Indonesian Journal of Electrical Engineering and Computer Science
Vol. 18, No.3, June 2020, pp. 1486~1493
ISSN: 2502-4752, DOI: 10.11591/ijeecs.v18.i3.pp1486-1493

Mobile edge computing for internet of things (IoT): security and privacy issues

Rahman Atiqur, Guangfu Wu, Ali Md Liton
Information and Communication Engineering, Chongqing University of Posts and Telecommunications, Chongqing, China

Article Info

Article history:

Received Sep 4, 2019
Revised Dec 1, 2019
Accepted Dec 21, 2019

Keywords:

Internet of things (IoT)
Mobile edge computing (MEC)
Privacy
Security

ABSTRACT

Nowadays, the masonry for environment-friendly and protected network infrastructure designs, for example, Internet of Things (IoT) and gigantic information analytics are increasing at a quicker pace comparing to earlier state. Mobile edge computing (MEC) for an IoT widget is data dispensation that is achieved at or chosen by the producers of information. Herein, we propose the concepts, features, protection, and privacy applications of IoT authorized MEC with its data protection in our information driven globe. We emphasize on illuminating a kind of components which needs to be taken into reflection with a consistent, scalable, impenetrable and disseminated MEC structure. Again, we summarize the fundamental concepts about security threat alleviation strategies, the existing opportunities and challenges in the area of MEC. Finally, we take autonomous vehicles for example to analysis the security protection mechanism of MEC in IoT system.

Corresponding Author:

Guangfu Wu,
Information and Communication Engineering,
Chongqing University of Posts and Telecommunications,
Chongqing, 400065, P.R. China.
Email: wugf@cqupt.edu.cn

1. INTRODUCTION

Internet of things (IoT) [1] is concerned on enjoying integral features with the information explosion of technology. Billions of gadgets interrelated with one another swap data amongst themselves through community infrastructures connected by using an amount of dispersed nodes. In this peak, a variety of IoT apps can competently supply a lot greater trustworthy and particular network services for persons. At that point, a rising wide variety of gadgets/sensors are linked through the IoT systems, which generates gigantic statistic data to customers. Generally speaking, every record has to be dispatched to a middle server where the bulk of calculation is needed. That is to say, this practical application creates a huge volume of calculation in the process of information diffusion. Thus upcoming computing will be much more than the conventional requirement. Specially, IoT structures are incorporated into everyday life in the near future. Substantial units and endpoints comprising of wearable wristbands, intelligent sensor units, vehicles & actuators, which represent a large upcoming applications over a wide range. Mobile edge computing (MEC) is a fundamental strategy for the IoT network. As a consequence of information transfer along with confined gadget quality, the middle cloud computing has been used to analyze the quantity of information gathered from the IoT units [2]. The substantial set of data from users may face the risk of large safety and privacy. The government related department can remove the information which may be considered as individual privacy troubles using the statistics method from the IoT gadgets MEC network [2]. MEC got special attention from the academic and industrial world. The concept and progress of growing tightly closed part computing are presently near the beginning stage. A wide variety of nominal boundaries are forward to be

fixed from each tutorial and business viewpoint. The predominant motive of this article is to review the features, concept, protection & purposes of the empowered IoT aspects including the protection and privacy elements in our information-driven globe. And then, we take autonomous vehicles for example to analysis the security protection mechanism of MEC in IoT system.

Road Map: In Section 2, we talk about the security and architecture of MEC [2]. In Section 3, we present the possible opportunities and challenges for MEC. In Section 4, the privacy mechanisms are introduced. Section 5, we gives the security algorithm used in MEC networks. In Section 6, we discuss MEC use cases that are particularly viable. Finally, we summarize the paper in Section 7.

2. MOBILE EDGE COMPUTING (MEC): SECURITY AND ARCHITECTURE

In this part, we first give the structure and task of MEC platform. Then, we assess the basic concepts of security measurement and risk alleviation techniques.

2.1. Tasks and Architecture [2]

MEC is a scattered structural design, which is defined as the dispensation of records. It emerged to be limited by both bandwidth and time in an IoT scheme. The exercise of an aspect computing method is necessary when the latency is necessary to be optimized to avoid community dispersion [3] and when the statistics meting out yoke is excessive at a central infrastructure. A prolonged edition of MEC is fog computing, which is a design that makes use of side gadgets to do an extensive quantity of calculation, storage space, contact regionally, which obviously possesses enter and production referred to as transduction. Fog nodes determine whether to make the statistics or load off the statistics to the cloud server [4].

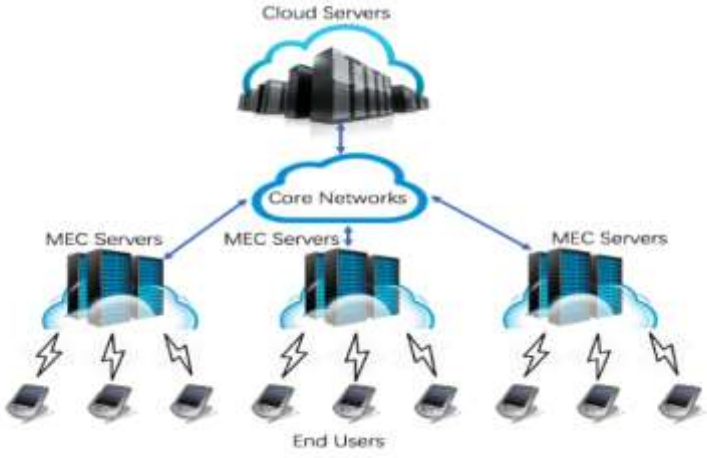

Figure 1.The fundamental MEC architecture

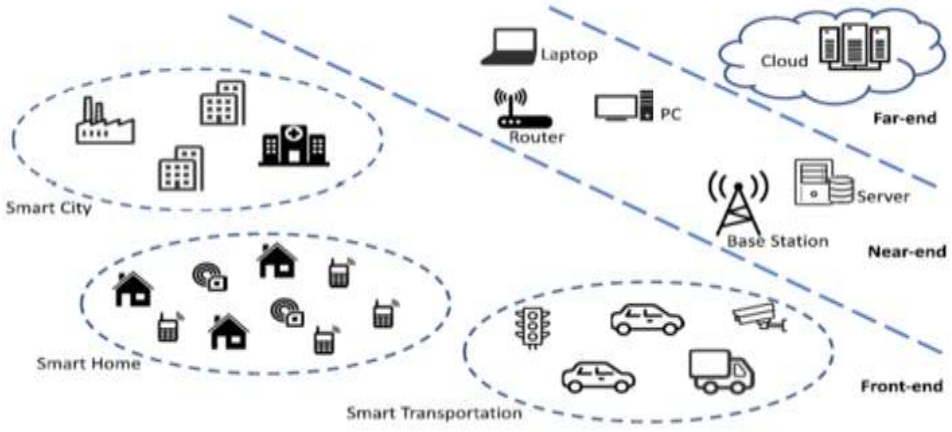

Figure 2. The classic MECarchitecture

Figure 1 and Figure 2 shows the fundamental MEC Architecture and classic MEC architecture respectively. The end users contain plentiful edge devices, for example smart phones, smart TV's, fitness and health activity tracker bands. Generally, fog nodes are attaching associations between the cloud servers and the end devices. End devices are interfaces between those diverse items connected with them [5].

2.2. Privacy and Security

An institute oversees and ensures the privatenessand protection of its IoT structure. Multiple termused in privacy-conducting management are itemize in the succession [6, 7].

a) Pseudonymity, is a phrase derived from a pseudonym, interpretation 'fake name', is a status of masked individuality. Pseudonym identifies an owner, that is, one or greater human beings who possess but do not expose their actual names (that is, lawful identities). Almost every of the pseudonym holders use pseudonyms owing to the fact they want to stay anonymous, however, vagueness is hard to gain & is often laden with prison vents. Real anonymity asks unlinkability, as an attacker's check of the pseudonym carrier's message offers no original statistics about the carrier's authentic identification. In Pseudonymity, the pseudonym is employ as an Identification to zq and characterize through groups for hazard alleviation the employ of the subsequent methods [8].

a) Rigid Password Mechanism: This mechanism makes sure that people obey with the perfect safety password policy. Passwords need not be a lexicon statement but have high entropies, for example, a mix of small and big letters with a mixture of one/two of a special character. Random password turbines should be utilize for generate robust passwords.

b) Encryption companies require encrypting inbound and outbound exchanges with the aid of using the modern-day cipher and continually have a calamity restoration backing sketch to be ready for possible statistics crossing.

c) Two-Factor Creditable (2FC): Via building use of 2FC, human beings are obligatory to prove their identities, which is after they have preliminary get entry to after coming into their username and key. It improve guard through commanding one greater point of examination & verification base totally ahead factors like ATM PIN, password, biometrics (For example, iris patterns, face recognition,& voiceprint).In adding up, 2FC ought to be in addition to classified as follows.

d) Voice-based and Short Message Service Texting: A code obtains by means of a short message service text, and interpretation the information permitted by way of an automatic voice name for impervious entry.

c) A tiny hardware gadget with an integral display to produce a one time password (OTP) for every deal.

e) S/W Application Tokens:A proxy of standard h/w coin, which is an invulnerable s/w program utility established in a token application downloaded to an end user's tab.

f) Push Notification:A "push" memo that turn up on a user' gadget via the network to authenticate the individuality of the person as a second-factor justification.

3. OPPORTUNITIESAND CHALLENGES [9]

Presently, digital globe delimited through millions of sensors implanted in interrelated IoT gadgets [10], which talk with every other. In reality, these sensors are impacting human communications with the digital globe, as a result making sure a flawless connection between people and gadgets. Beside with a huge amount of sensors & the rising amount of information created through them, we encounter a few demanding difficulty [11].

3.1. Privacy

Consumer privateness in present's earth consists of some statistics that can probably divulge a user's individuality, activities, & place. The intention of protection a user's personal data and growing number of contradicts the broader exploitation of IoT-enabled gadgets. So, a trustworthy gadget has to be intended to gather & procedure a gigantic quantity of records barring illuminating a user's confidential data [12].

3.2. Optimization Metrics

Here are many steps amid a variety of totaling ability in MEC. Deciding what step to contract with the workload difficulty is a complex job [13]. Yet, there are 4 metrics for decide on a most efficient workload distribution: 1) Latency, which is due to network & calculation, 2) Electricity utilization, 3) Price to accumulate and maintain, & 4) Bandwidth.

3.3. Jobs Offloading

In challenge offloading, the jobs of a machine must be outsourced [14]. Job offloading is noticeable for the IoT structures and ought to take region in all sorts of the IoT devices. Nonetheless, making employ of aspect nodes for calculation offloading is a difficulty owing to the impasse of properly partitioning computational jobs in an automatic method.

3.4. Public Accessibility of Edge Nodes

When a branch appliance (for example, a base station, switch, & a router) is supposed to be used for open right of entry, loads of accusations want to be deal with [15]. A public or private organization has to identify the fear associated by way of their personal devices barring compromise the preferred motive of the device (for example, a switch) to be use as an area knot. Multi-tenancy of feature nodes is single viable with up to date applied sciences that set security [16] as their very individual deliberation. Additively, different worries comprise the cost of upholding, information position, & workload for organizing excellent rate fashions making aspect nodes simply available [17].

4. PRIVACY MECHANISMS

For creating a sustainable edge model system with privacy & obtainable services [18], it is vital to implement a variety of privacy mechanisms, & put off any appeal from spiteful adversary. In this section presents the open privacy mechanisms that can be usage in MEC model [19].

4.1. Privacy Preserving [20]

Privacy is one of the most noteworthy challenges in other computing models as the ending user's sensitive data and private information are shifted from edge devices to the far servers [21]. In MEC, privacy question is more important because there are an amount of truthful but probing adversary, such as edge information centers, infrastructure provider, services provider, and even a number of users. These attackers are generally endorsed entities whose inferior aim is to get more responsive information that can be employing in a variety of insensible ways. In this situation, it is not possible to know whether a service provider is dependable in such open ecosystem with diverse faith domains. For example in Smart Grid, a group of private information of a house can be disclosed from the analysis of the smart meters or some other IoT devices [22], it way that no matter the house is empty or not, if the smart meters were manipulated by a hateful enemy, the user's privacy is totally leaked.In picky, the flee of private information, such as data, uniqueness and place, can direct to the very grave situations. At first, edge servers and sensor devices can gather sensitive data from the end devices; methods such as data aggregation based on homo-morphic encryption can recommend a privacy-preserving data study without decryption. Probabilistic public key encryption and pseudo-random permutatio can be used to drawing lightweight data privacy-preserving methods. Secondly, in the go-ahead and scattered computing surroundings, it is essential for users to guard their identity information throughout the verification and management processes. Finally, the place information of users is fairly expected as they frequently have a comparatively permanent point of interests (POIs), which means users will most likely make employ of the same edge servers repeatedly [23]. In this case, we should give additional concentration to defending our location privacy.

5. SECURITY ALGORITHM USED IN MEC ENVIRONMENT

5.1. Rivest, Shamir and Adelson (RSA) Algorithm

RSA which is the main universal Public Key algorithm and namedabbreviated from its inventors Rivest, Shamir, and Adelson (RSA). Rivest, Shamir, and Adelson (RSA) which is known as an asymmetric encryption/decryption algorithm. It is inconsistent in logic, that here public key approved all via which one be capable to encrypt the letter/message and private key which is second-hand for decryption is reserved secret and is not public to each person.

How Rivest, Shamir and Adelson (RSA) Algorithm is Available at Mobile Edge Scenery is Defined as: The Rivest, Shamir, and Adelson (RSA) algorithm is accustomed to promise the safety figures in mobile edge environment. Through Rivest, Shamir, and Adelson (RSA) algorithm, we encrypt our information for security reason. The cause of securing information is that solely involved and licensed consumers can get entry to it. After encryption information is preserved in the edge nodes so that when it is necessary then a call can be positioned to edge supplier. Edge supplier verifies the consumer and supplies the facts to the user. Like RSA is a Block CipherAlgorithm in which every communication is designed to an integer. In the planned mobile edge surroundings, public key is recognized to all, butprivate key is recognized only to the user who at the beginning owns the information. Thus encryption is made by means of mobile edge carrier

supplier and decryption is performed by the area client or consumer. If the information is encrypted with the public key, it will be decrypted by the matching private key only.

5.2. Advanced Encryption Standard (AES) Algorithm

AES in addition recognized as Rijndael is used for securing data. Advanced encryption standard is a symmetric key block cipher that has been examine significantly and used mostly nowadays. How the AES Algorithm will be work in part computing environment?Advanced encryption standard is the symmetric key encryption algorithm and is used by a key length of 128-bits for this principle. Advanced encryption standard is used widely at present for the protection of mobile edge gadgets data and privacy. Execution thinking states that first, side unit's user decides to use feature nodes services and will migrate his proceedings on area nodes. Then aspect devices user submits the requirements of his service to edge nodes and chooses the best-specified services presented by aspect nodes. When the migration of information to the chosen edge nodes happens and in future each time a utility uploads any data on edge, the facts will first be encrypted using the AES algorithm and then sent to edge nodes. Once encrypted, information is uploaded on the edge, any request to study statistics will occur after it is decrypted on the customers quit and then unquestionable text information can be studied by using the user. The undeniable text records are by no means written somewhere on edge. This includes all sorts of data. This encryption solution isobvious to the application and can be built-in rapidly and without difficulty besides any adjustments to the application. The key is by no means saved subsequent to the encrypted data, for the reason that it may compromise the key also. To keep the keys, a physical key administration server can be set up in the user's premises. This encryption protects information and keys guarantees that they continue to be under the users influence and will be exposed in storage or in transit. Advanced encryption standard algorithm has replaced the data encryption standard algorithm as permitted general for an extensive variety of applications.

5.3. Data Encryption Standard (DES) Algorithm

The DES algorithm is a block cipher. It encodes info in blocks of measurement 64 bits all. I.E. 64 bits of easy text goes as key to Data Encryption Standard algorithm, which produces 64 bits of ciphertext. The similar algorithm and key are used for encoding and decoding. The key span of this algorithm is 56 bits; however, a 64 bits key is input. Data Encryption Standard is, consequently, a symmetric key algorithm.

6. AUTONOMOUS VEHICLES APPLICATION OF MEC

While driverless vehicles are expected to be takenon the highway in the near future, the automobile industry has already invested billions of bucks in creating the technology. For operation, safely, these automobiles will need to acquire and analyze great quantities of data pertaining to their surroundings, guidelines, climate conditions, and the communication information with the other driving vehicles on the same road. They will additionally need to send same automobile information to manufacturers for quality improvement and same driving informationto the nearby municipal networks for properly law enforcement. Unfortunately, the transmitted information will require the aid of cell phones, private computers, and vary of the other connected devices. With so many gathering and transmitting automobiles data, the autonomous vehicles may become infeasibleif producers don't adopt new computing solutions. MEC structure makes it viable for self-reliant cars to collect, process, and share data between cars and mobile edge nodes networks in real time with nearly no latency.With the assist of the RSA algorithm, autonomous vehicles information security and privacy are maintained. The concept of how RSA algorithm works in a typical MEC network as a self-sustaining motor is given in Figure 3 [24, 25].

The flow of autonomous vehicles security mechanism by using RSA algorithm is as follows:

1) Encrypt the vehicle's data
2) Data is stored in the mobile edge nodes
3) When data is required to read a request is placed to mobile edge nodes
4) Mobile edge nodes authenticate the vehicles and
5) Deliver data to the perspective vehicles

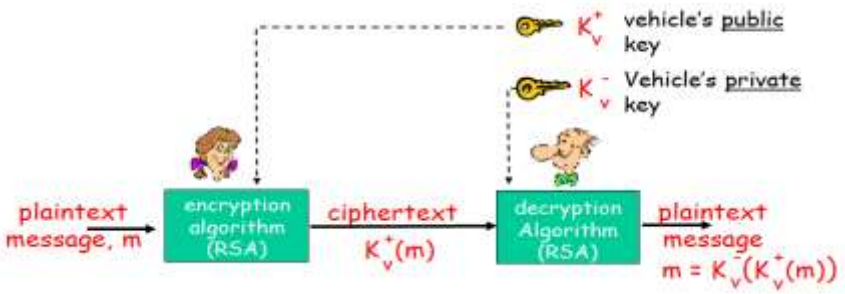

Figure 3. How security is ensured for an autonomous vehicle

7. CONCLUSION

In this paper, we assess the concept & architecture of Mobile Edge Computing (MEC) in the IoT epoch. We sum up the protection and confidentiality mechanisms of MEC discover the opportunities & challenges appeared in the latest year. At last, we talk about a use case scenario that shows how to authenticate user in autonomous vehicle system. MEC is started to be used in some fields and we expect that this article will encourage more researches in the area of MEC.

ACKNOWLEDGEMENT

This work is supported partly by the project of Science and Technology Research Program of Chongqing Education Commission of China under Grants KJQN201800642, the Doctoral student training program under Grants BYJS2016009.

REFERENCES

[1] K. Ashton et al., "That internet of things thing," *RFID journal*, vol. 22, no. 7, pp. 97–114, 2009.
[2] Alrowaily, M., & Lu, Z. (2018, October). Secure Edge Computing in IoT Systems: Review and Case Studies. In 2018 IEEE/ACM Symposium on Edge Computing (SEC) (pp. 440-444). IEEE
[3] C. M. Ferna´ndez, M. D. Rodr´ıguez, and B. R. Mun˜oz, "An edge computing architecture in the internet of things," in 2018 IEEE 21st International Symposium on Real-Time Distributed Computing (ISORC). IEEE, 2018, pp. 99–102.
[4] M. Mukherjee, R. Matam, L. Shu, L. Maglaras, M. A. Ferrag, N. Choud- hury, and V. Kumar, "Security and privacy in fog computing: Challenges," *IEEE Access*, vol. 5, pp. 19 293–19 304, 2017.
[5] M. Schaberg, Partnering on your Journey. KLM Services, LLC, 2017. [Online]. Available: https://www.klmservices.com/mt-content/uploads/2017/12/our-journey-presentation-osme-120417.pdf
[6] A. Pfitzmann and M. Hansen, "Anonymity, unlinkability, undetectability, unobservability, pseudonymity, and identity management-a consolidated proposal for terminology," *Version v0*, vol. 31, p. 15, 2008.
[7] J. Zhang, B. Chen, Y. Zhao, X. Cheng, and F. Hu, "Data security and privacy-preserving in edge computing paradigm: Survey and open issues," *IEEE Access*, vol. 6, pp. 18 209–18 237, 2018.
[8] B. Archana, A. Chandrashekar, A. G. Bangi, B. Sanjana, and S. Akram, "*Survey on usable and secure two-factor authentication*," in Recent Trends in Electronics, Information & Communication Technology (RTE- ICT), 2017 2nd IEEE International Conference on. IEEE, 2017, pp. 842–846.
[9] B. Varghese, N. Wang, S. Barbhuiya, P. Kilpatrick, and D. S. Nikolopou- los, "Challenges and opportunities in edge computing," *arXiv preprint arXiv*:1609.01967, 2016.
[10] A. Khanna and R. Anand, "*IoT based smart parking system*," in Internet of Things and Applications (IOTA), International Conference on. IEEE, 2016, pp. 266–270.
[11] Dey, H., Islam, R., & Arif, H. (2019, January). "*An Integrated Model To Make Cloud Authentication And Multi-Tenancy More Secure*," In 2019 International Conference on Robotics, Electrical and Signal Processing Techniques (ICREST) (pp. 502-506). IEEE.
[12] Tyagi, M., Manoria, M., & Mishra, B. (2019). "A Framework for Data Storage Security with Efficient Computing in Cloud," In International Conference on Advanced Computing Networking and Informatics (pp. 109-116). *Springer*, Singapore.
[13] Kaviya, K., Shanthini, K. K., & Sujithra, M. (2019). "Evolving Cryptographic Approach for Enhancing Security of Resource Constrained Mobile Device Outsourced Data in Cloud Computing."
[14] Garg, P., Sharma, M., Agrawal, S., & Kumar, Y. (2019). "*Security on Cloud Computing Using Split Algorithm Along with Cryptography and Steganography*," In International Conference on Innovative Computing and Communications (pp. 71-79). Springer, Singapore.
[15] Karajeh, H., Maqableh, M., & Masa'deh, R. (2020)."*Privacy and Security Issues of Cloud Computing Environment*," In Proceedings of the 23rd IBIMA Conference Vision (pp. 1-15).

[16] Namasudra, S. (2019). "An improved attribute-based encryption technique towards the data security in cloud computing,"*Concurrency and Computation: Practice and Experience*, 31(3), e4364.
[17] Garcia Lopez, P., Montresor, A., Epema, D., Datta, A., Higashino, T., Iamnitchi, A.,& Riviere, E. (2015). "Edge-centric computing: Vision and challenges,"*ACM SIGCOMM Computer Communication Review*, 45(5), 37-42.
[18] Huang, X., Yu, R., Kang, J., & Zhang, Y. (2017). "Distributed reputation management for secure and efficient vehicular edge computing and networks,"*IEEE Access*, 5, 25408-25420.
[19] Wang, T., Zhang, G., Liu, A., Bhuiyan, M. Z. A., & Jin, Q. (2018). "A secure IoT service architecture with an efficient balance dynamics based on cloud and edge computing,"*IEEE Internet of Things Journal*.
[20] Pang, H., & Tan, K. L. (2004, March). "*Authenticating query results in edge computing*," In Proceedings. 20th International Conference on Data Engineering (pp. 560-571). IEEE.
[21] Puthal, D., Obaidat, M. S., Nanda, P., Prasad, M., Mohanty, S. P., & Zomaya, A. Y. (2018). "Secure and sustainable load balancing of edge data centers in fog computing,"*IEEE Communications Magazine*, 56(5), 60-65.
[22] Rahman, A., Hassanain, E., & Hossain, M. S. (2017). "Towards a secure mobile edge computing framework for Hajj,"*IEEE Access*, 5, 11768-11781.
[23] Hu, Y. C., Patel, M., Sabella, D., Sprecher, N., & Young, V. (2015). "Mobile edge computing-A key technology towards 5G". *ETSI white paper*, 11(11), 1-16.
[24] Mollah, M. B., Azad, M. A. K., & Vasilakos, A. (2017). "Secure data sharing and searching at the edge of cloud-assisted internet of things,"*IEEE Cloud Computing*, 4(1), 34-42.
[25] Xu, Q., Su, Z., Zheng, Q., Luo, M., & Dong, B. (2018). "Secure content delivery with edge nodes to save caching resources for mobile users in green cities,"*IEEE Transactions on Industrial Informatics*, 14(6), 2550-2559.

BIOGRAPHIES OF AUTHORS

Mr. Rahman Atiqurreceived his Bachelor of Science (B.Sc) and Master of Engineering (M.Engg.) degree from the Department of Computer Science and Engineering at University of Chittagong, Chittagong, Bangladesh. In profession, he worked in the Department of Computer Science and Engineering, University of Chittagong, Bangladesh as an Assistant Professor since April 2016.Formar he was a lecturer in the Department of Computer Science and Engineering, University of Chittagong, Bangladesh. He is now conducting his Ph.D. research works under the Chinese Government Scholarships (CGS) Program at Chongqing University of Posts and Telecommunications, Chongqing, China. His current research interest lies in the field of edge computing based IoT systems.

Guangfu Wuis a senior engineer in school of Software Engineering, Chongqing University of Posts and Telecommunications, China. He received the B.S. degree inElectronic and Information EngineeringfromChongqingThree Gorges University and M.S. degree inCommunication and Information Systems fromChongqing University of Posts and Telecommunications, Chongqing, China, in 2004 and 2007, respectively,where he is currently pursuing the Ph.D. degreewith the School of Communication and Information Engineering.He current research interests include signalprocessing and the 5G wireless communication technology.

Mr.AliMdLiton received his Bachelor of Science (B.Sc) degree from the Department of EEE at,(Adust), Dhaka Bangladesh and Master of Engineering degree from the department of information and communications engineering atChongqing University of Posts and Telecommunications (CQUPT), Chongqing, China. He is now conducting his ph.D research works under the huawei Scholarship program at Chongqing University of Posts and Telecommunications (CQUPT), Chongqing, China. His Current research interest lies in the field of edge computing based IoT systems, wireless communication network PLC, LoRa.