Augmentation and Orchestration of Security Techniques in Fog Computing

G.Usha , S.Kannimuthu, Vinoth N A S, H.Karthikeyan

Abstract*: *The inventions in the field of Cloud computing with mobile devices, cloudlets, Edge computing are sizzling growth of IoT(Internet of Things) devices. The cloud computing technology has its limitation in various attributes such as bandwidth, latency, location awareness, resource constraints etc. In order to overcome these issues, the edge computing, which is known as manipulating the data at the edge of the network. In order to support various integrated features with IoT such as storage, networking, home energy management, augment reality fog computing provides resource access to the network edge of the user. In the user side it is confronted with serious security issues for data security. This article provides the augmentation and orchestration of security issues in fog computing. In this paper, first we check the architecture of fog computing. Then we suggest broad taxonomy of fog architecture with various architectures. Finally, this paper is concluded with scope and future research in fog computing.

IndexTerms*:*Fogarchitecture,Access,control,cryptographyAuthentication.

I. INTRODUCTION

The real time environment information's are identified by enabling them with sensors with large number of intelligent devices. However, this scenario is changed in such a way that the intelligent thigs such as laptops, sensors, smart cars, and smart homes are connected through network of network in order to perform data analysis. Hence, IoT devices play an explosive growth with huge volume of data from physical world. In 2020, 500 Zettabytes (ZB) of data will exceed in IOT devices. Hence such situation move towards to the period of Internet of Everything (IoE). Managing the physical objects in the IoT network that are connected with various devices and keeping the data securely is an important issue in IoT.

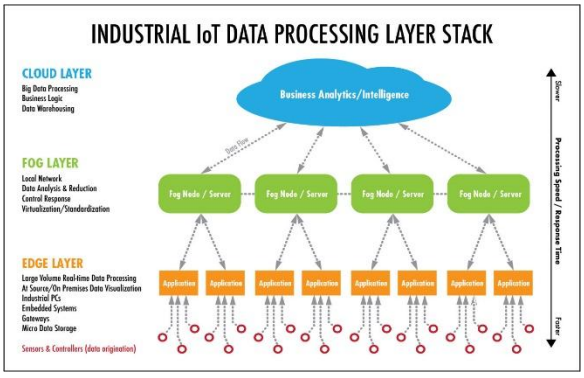

Fig 1 Layered architecture of Fog Computing

Revised Manuscript Received on July 05, 2019.

Dr.G.Usha ,
Dr.S.Kannimuthu,
Mr.Vinoth N A S ,
Mr.H.Karthikeyan,

The above Fig 1 explains the three layered architecture for Industrial IoT data processing layer stack. The Cloud layer includes the Big data processing, Business logic, data ware housing. The Fog layer [1][10]consists of processing data's in local network, data analysis and reduction, control response, visualization/standardization. The edge layer consists of Large volume of real time data processing. For example embedded systems, gateways micro data storage devices are example of edge devices. In real fog computing and edge computing techniques are related. Both the techniques involve bringing intellect and handling of data which are closer to construction of data. The question arise is why cloud computing network itself is not enough to process data. The answer is in real time various physical constraints are exist such as energy, space etc. In cloud, Fog computing platform required by various application, such applications that require very low and predictable latency, geo-distributed applications such as pipeline monitoring, fast mobile applications such as smart connected vehicles, rail communications, and large scale distributed control systems such as smart grid. Fog computing brings big data with a twist in the field of data sources distributed geographically.

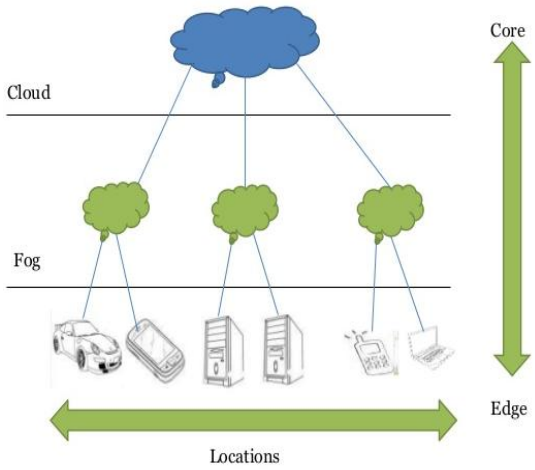

Fig 2. Relationship between cloud, Fog and Edge devices

The Fig 2 depicts three level three level hierarchy of Fog devices. In Fig 2, in order to attain inter layer and cross layer communications various techniques are applied to unite with each entity, wireless communications and various wired communications. Each layer is accessible and flexible to enhance the services to various entities based on the demand. Cloud Computing is[11][12] involved in various areas of Computer networking. Cloud computing based IoT applications deliver diverse services in heterogeneous collection of IoT infrastructure based devices. The data's which are collected from IoT devices are stored in

cloud data center. The base layer i.e, the edge layer consists of mobile IoT devices and static IoT devices. The devices [13][14]belonging to similar proprietor form group to communicate each other using adhoc networks. The IoT devices are pre deployed in specific area to fulfil the tasks predefined.

Fog Computing frame work spreads cloud computing to the advantage of the network. Fog computing offers data, application services to end-users. In various real time applications such as smart grid, vehicular networks, software defined networks the objective of Fog architecture is used. Fog computing is initially visioned by CISCO to run directly on the edge of the network. All network operating systems are together framed as a single networked device by single networked device. Unlike traditional Cloud data Centers Fog devices are geographically distributed over various heterogeneous platforms. Even though cloud computing frees the enterprises, but various latency sensitive applications have physical constrains such as energy, space to access the data. For example, smart traffic light[15-22] systems which are equipped with sensors need to measure the speed and distance of vehicles from all the directions, need to detect presence of pedestrians and the vehicles crossing the street. Smart traffic light has goals such as accident prevention, steady flow of traffic, collecting and improving the system.

II. AUGMENTATION AND ORCHESTRATION OF FOG COMPUTING

A. Block Chain Technique

Fig 3 depicts the proposed orchestration of fog computing methodology In order to enhance security in existing cloud architecture they proposed technique that consists of four steps which are shown in Fig 4. Initially, cloud users selected the cloud service provider. After the service has been selected, the cloud users are given services such as task execution, data management for users. Once the registration has been over, the service provider accesses the transaction in the form of block chain. The user supplies the reward for the provider. The different services are made available to different resource. Hence the proposed technique is fully transparent.

B. Content Aware Security Technique

Content aware security technique consists of content classification based on various criteria's. Fig 5 describes the hierarchy of content classification technique. Content matching is done by transferring related conditions. The backward distance is calculated by computing current possible distance. According to Open fog community, the fog networks can have any attractive computing functions with features. Fog networks can support horizontal structure, continuous cloud to terminal service and system level. In this work, the authors proposed horizontal structure. The security [23-31]of the information content is given by managing directly the objects. Hence, sender and receiver do not tamper the messages. Additionally they used classification labels and verified that the labels are not tampered between sender and receiver. The filtering scheme is used in fog computing. The filtering technique involves content matching and applying filters for security services. The services are classified by based on the glossaries. The glossaries consists of violence, sexual descriptions and secrets of states. In fog, the application layer information are considered based on the header of the protocol. Hence, the protocol files consists of classification labels, which are delivered via the communication technique. Two types of modes are used for content classification using filters.

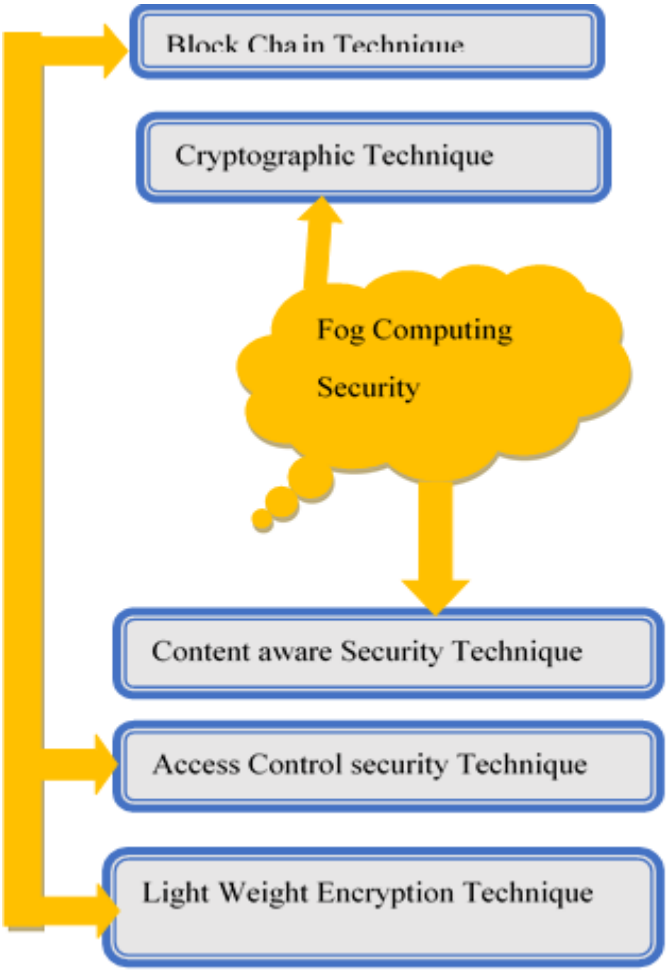

Fig 3. Orchestration of Fog computing Security

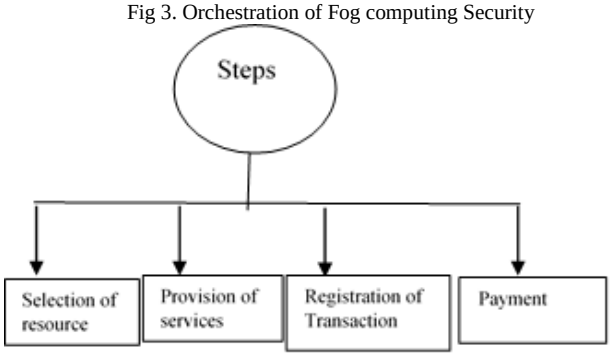

Fig 4. Steps in Block Chain Technique

The Middle ware fog mode consists of filtering canter and supervision center. The supervision center consists of random information, which passes the information to the users for human inspection. The client fog software mode uses the classification labels that are provided by criterion center. Finally, they evaluated the performance with various parameters such as end-to-end communication delay, hit ratio, accuracy, filtering accuracy.

The authors proposed fog computing based content aware filtering method that provides security services, which are used in information-centric social networks. The proposed Information-Centric Social Networks(IC-SN) improves significant security in fog networks.

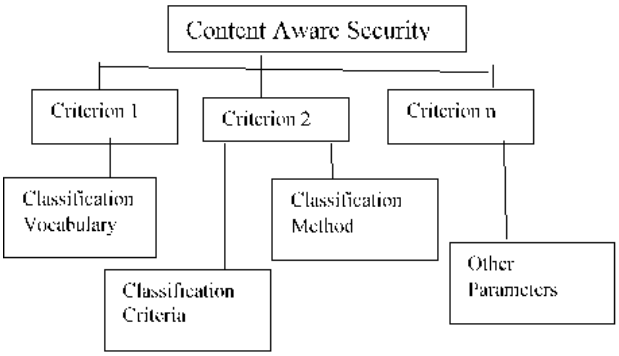

Fig 5. Content Classification Method

Figure 6 explains types of modes presented in the proposed technique.

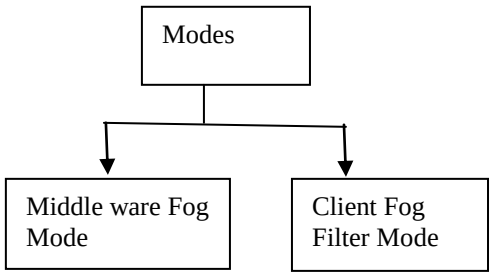

Fig 6. Modes in content aware security technique

The Middle ware fog mode consists of filtering canter and supervision center. The supervision center consists of random information, which passes the information to the users for human inspection. The client fog software mode uses the classification labels that are provided by criterion center. Finally, they evaluated the performance with various parameters such as end-to-end communication delay, hit ratio, accuracy, filtering accuracy. The authors proposed fog computing based content aware filtering method that provides security services, which are used in information-centric social networks. The proposed Information-Centric Social Networks(IC-SN) improves significant security in fog networks.

C. Data and Cryptographic based Security Technique

In this technique, the trusted node is assumed as coordinator or trusted authority. Fig 7 depicts the steps in detail.

List of procedures followed in this technique.

- Generation of Key
- Encryption(Client)
- Reencryption(Fog)
- Decryption(Fog)
- Decryption(Client)

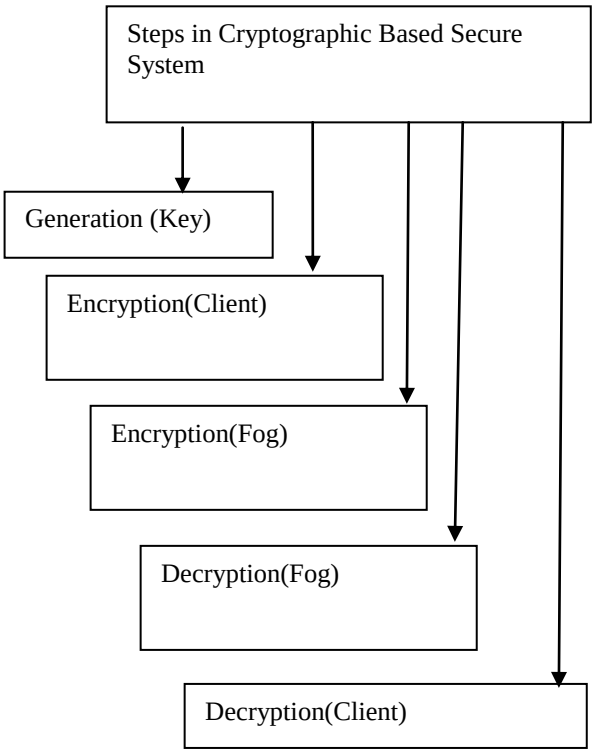

Fig 7.Cryptographic based Encryption and Decryption

In key generation Public Elliptic curve parameters and a secret master key is considered with fog node. In client encryption, technique the cipher text is generated by considering the random parameters with private key. In Fog, re-encryption procedure the cipher text is computed by using elliptic curve parameters. Next in Fog, decryption technique the intermediate cipher is computed by using client key. Finally, the client decryption[32-42] technique gets the intermediate cipher from the private key and original message is obtained. They compared their technique with RSA technique. They used various types of parameters to evaluate their proposed technique such as security level in the terms of bits with execution time in milli seconds and with various types of data sized in bytes. Finally, they proved that their proposed technique performs better than existing RSA technique.

D. Data and Privacy in Fog Technique

W Data and Privacy[43-46] of any network consist of various types of factors such as confidentiality, integrity, security in data search, authentication, authorization, access control, privacy-preserving etc. Various work has been carried out in literature to provide data and privacy of edge devices. Data confidentiality is done by considering encryption techniques such as attribute Based Encryption, homomorphic encryption and proxy re-encryption. The integrity of the data is considered by using various functional aspects such as batch, dynamic, privacy-preserving and low difficulty. Searching data securely by applying the concepts of various

encryption techniques. Various types of searching techniques are available such as dynamic search, dynamic updating,

proxy re- encryption. These techniques are provided to improve the security of data. Authentication is very important factor to trust domains in order to communicate with multiple functional services and infrastructures. External and internal adversaries are need to access sensitive information with legitimate access. Each edge an fog domain should be authenticated and trust validated.

Access control provides proper authentication technique where the non-legitimate users can abuse the service resources. Hence, it becomes the most important security problem. The traditional security mechanisms, which provides access control, are addressed to provide single security. But the fog computing technology needs

distributed access control and access policies. Hence various types of cryptographic created solutions such as attribute created encryption, TPM founded access controls are used in edge computing. Privacy preserving is the most important security component in securing networks. One's private info such as data, location, identity leakages may lead to very serious condition..

Various types of security solutions are provided to secure data and privacy of users. In identity based encryption, the sender and receiver communicate securely by verifying the signatures without exchanging the private or public key. Thus the identity based encryption technique utilizes the services with possession key directories and without using the services of third party. This technique involves three main phases. They are Encryption, Identity authentication and decryption. The Attribute based encryption technique implements the concept of controlling the capacity of the decrypted data owner in the encrypted data. In this method it consists of two entities, they are Trusted Authority (TA) and the user.

E. Access control in Fog Technique

Access control policy[47-51] in fog computing is known as if the user needs to access some devices in order to do storage and computational services it should be properly authorized by data and services. Both the cloud and Fog environment need to be reciprocally need access control policies. Side channel attacks should be avoided to control virtual machines (VMs). Latency is one of the most important characteristics of fog computing where a reasonable response time must be granted for applications. Various types of model are proposed in literature to provide access control. The following fig 8 explains the classification of various types of access control model in detail.

In DAC model based on user id's the data owner gives permission to other users in the group. But this model is very flexible and less secure This model results to overhead for various applications in fog computing with multiple users. In Mandatory Access Control technique based on resource-user mapping the resources are distributed. The multi-layer security system is applied where each object is mapped to each subject based on key rules. In role based access control model, this technique is more scalable to use in fog/cloud environment

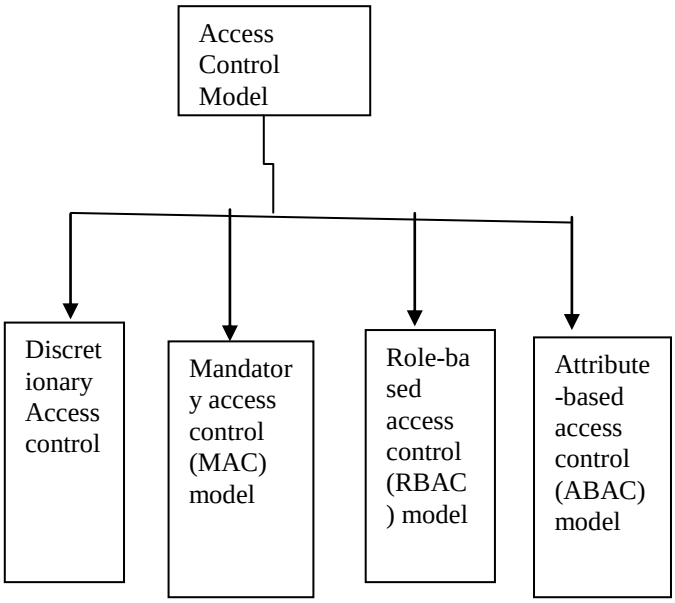

Fig 8: Types of Access control model

III. CONCLUSION

In this paper we surveyed various types of fog computing orchestration and augmentation techniques in detail. This paper suggests a wide survey in various aspects of security issues and solution for fog computing. Fog computing has its own advantages such as it reduces latency of applications. Fog computing methodology can be deployed in mobile and vehicular networks to obtain the good quality of service. In this article first we have given the taxonomy of various techniques involved in fog computing. Then we have analyzed various security issues provided for fog architecture. Various cryptographic algorithms are provided to secure fog networks. Even though various security solutions are provided for fog computing, the access control schemes are not suitable for fog computing unlike cloud computing. Thus this paper provides various techniques in fog computing conclusion section is not required. Although a conclusion may review the main points of the paper, do not replicate the abstract as the conclusion. A conclusion might elaborate on the importance of the work or suggest applications and extensions.

REFERENCES

[1] Peng Zhang, Joseph K. Liu, F. Richard Yu, Mehdi Sookhak, Man Ho Au, and Xiapu Luo,"A Survey on Access Control in Fog Computing",IEEE Communications Magazine,February 2018.
[2] J. Zheng et al., “The Internet of Things,” IEEE Commun. Mag.,vol. 49, no. 11, Nov. 2011, pp. 30–31.
[3] F. Bonomi et al., “Fog Computing and Its Role in the Internet of Things,” 1st ACM MCC Wksp. Mobile Cloud Computing,MCC@SIGCOMM 2012, 2012, pp. 13–16.
[4] L. M. Vaquero and L. Rodero-Merino, “Finding Your Way in the Fog: Towards a Comprehensive Definition of Fog Computing,” ACM SIGCOMM Comp. Commun. Rev., vol. 44, no.5, 2014, pp. 27–32.
[5] S. Yi et al., “Fog Computing: Platform and Applications,” 3rd IEEE Wksp. Hot Topics in Web Systems and Technologies,2015, pp. 73–78.
[6] Amine Abouaomar, Abderrahime Filali and Abdellatif Kobbane,"Caching, Device-to-Device and Fog computing in 5th Cellular Networks Generation : Survey ",IEEE International Conference on Wireless Networks and Mobile Communications,2017.
[7] Xiang Wang, Supeng Leng, and Kun Yang, Social-Aware

Edge Caching in Fog Radio Access Networks, IEEE Access (Volume: 5), pages (8492 -8501) 24 April 2017
[8] Tom H. Luan, Longxiang Gao, Zhi Li, Yang Xiang, Guiyi We and Limin Sun Fog Computing: Focusing on Mobile Users at the Edge,arXiv:1502.01815 [cs.NI] 2015
[9] Mohammed S. Elbamby, Mehdi Bennis and Walid Saad, Proactive Edge Computing in Latency-Constrained Fog Networks, arXiv:1704.06749v1[cs.NI] 22 Apr 2017.
[10] S. W. Ko, K. Huang, S. L. Kim, H. Chae, Live prefetching for mobile computation offloading in IEEE Trans. Wireless Communication., vol. PP, no.99, pp. 11, 2017
[11] Ejder Batu, Mehdi Bennis, Muriel Mdard and Mrouane Debbah Towards Interconnected Virtual Reality: Opportunities, Challenges and Enablers,arXiv:1611.05356 [cs.NI] 2016.
[12] Y. Mao, C. You, J. Zhang, K. Huang, and K. B. Letaief, Mobile edge computing: Survey and research outlook ArXiv e-prints, 2017
[13] JIALE ZHANG, BING CHEN, YANCHAO ZHAO, XIANG CHENG, AND FENG HU,"Data Security and Privacy-Preserving in Edge Computing Paradigm: Survey and Open Issues ",IEEE transactions on security and privacy,Page(s): 18209 - 18237, Volume: 6,2018.
[14] D. Evans, "The internet of everything: How more relevant and valuable connections will change the world," Cisco IBSG, pp. 1–9, Dec. 2012.
[15] H. Sundmaeker, P. Guillemin, P. Friess, and S. Woelfflé,"Vision and challenges for realising the internet of things," Cluster of European Research Projects on the Internet of Things, European Commision, vol. 3, no. 3, pp. 34–36, Mar.2010.
[16] D. E. Culler, "The once and future internet of everything," GetMobile: Mobile Computing and Communications, vol.20, no. 3, pp. 5–11, Jul. 2016.
[17] P. G. Lopez, A. Montresor, D. Epema, A. Datta, T. Higashino,A. Iamnitchi, M. Barcellos, P. Felber, and E. Riviere,"Edge-centric computing: Vision and challenges," ACM SIGCOMM Computer Communication Review, vol. 45, no.5, pp. 37–42, Oct. 2015.
[18] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of things (iot): A vision, architectural elements, and future directions," Future generation computer systems, vol.29, no. 7, pp. 1645–1660, Sep. 2013.
[19] V. Turner, J. F. Gantz, D. Reinsel, and S. Minton, "The digital universe of opportunities: Rich data and the increasing value of the internet of things," IDC, White paper, Apr. 2014.
[20] J.S. Preden, K. Tammemae, A. Jantsch, M. Leier, A. Riid, E. Calis, "The Benefits of Self-Awareness and Attention in Fog and Mist Computing," Computer, vol.48, no.7, pp. 37-45, July 2015.
[21] A.V. Dastjerdi, H. Gupta, R. Calheiros, S. Ghosh, R. Buyya, "Fog Computing: Principles, Architectures, and Applications," Internet of Things: Principles and Paradigms,Morgan Kaufmann, Burlington,Massachusetts, USA, 2016.
[22] D. Guinard, V. Trifa and E. Wilde, "A resource oriented architecture for the Web of Things," Internet of Things, 2010, Tokyo, 2010, pp. 1-8.
[23] A.-R. Sadeghi, C. Wachsmann, M. Waidner, "Security and privacy challenges in industrial Internet of Things," Design Automation Conf.(DAC), 2015 52nd ACM/EDAC/IEEE, pp. 1-12, June 2015.
[24] G. Tanganelli, E. Mingozzi, C. Vallati, C. Cicconetti, "A distributed architecture for discovery and access in the internet of things," IEEE INFOCOM WKSHPS, pp. 45-46, 14-19 April 2013.
[25] Y. Li, M. Hou, H. Liu, and Y. Liu, "Towards a theoretical framework of strategic decision, supporting capability and information sharing under the context of Internet of Things," Inf. Technol. Manage., vol. 13, no. 4,pp. 205–216, 2012.
[26] C. Edwards, "Not-so-humble raspberry pi gets big ideas," Engineering & Technology, vol.8, no.3, pp. 30-33, April 2013.
[27] S. Joardar, A. Chatterjee and A. Rakshit, "A Real-Time Palm Dorsa Subcutaneous Vein Pattern Recognition System Using Collaborative Representation-Based Classification," in IEEE Trans. on Instrumentation and Measurement, vol. 64, no. 4, pp. 959-966, April015. doi: 10.1109/TIM.2014.2374713
[28] S. Sivaranjani, S. Sumathi, "Implementation of fingerprint and newborn footprint feature extraction on Raspberry Pi," Innovations in Information, Embedded and Communication Systems (ICIIECS), 2015Int'l Conf., pp. 1-6, 19-20 March 2015.
[29] V. Sandeep, K.L. Gopal, S. Naveen, A. Amudhan, L.S. Kumar,"Globally accessible machine automation using Raspberry pi based on Internet of Things," Advances in Computing, Communications and Informatics (ICACCI), Int'l Conf., pp. 1144-1147, 10-13 Aug. 2015.
[30] N. Agrawal, S. Singhal, "Smart drip irrigation system using raspberry pi and arduino," Computing, Communication & Automation (ICCCA),2015 Int'l Conf., pp. 928-932, 15-16 May 2015.
[31] P.T. Fung, D.R. White, S. Jouet, J. Singer, D.P. Pezaros, "The Glasgow Raspberry Pi Cloud: A Scale Model for Cloud Computing Infrastructures," Distributed Computing Systems Workshops (ICDCSW),2013 IEEE 33rd Int'l Conf., pp. 108-112, 2013.
[32] P. Abrahamsson, S. Helmer, N. Phaphoom, L. Nicolodi, N. Preda, L.Miori, M. Angriman, J. Rikkila, W. Xiaofeng, K. Hamily, S. Bugoloni,"Affordable and Energy-Efficient Cloud Computing Clusters: The Bolzano Raspberry Pi Cloud Cluster Experiment," Cloud Computing Technology and Science (CloudCom), 2013 IEEE 5th Int'l Conf., vol.2,p. 170-175, 2-5 Dec. 2013. doi: 10.1109/CloudCom.2013.121
[33] P. Turton, T.F. Turton, "PiBrain — A cost-effective supercomputer for educational use," Engineering and Technology (BICET 2014), 5th Brunei Int'l Conf., pp. 1-4, 1-3 Nov. 2014. doi: 10.1049/cp.2014.1121
[34] Matin Pirouz, and Justin Zhan. "Optimized relativity search: node reduction in personalized page rank estimation for large graphs." Journal of Big Data 3.1 (2016): 12. doi: 10.1186/s40537-016-0047-2
[35] C.Y Yum, Y.S. Beun, S. Kang, Y.R. Lee, J.S. Song, "Methods to use 6LoWPAN in IPv4 network," Advanced Communication Technology,The 9th Int'l Conf., vol.2, pp. 969-972, 12-14 Feb. 2007.
[36] S.H. Kim, J.S. Kang, H.S. Park, D. Kim, Y.J. Kim, "UPnP-ZigBee internetworking architecture mirroring a multi-hop ZigBee network topology," in IEEE Trans. on Consumer Electronics, vol.55, no.3, pp.1286-1294, August 2009. doi: 10.1109/TCE.2009.5277989
[37] A. Willig, K. Matheus, A. Wolisz, "Wireless Technology in Industrial Networks," in Proceedings of the IEEE, vol.93, no.6, pp. 1130-1151, June 2005. doi: 10.1109/JPROC.2005.849717
[38] P. Nikander, A. Gurtov, T. R. Henderson, "Host Identity Protocol (HIP):Connectivity, Mobility, Multi-Homing, Security, and Privacy over IPv4 and IPv6 Networks," in IEEE Communications Surveys & Tutorials, vol.12, no. 2, pp. 186-204, Second Quarter 2010.
[39] Nominated Projects for 4th Annual Internet of Things Awards [Last accessed: October 2015] Available: http://postscapes.com/internet-ofthings-award/2014/
[40] M. Hassanalieragh et al., "Health Monitoring and Management Using Internet-of-Things (IoT) Sensing with Cloud-Based Processing: Opportunities and Challenges," 2015 IEEE International Conference on Services Computing, New York, NY, 2015, pp. 285-292. doi:10.1109/SCC.2015.47
[41] M. Stecca, C. Moiso, M. Fornasa, P. Baglietto and M. Maresca, "A Platform for Smart Object Virtualization and Composition," in IEEE Internet of Things Journal, vol. 2, no. 6, pp. 604-613, Dec. 2015.
[42] EunJung Ko, J. Kang, J. Park, "A middleware for smart object in ubiquitous computing environment," Computing Technology and Information Management, 2012 Int'l Conf on, Seoul, pp. 400-403, 2012.
[43] L.F. Zeng, D. Feng, L.J. Qin, "SOSS: smart object-based storage system," Machine Learning and Cybernetics, 2004. Proceedings of 2004 Int'l Conf., vol.5, pp. 3263-3266 vol.5, 26-29 Aug. 2004.
[44] S. Cirani, L. Davoli, G. Ferrari, R. Leone, P. Medagliani, M. Picone, L.Veltri, "A Scalable and Self-Configuring Architecture for Service Discovery in the Internet of Things," in IEEE Internet of Things Journal, vol.1, no.5, pp. 508-521, Oct. 2014.
[45] I. Stojmenovic, W. Sheng "The Fog computing paradigm: Scenarios and security issues," Computer Science and Information Systems (FedCSIS), 2014 Federated Conf., pp. 1-8, 7-10 Sept. 2014.
[46] I. Demertzis et al., "Practical Private Range Search Revisited,"Proc. ACM SIGMOD'16, 2016, pp. 185–98.
[47] S. Han et al., "PPM-HDA: Privacy-Preserving and Multifunctional Health Data Aggregation with Fault Tolerance," IEEE Trans. Information Forensics and Security, vol. 11, no. 9,Sept. 2016, pp. 1940–55.
[48] C. Dwork, "Differential Privacy: A Survey of Results," Proc.5th Int'l. Conf. Theory Applications Models Computation,Berlin, Heidelberg: Springer, 2008, pp. 1–19.
[49] I. Demertzis et al., "Practical Private Range Search Revisited,"Proc. ACM SIGMOD'16, 2016, pp. 185–98.
[50] S. Han et al., "PPM-HDA: Privacy-Preserving and Multifunctional Health Data Aggregation with Fault Tolerance," IEEE Trans. Information Forensics and Security, vol. 11, no. 9,Sept. 2016, pp. 1940–55.

AUTHORS PROFILE

Dr.Usha is currently working as an associate professor at the software engineering department in SRMIST.She has 12 years of teaching experience.While working in Anna University chennai she worked in research projects for Smart and Secure techniques Research Lab. Her research interest include network security, machine learning, Bio informatics. Dr.Usha published nearly 40 research articles in peer reviewed journals and international conferences. She is GATE scorer and awarded as college first rank holder in UG. She is editorial board member for the journal Progress of Electrical and Electronic Engineering. She was awarded as Outstanding Reviewer within Top 10 percentile of reviewers in Elsevier-Pattern Recognition Letters in 2017.She is reviwer of Elsevier Journal - Computer and Electrical Engineering, Elsevier Journal- Pattern Recognition Letters, Springer- Multimedia tools and Applications,IEEE Access. She has coordinated IET sponsored Workshop on Cyber Security ,National Workshop on Internet of Things , National work shop on VANET and its security IET sponsored National Conference on Big data, cloud and Security. She is a active member of IET, ISTE, Indian Science Congress. Currently she is guiding 6 Phd Students..

S. Kannimuthu is currently working as Associate Professor in the Department of Computer Science and Engineering at Karpagam College of Engineering, Coimbatore, Tamil Nadu, India. He is also an In-Charge for the Center of Excellence in Algorithms. He did his PhD (CSE), M.E (CSE) and B.Tech (IT) at Anna University, Chennai. He has more than 12 years of teaching and industrial experience. He is the recognized supervisor of Anna University, Chennai. He is now guiding 7 PhD Research Scholars and One of his scholars completed the research. He has published 35 research articles in various International Journals. He published 1 book on "Artificial Intelligence" and 3 Book Chapters (SCI and Scopus Indexed). He has presented a number of papers in various National and International conferences. He has visited more than 45 Engineering colleges and delivered more than 80 Guest Lectures on various topics. He is the reviewer for 6 Journals and 3 Books. He has successfully completed the consultancy project through Industry-Institute Interaction for ZF Wind Power Antwerpen Ltd., Belgium. He has received funds from DRDO and ISRO to conduct workshops / seminars. He has guided a number of research-oriented as well as application oriented projects organized by well known companies like IBM. He is actively involving in setting up lab for Cloud Computing, Big Data Analytics, Open Source Software, Internet Technologies etc., His research interests include Artificial Intelligence, Data Structures and Algorithms and Machine Learning.

Mr.N.A.S.Vinoth is currently working as an assistant professor at software engineering department in SRMIST. He has 4 years of teaching experience. While working in Kalasalingam Institute of Technology he worked in research projects for Networking Research Lab. His research interest include network security, Big Data, machine learning. Vinoth presented nearly 4 research articles in National and international conferences. He has organized IET sponsored National work shop on VANET and its security, International Conference on Artificial intelligence and evolutionary computations in engineering systems. He is an IELTS Scorer and also an member of IEI.

H.Karthikeyan, received the B.Tech. degree in Information Technology from Veltech Hightech Engineering College, Avadi, Chennai, which is affiliated under Anna University, Chennai, India in 2010 and the M.Tech degree in Computer Science Engineering from SRM Institute of Science and Technology, Kattankulathur, Chennai, India, 2014. He is currently working toward the Ph.D.degree with SRM Institute of Science and Technology. His research interests include security in VANETs.