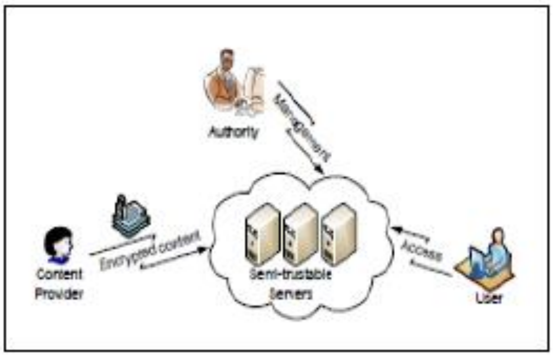


Fig. 2. Scenario of Data Sharing

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

A significant model could likewise be a very modern Broadcast Encryption, where clients are portrayed by (and hence connected with) different properties. At that point, one could make a ciphertext which can be opened as long in light of the fact that the qualities of a client coordinate an arrangement. For example, during an army setting, people will communicate a message which is intended to be perused uniquely by clients who are having the higher position.

IV. PROPOSED SYSTEM

A. Information Sharing with Domain Separation

Industrious Health Records (PHR) is taken care of at outcast servers, for instance, cloud provider. With the objective that initially makes accepted server then it masterminded into two regions, one for open space and another for singular space. The two zones are confined by the customer data get to necessities. The different use of these zones for security and key organization.

B. Fine grained get to control versus versatility

Disclosure of sensitive data for the premier part requires fine-grained get the opportunity to oversee as in different customers may move toward advantages to shifted sorts/sets of information. Regardless, Current approach and capacity control, to be approved with security strategies, has the versatility issue. There are a couple of progressing work [4-5], inside the field of cryptography and security and control over redistributed data keeping an eye on the practically identical issue of information get the chance to deal with cryptographic keys. At the point when these plans are sensible for ordinary record structures, most of them are not suitable for impenetrable data get the chance to oversee in gigantic extension server ranches which may have an immense number of customers and information reports. Characteristic based encryption (ABE) [6-8], an as of late composed one to-various open key cryptography, can maintain the fine-grained get to approaches for immense extension structures.

C. Client elements

A convincing and gainful customer the board segment got the opportunity to be recognized to oversee customer get the chance to benefit grant and forswearing. Existing plans [6-9], prescribe accomplice end time attributes to customer puzzle keys. At the point when these sorts of courses of action can revoke customer puzzle keys at the appointed time. Be that since it's going to, it's more proper for steady correspondence than data/record amassing.

D. Protection safeguarding

As the data amassing servers can't be accepted; it's appealing to uncover as less customer security information as possible to servers wish to remain her passageway plan information mystery to servers and customers may separate from data protection. In particular, the information owner would have stresses on divulging their passage advantage information to servers.

1. Client gets to benefit classification

This system just reveals the leaf center point information of a customer get the opportunity to tree to Cloud Servers. As inside centers of a passageway tree are frequently any edge entryways and are not suitable to cloud based servers, it's difficult for Cloud based Servers to recover the entryway setup and through along these lines deduce customer get the chance to benefit information.

2. Area Separation

After produce accepted server territories are orchestrated into two, for instance, open space and individual region. The two spaces are confined by the customer data get to necessities. The different usage of these spaces for security and key organization.

2.1 Multi Aspect Encryption

Multi Aspect Encryption is open key cryptography for one-to-various exchanges. It allows the sender to point for each force k a lot of characteristics saw by that position and assortment dk (decryption key) with the objective that the message are frequently unscrambled exceptionally by a customer who has at any rate dk of the given attributes from each force.

2.2 Key Policy Encryption

Key Policy Encryption is a public key security measure which is unrefined for one-to-various correlation. In this policy based, data is asserted with effects of all of which a public key fragment is described. The make secure or accomplices the course of action of attributes to the message by move it along with public key.

3. MA-ABE for User Revocation

Mother ABE plan engages compelling and on-demand customer disavowal. In precise an owner can deny a customer or customer's values suddenly by pushing the encoded text and invigorating customers' private keys, while a colossal bit of these undertakings is frequently doled out to the server which improves adequacy. It’s nine computations, where MinimalSet, ReKeyGen, ReEnc and Key Update are related to customer repudiation, and Policy Update is for dealing with dynamic game plan changes.

3.1 Access control Implementation

If no objection to create, other PHR can be used to write by someone using simply open keys that are heartbreaking. Just By surrendering create get to, we mean a data sponsor got the chance to secure suitable endorsement from the affiliation she is in (and furthermore from the focus on owner), which may have the determination to be checked by main place where it can be granted or rejected make get to. The observation is that, it's alluring and right directly rational to endorse as showed by timespans whose granularity are regularly adjusted.

3.2 Holding Policy Changes

Mom ABE plan should reinforce the dynamic incorporate/modify/eradicate of an area of the chronicle get to approaches or data characteristics by the owner. Counting and modification of characteristics/get to courses of action should be conceivable as substitute re-encryption techniques.

3.3 Gaining - Access

In explicit bits of the data, clinical they have to be fleeting access when there is emergency situation happening for the patients,

Retrieval Number: D8439049420/2020©BEIESP
DOI: 10.35940/ijeat.D8439.049420
Journal Website: www.ijeat.org

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

which cannot be neglectful and can't alter the passageway courses of action beforehand. The clinical staffs would require some passing endorsement to decipher that data. In this model, this might be ordinarily cultivated by allowing the patients to give the emergency key to office. Particularly, at the starting each person portrays an "emergency" trademark and joins it with the PSD an area of the encoded text of each report that will be allowed.

V. SECURITY ANALYSIS

This module investigates capability of security arrangement. It accommodates the data that is forestalling unapproved read gets to), by producing the modified Encryption conspire (with effective renouncement) to be safe based on the quality of specific model. This structure additionally accomplishes forward mystery, and security of compose get to control. In option, the proposed system explicitly addresses the entrance necessities in cloud-based wellbeing record the executives frameworks by consistently separating the framework, which has both individual and higher level PHR clients. The denial techniques Encryption in the two sorts of areas are reliable.

A. Information Confidentiality

The improved Encryption plot supports data grouping of the PHR data on unapproved customers and in this way the cloud expert association, by keeping up the understanding resistance against customers.

VI. RESULT AND DISCUSSIONS

A. ROUTING AND PROTOCOL ADAPTATION

Input: Routing Protocol
Output: Finding Route

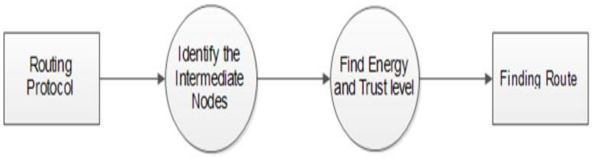


Fig. 3. DFD level 0 for Routing and Protocol Adaptation

Input: Discovered Route
Output: Transfer the data

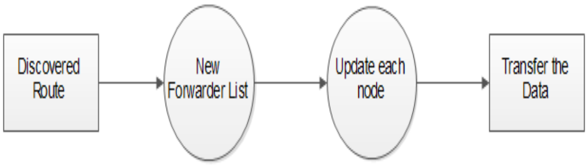
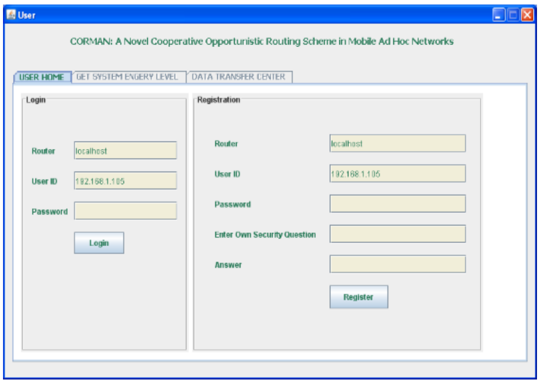


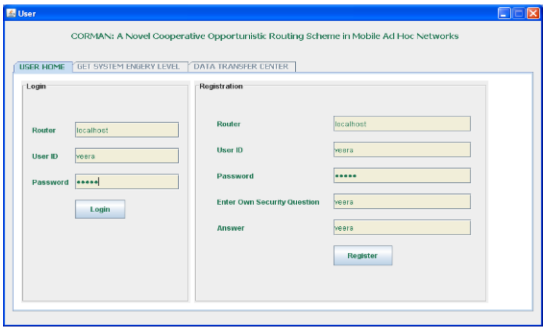
Fig. 4. DFD level 1 for Routing and Protocol Adaptation


User

CORMAN: A Novel Cooperative Opportunistic Routing Scheme in Mobile Ad Hoc Networks

Login
Router: localhost
User ID: 192.168.1.105
Password:

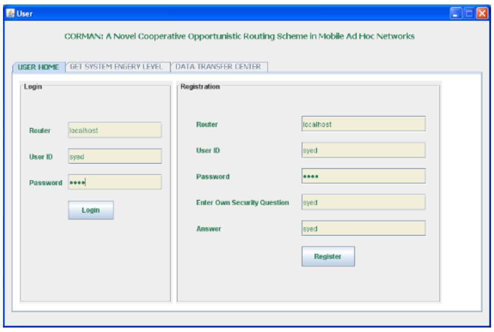
Registration
Router: localhost
User ID: 192.168.1.105
Password:
Enter Own Security Question:
Answer:


User

CORMAN: A Novel Cooperative Opportunistic Routing Scheme in Mobile Ad Hoc Networks

Login
Router: localhost
User ID: veera
Password: •••••

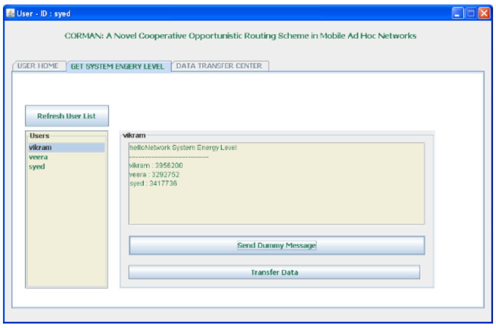
Registration
Router: localhost
User ID: veera
Password: •••••
Enter Own Security Question: veera
Answer: veera


User

CORMAN: A Novel Cooperative Opportunistic Routing Scheme in Mobile Ad Hoc Networks

Login
Router: localhost
User ID: syed
Password: ••••

Registration
Router: localhost
User ID: syed
Password: ••••
Enter Own Security Question: syed
Answer: syed


User - ID : syed

CORMAN: A Novel Cooperative Opportunistic Routing Scheme in Mobile Ad Hoc Networks

vikram

```
helloNetwork System Energy Level
------------------------------------
vikram : 3956200
veera : 3292752
syed : 3417736
```

VII. CONCLUSION

In earlier system, there are various troubles proceed with the patient-driven pattern of prosperity data transfer which is ordinarily redistributed to be taken care of at an untouchable, for instance, cloud providers. These structures have various limitations, for instance, threat of insurance introduction, versatility in key organization, versatile access and capable customer revocation, have remained the first critical threat on getting course-grained, secured data get the opportunity to oversee. To vanquish these issues, an absolutely one of a kind patient-driven structure is proposed.

It secludes the customer's PHR information into various passage zone by creating specific key to the relating space by using the Encryption and Multi Authority Encryption. By using this framework, security and versatility of patient PHR records are depended upon to be achieve during a capable way

REFERENCES

1. M. S. Obaidat P. Nicopolitidis Smart Cities and Homes: Key Enabling Technologies Morgan Kaufmann May 2016.
2. "Technology and Computing Requirements for Self-Driving Cars" in Intel 2016 [online] Available: http://Ies-svc.org/wp-content/uploads/2015/06/pp.2016-05-18-lntel-automotive-au-tonomous-driving-vision-paperpdf.
3. K. Zaidi et al. "Host-Based Intrusion Detection for VANETs: A Statistical Approach to Rogue Node Detection" IEEE Trans. Vehic. Tech. vol. 65 no. 8 pp. 6703-6714 2016.
4. T. Bouali S.-M. Senouci H. Sedjelmaci "A Distributed Detection and Prevention Scheme from Malicious Nodes in Vehicular Networks" Int'l. J. Commun. Systems vol. 29 no. 10 pp. 1683-1704 2016.
5. X. Hou et al. "Vehicular Fog Computing: A Viewpoint of Vehicles as the Infrastructures" IEEE Trans. Vehic. r Tech. vol. 65 no. 6 pp. 3860-73 2016.
6. K. Kaur et al. "Edge Computing in the Industrial Internet of Things Environment: Software-Defined-Networks-Based Edge-Cloud Interplay" IEEE Commun. Mag. vol. 56 no. 2 pp. 44-51 Feb. 2018.
7. S. Garg et al. "UAVEmpowered Edge Computing Environment for Cyber-Threat Detection in Smart Vehicles" IEEE Network vol. 32 no. 3 pp. 42-51 May/June 2018.
8. M. M. Mehdi I. Raza S. A. Hussain "A Game Theory Based Trust Model for Vehicular Ad hoc Networks (VANETs)" Computer Networks vol. 121 pp. 152-72 2017.
9. 9. H. Sedjelmaci S. M. Senouci M. A. Abu-Rgheff "An Efficient and Lightweight Intrusion Detection Mechanism for Service-Oriented Vehicular Networks" IEEE Internet of Things J. vol. 1 no. 6 pp. 570-77 2014.
10. M. Sookhak F. R. Yu H. Tang "Secure Data Sharing for Vehicular Ad-hoc Networks Using Cloud Computing" in Ad Hoc Networks Springer pp. 306-15 2017.
11. IBM X-Force Threat Intelligence IBM Security Mar. 2016 [online] Available: http://www.foerderland.de/fileadmin/pdf/IBMXForceReport2016.pdf.
12. S. Dutta A. Narang S. K. Bera "Streaming Quotient Filter: A Near Optimal Approximate Duplicate Detection Approach for Data Streams" Proc. VLDB Endowment vol. 6 no. 8 pp. 589-600 2013.
13. M. Al-hisnawi M. Ahmadi "Deep Packet Inspection Using Quotient Filter" IEEE Commun. Letters vol. 20 no. 11 pp. 2217-20 2016.
14. R. Yu et al. "Optimal Resource Sharing in 5G-Enabled Vehicular Networks: A Matrix Game Approach" IEEE Trans. Vehic. Tech. vol. 65 no. 10 pp. 7844-56 2016.
15. A. Singh et al. "Probabilistic Data-Structure-Based Community Detection and Storage Scheme in Online Social Networks" Future Ceneration Computer Systems vol. 94 pp. 173-84 2019.
16. N. Chand P. Mishra C. R. Krishna E. S. Pilli M. C. Govil "A comparative analysis of SVM and its stacking with other classification algorithm for intrusion detection" Proc. Int. Conf. Adv. Comput. Commun. Autom. (ICACCA) (Spring) pp. 1-6 Apr. 2016.
17. Dr. L. Godlin Atlas, D. D. M. M. V. (2019). Performance Comparison of Geographic Routing in WSN for measuring Coverage Constraints and Energy Consumption in Cloud Environments. International Journal of Advanced Science and Technology, 28(16), 1594
18. S. Otoum B. Kantarci H. T. Mouftah "Adaptively supervised and intrusion-aware data aggregation for wireless sensor clusters in critical infrastructures" Proc. IEEE Int. Conf. Commun. (ICC) pp. 1-6 May 2018

AUTHORS PROFILE

Dr. L. Godlin Atlas has got more than eight years of academic experience in various institutions and currently working as Assistant Professor in the School of Computing Science and Engineering, Galgotias University, Greater Noida, Uttar Pradesh, India. He received his Doctorate Degree in Computer Science and Engineering from MS University, Thirunelveli 2018. He has completed his B.Tech, Information Technology from CSI Institute of Technology and M.E. from The Indian Engineering College, Nagercoil. He has authored over 10+ research papers in various national and international journals and conferences. His publications are indexed in SCI, Scopus, Web of Science and Google scholar. He is member of Professional bodies like Indian Society for Technical Education. His research interests includes Medical Image Processing, Big Data analytics, Cloud Computing, Artificial Intelligence, Machine Learning and Deep Learning.

Arjun K P is currently working as Assistant Professor in the School of Computer Science and Engineering, Galgotias University, Greater Noida, Uttar Pradesh, India. He received M.Tech degree in Computer Science and Engineering from University of Calicut, Kerala in 2016 and B.Tech degree in Computer Science and Engineering from University of Calicut, Kerala in 2014. His research interests are Big Data Analytics, Cloud Computing, Artificial Intelligence, Machine Learning and Deep Learning. He has authored over 5+ research papers in various national and international journals and conferences. His publications are indexed in SCI, Scopus, Web of Science and Google scholar.

Sreenarayanan N M is currently working as Assistant Professor in the School of Computer Science and Engineering, Galgotias University, Greater Noida, Uttar Pradesh, India. He received M.Tech degree in Computer Science and Engineering from University of Calicut, Kerala in 2016 and B.Tech degree in Computer Science and Engineering from University of Calicut, Kerala in 2014. His research interests are Artificial Intelligence, Machine Learning, Neural Networks and Deep Learning. He has authored over 5+ research papers in various national and international journals and conferences. His publications are indexed in SCI, Scopus, Web of Science, DBLP and Google scholar.

Dr. N. Thillaiarasu has 8 years of teaching experience, obtained his B.E., in Computer Science and Engineering from Selvam College of Technology in 2010 and received his M.E., in Software Engineering from Anna University Regional Center, Coimbatore in 2012. He received his Ph.D., Degree from Anna University, Chennai in 2019, He worked 7 Years has an Assistant Professor in the Department of Computer Science and Engineering, SNS College of Engineering, Coimbatore. Currently, he is the Assistant Professor of School of Computing Science & Engineering, Galgotias University, Greater Noida. His area of interest includes Cloud Computing and Web Services.