A Novel Security Architecture of Internet of Things

Farhan Ali, He Yigang, and Ruan Yi

***Abstract*—In this era, the preeminent internet of things industry paradigms grasps the pledge to transfigure the concept of communication with the connectivity of billions of devices and objects, that's why, IoT persuasion is being appraised for this revaluation. Thousands of scientists, researchers, scholars and organizations are endowing worthwhile attention to support this regime change. Reasoning from this fact, security and privacy issues of IoT are getting highest cogitations in this decade. In this paper, we reviewed previous presented models, which have unanimously great efforts by it selves. But did not pay significant attention towards security and privacy layers as independent layers, so, we suggested that privacy and security layers must be considered in architecture of IoT, because sooner or later, both layers will be the parts of IoT model. We also included different types of threats of IoT layers and their perspective solutions. This contribution of work will be helpful to design and achieve a better security solution regarding IoT to overcome security risks and privacy breaches.**

***Index Terms*—Internet of things(IoT), architecture, privacy, security.**

I. Introduction

The Internet of things industry is appreciably state of the art rising industry in present time. It is being acclaimed for regime change in concept of communication with connectivity of trillion devices and objects in proximate future through its tactile physical and virtual infrastructure such as smart homes [1], smart transportation [2], smart city [3], smart grids [4], smart business e.g. logistics [5] so on and so forth. With the rising of last decade, IoT revolution dreamily changed our life [6], [7] and made communication tranquil is in this era, now it is proceeding towards largest computing platform [8]. Thousands of scientists, researchers, scholars, engineers are endeavoring their worthwhile attentions to support this revolution.

Researchers presented their work regarding to internet of things with 3,4 5 and even six-layer architecture but they didn't pay significant attention to security and privacy layers as distinct parts of architecture in internet of things. Because with escalating number of devices, the threats would be rapidly increased. So, with the connectivity of billions or trillions of devices as IoT is proclaiming, the security and privacy issue will be very difficult to tackle. So, whether architecture of IoT three, four, five or six layers, security and privacy layers must be the part of it.

In Section II we described previous presented and published architecture of internet of things and we suggested two additional layers (I) privacy and (II)security. In section III we defined previous published threats and in section IV we delineated their perspective solutions described by the researchers. And In section VI conclusion and future discussion.

Manuscript received May 20, 2019; revised July 20, 2019.

The authors are with the School of Electrical Engineering and Automation, Hefei University of Technology, China (e-mail: farhanali@mail.hfut.edu.cn, 18655136887@163.com, ruanyi0225@outlook.com).

II. Previous Work in Architecture of IoT

The fact is exceedingly thought provoking that from the start to rise of internet of things, every paper and every scholar who is getting significant attention to IoT has taken into consideration on architecture of IoT. Some scholars precisely described three-layer architecture application layer, network layer and perception layer [9]. Whereas other described four layers such as semantic layer, service layer, pattern layer and network layer [10]. Few authors depicted five layers for example perception layer, middleware layer, application layer, business layer and network layer [11]. while some defined other layers e.g. application, network, transport, 6lopwan and data link layer [12]. So, if we categorize publish research by scholars [1]-[33], we will have knowledge of different IoT layers such as internet layer, adaptation layer, things layer, network layer, transport layer, sensing layer, business layer, internet or decision layer, support and action layer, link layer, session layer, transmission layer, router/hub layer, cloud layer, messaging layer, middleware layer, SOA layers, object oriented layer and so on. So, but did not find privacy and security layers as they are extremely indispensable (See Fig. 1). Because high security is essentially required to protect critical physical infrastructure and sensitive data [34].

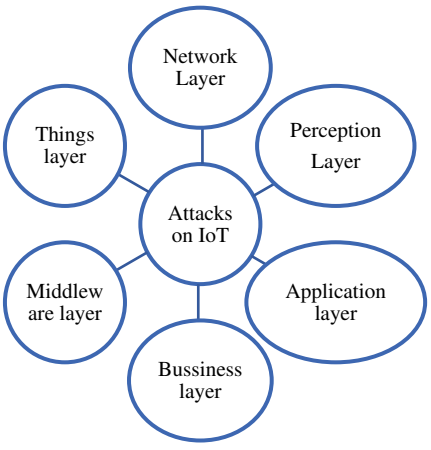

Fig. 1. Attacks upon few famous layers of IoT from literature.

Once a hacker/attacker gained access to unprotected device, cyber security system may be compromised [35].and it can lead to serious circumstances such as collecting the data from smart house can reveal the owner activities [36], [37], monitoring the power consumption can also disclose routine life [38]. Furthermore, false data injection [39]-[41],

DOI: 10.7763/IJCTE.2019.V11.1249

attacks up against data integrity [42], [43] and so on. As the number of devices will be increased, number of threats will be increased. So, a low complexity precoding and effective compressed sensing communication strategies will play better role to achieve the most effective results to minimize it. (As shown in Fig. 1 every layer is affected, please see Fig. 1).

III. Suggested Layers in Architecture Model of IoT

The culmination of security problem is significantly escalating, the global digital attacks has been used as a war weapon such as Stuxnet, Sucuri [44] at high level. Lower level vulnerabilities are increasing on daily basis, some revealed by researchers in the reference of smart communication [45]-[52]. So, it is imperative to protect sensitive data and information moving through the critical assets around in the system [53]-[55]. Now we step up towards our delineated model in which first and most prominent layer is security layer (See in Fig. 2).

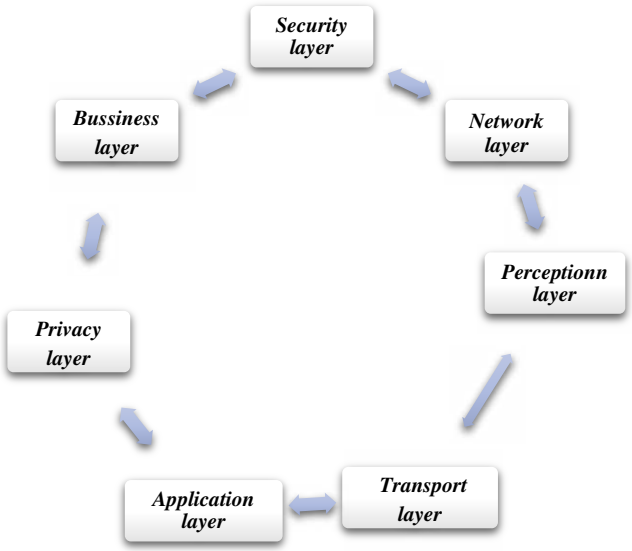

Fig. 2. Proposed model of seven layer.

First and most prominent layer is security layer (See in Fig. 2). The security layer is preponderantly necessary for secure communication executed by network layer for transmitting and receiving data between devices, services, software and applications. For software perceptive, security problems are engendered by vulnerabilities due to remiss design and implantations [56]. It must be assured all interfaces, communication through software or hardware, applications are free from attacks, viruses, bugs and threats. So, it's ought to be mandatory on network layer and surveillances upon all layers. Second layer of this model is network layer which is principally responsible to transmit and receive data through network and devices. It must be responsible to check data encryption and decryption in communication session because encryption attacks are most prominent in classification of attacks. It is most significant layer for hackers and attackers to manipulate information, hacking data, sensitive information, damaging systems and to destroy network. In case of vulnerability, it always leads to serious circumstances. Third layer is perception layer which can be compared with physical layer of OSI model. It is mainly responsible for device management, data collections and gathering information through virtual and physical world. It must be able to proceed the collected information, digitizing data and transfer via network layer. Fourth layer of this model is transport layer which is predominantly responsible to provide interface for communication. Fifth layer of this model is application layer which is usually responsible to compute and execute information or data provided through transport layer. Sixth layer of this model is privacy layer whom competence and capabilities are essentially required for data management, monitoring of data/information and protection. It must be essentially required for this layer to be assured that there is no leakage, collection, hacking or observing of information via internal or external source through any layer or device such as cookies. Cookies are considered or used for two purposes to identify user and authenticate user therefore, attacker might be stealing from a browser with potential attacks [57]-[66] such as cross site scripting attack (XSS). [57]. If it is transpiring, it must initiate for prevention of collection of information otherwise, it should generate a message to send the owner that from where and which kind of data/information is acquiring. Even, a common person should be able to understand. Last layer of this model is business layer, it must be divided in two parts, upper part is QoS and the lower part has ability of management of activities and all-embracing services to generate performance report, so the evaluation might easily be possible. Moreover, explanation in Fig. 4. (See Fig. 4)

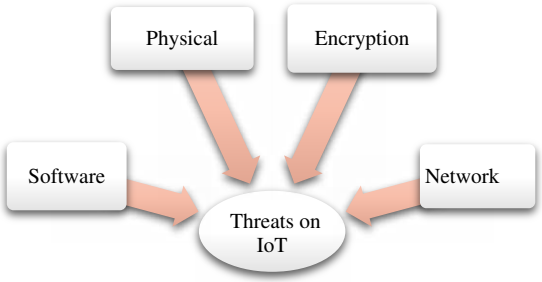

Fig. 3. Major classification of threats in IoT.

The reason of suggesting two layers in this architecture, if we categorize the threats, there are two prominent types of threats; **Internal and External. Internal security** expounds to protect the internal data and inside communication. While external security explicates to protect external communication. Furthermore, in details, (see Fig. 3) there are also four major types of threats; physical, network, software and encryption.

Furthermore, The IoT security and privacy model should be divided in three parts (See Fig. 4). Firstly, all layers must be capable to resolve their threats by themselves, secondly privacy layer must be able to tackle the internal threats which usually contains in IoT from 40 to 60% and also coordinate will all layers. Finally, security layer it should be able to handle external threats which are around 40 to 50% of threats. So, if we divide privacy and security categorically, we will be able to minimize the vulnerabilities of IoT system. It is quoted and stated that prevention is

better than cure. For IoT market wroth is estimating trillion-dollar net worth that describes connectivity of billion devices with billion people and their security concerns.

Privacy and Security are the most sensitive concern and hottest discussion now a days and organizations are responsible to provide their users to user friendly environments for smart communication. They should also deliver legitimate access for their private data concern against vulnerabilities and threats. Threats classification can be described in three most prominent classifications of attacks (See Table I).

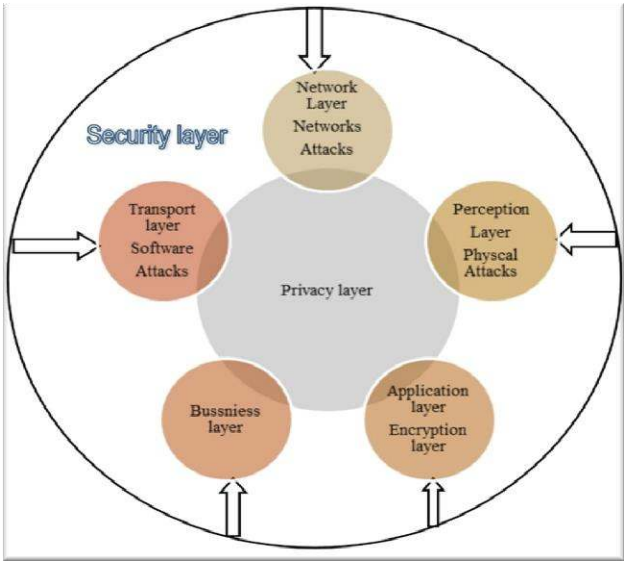

Fig. 4. Categorically division and explanation of privacy and security of seven-layers model Ref. Fig. 2.

TABLE I. CLASSIFICATION OF THREATS

Weak	• Unclassified data • weak passwords • low number of sensitive data within network/ system • by monitoring system vulnerabilitites • hourly/daily basis
Moderate	• Classified data • lack of monitoring contol • Systems transfer large amount of sensitive data over internet • common user interface • weakly/mothly basis
High	• Classified and Confidential data with legal/Private regulated data • Lack of transmission • Systems transfer sensitive data over network • Isolated systems • yearly basis

IV. PRIVACY AND SECURITY CHALLENGES OF IOT AND PROSPECTIVE SOLUTIONS

Common attacks on internet of things on different layers

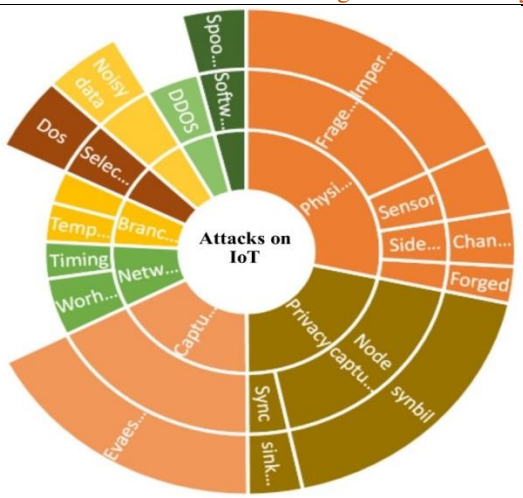

Chart 1. Consists upon random types of attacks [22], [30]-[33], [67]-[115] in internet of things.

According to Ericson connectivity of internet of things devices is 5.7 million every day. And Cisco estimated 37 billion new things connectivity and 4.5 billion new people will join up to 2020. With passage of time as the connectivity of devices will proliferate, the threats will also escalate. According to different surveys such as Forrester, internal threats are 42 to 58%, and 83% organizations suffered from it. So, rest of threats are external. Some parameter or principles must be mandatory such as integrity [76], confidentiality [77], [78], authentication [79], data management [80] and interoperability [81] to achieve reliable and secure communication. The purpose of this section is to validate our idea that security and privacy layer are important part of it. Without them it is very difficult to handle all vulnerabilities and threats under umbrella of IoT and also to consider all of them to achieve better security design and implementation to overcome privacy breaches and security risks. A standard model is required to handle security and privacy issues as previously OSI model was described a standard model. So, in present time a frame of reference architecture is required [115]. Limitation of IoT should be define with every prospect like edge and fog computing [116]-[119]. There are numerous types of attacks in which few important are being defined (See chart 1).

Physical attacks accomplish nearby or short distance from device such as physical capture and electronic jamming [30]. Network attacks are executed on network layer to stratagem for manipulation or destruction of the IoT network and also for hacking passwords, larceny of information and data. Software attacks are happened in the result of vulnerabilities that systems contain and provide chance to attacker to enter in system. Encryption attacks usually ensues for breaking encryption [31]. Sensor attacks commonly betide in gateways/nodes. Fake node Attack perpetrates malicious data to damage/destroy network. Side channel attack transpires on encrypted devices. Radio inference attack defines fake routing in system. [32]. Fragmented attack occurs in the lacking of layer end to end security [33].

Active jamming attack: User might be interposed/interfered/impeded through close by or accessible device which have the capability to send radio signals. Reader frequency modification attack: Any frequency applied to unauthorize to detect the communication between readers and tags. Tags frequency modification attack: Transfers information via reserved frequency. Kill order mechanism attack: Physically destruction of tags/nodes gateways [67]. Channel blocking attack: The hacker/ attacker engaged the channel for long time and block the communication. Impersonation attack: Fake data reader. Tempering attack: This attack has two phases, attacker listen the information, modify and passes through receiver [68]. Selfish threats: Few IoT end nodes break-off to save bandwidth or resources or because of node-failure. Malicious threats: Malicious threats causes software failure junk messages e.g. trojan virus. Dos: Endeavor to unavailable resource for its user in IoT for transmission. Routing attack: it usually occurs on routing path [69]. Sybil attack: The attacker maneuvers the single node into multiple identities through which they are being regarded as system parts. The system might be compromised with false redundant-ant information. Sinkhole attack: In which an opponent makes a damage node look attractive with close by nodes, so all data flows diverts to particular node through compromised node. So, as the outcomes of this attack, the system is being fooled to give credence that the data has been procured on the other side, all traffic is muted. In addition, this attack consequences in additional amount of energy consumption, which may lead to DoS attacks. Sleep deprivation attack: In which the node remains awake, ramifications of extra battery utilization, curtailing battery life and causing the node to shut down. Man-in-the-Middle attack: The goal of this attack is the communication channel; the unauthorized party can observe, monitor or keep track of all confidential, secret and classified communications between the two sides. An unauthorized party may even falsify the identification of the victim and communicate ordinarily to obtain extra extent of information [75]. Capture attacks: Directly capture node either physically or by modifying software. Atmosphere attack: Usually atmosphere destroy node/gateways or network e.g. wind or snow. So, they cannot work properly. Privacy disclosure: Data access from store via unauthorize secondary medium. Noisy Data attack: Additionally, add noise in data for sending false message or misinterpretation of message. Illegitimate data access: Spreads malicious information in IoT network. Software bugs: Access in a system through written code that does not follow any pattern [76] Cross-heterogenous attack: This attack ingress in access layer and network layer via message switching through which heterogenous networks security protection becomes weak and system becomes vulnerable to Man-in-Middle attack [82]. Spoofing attack: Ip address spoofing, mac address spoofing and fake domain name. Eavesdropping attack: Information transfers through IoT system has the highest probability to transmit through Eavesdropping attack. Insert attack: Alludes to insertion of system commands when system requires data input. Location tracking attack: Track the data through illegal access to tags and reveal the action of things layer [83]. Relay attack: Hacker might obtain valid data from the transmitted RFID signals between the tags and the reader, store the data and send it to the reader at a later time. Because the data is valid, so, the system will receive and process the data [84], [85]. Node Capture attacks: Key nodes are attained by hacker to get communication between parties, radio keys, or matching keys and so on. Node capture attack is kind of passive, active and physical attack it has three types (i) short communication attacks takes less than five minutes to compromise node (ii) Medium attacks take less than 30 minutes to compromise attack (iii) Long attacks take more than 30 minutes to compromise node [85], [86]. Timing attack: By obtaining the key information with analyzing the required time to break encryption algorithm [86]. Selective forward attack: Nodes acquires the packets but do not forward to its correct destination Wormholes attack and Sinkhole attack: Select a node through routing path, all data and information send to same destination [87]. Node tempering attack: Physically replacing node or part of hard ware or by electronically attaining access to communication layer to change sensitive information such as routing tables or cryptographic keys. Social engineering Attack: The attacker extracts the information to perform action by manipulating the user of IoT system. It also has six types Phishing, vishing, smishing, baiting, direct approach, Nigerian attacks and reverse social engineering [89], [92]. Proximity attacks: Hacker observe the communication between channel and interact them with injecting false data [90]. Collusion attack: Hacker achieve the data which is sent by aggregate node to base station [91]. Advanced persistent threats: these kinds of threats introduce false alarm rate and miss detection rates in IoT systems [92]. Network sniffers: Encrypts all passwords, disable CDP, SSH, SSL and IP security [95] Transmission threats: Fake data insertion in between communication links through three processes insertion, replication and manipulation [99].

V. Prospective Solutions for IoT

In this section we described the proposed solution of internet of things defined by different scientist, scholars and researchers against vulnerabilities and threats. And regarding to these solutions to validate our suggestion that security and privacy layers did not get so much attention as separate layers which are indispensable for IoT. They should be the parts of internet of things model to minimized the vulnerabilities, privacy breaches and security threats of IoT. In [66] IoT security can cleave in two categorizes parts (i) first is potential inherent security implications in IoT while second comes from protocol flaws and security vulnerabilities in IoT. The best solution is considered IPV6 technology. In [67] Lan li described Electronic screening for signals of particular frequencies and Blocker tags for faker serial numbers. In [68] Yu ping depicted point to point and end to end encryption in Transport layer. In [70] Hinai presented two-way security authentication in IoT through DTLS handshake established upon exchanging of certificate X.509 holding RSA Keys. In [74] Sun analyzes IoT security schemes for five layers. In [75] Vashi suggested six steps for IoT data safety which can be described as encryption, confidentiality, authentication, authorization, certification

and access control. In [78] Roman gave his recommendations firstly, ensure security of objects by default secondly, design secure protocols and final, improve quality of software implementations. In [82] Zhang defined that IoT security elements are being analyzed in three dimensions; network layer, security domain and security services. Perception domain is responsible for collection of data about environment or objects. In [85] Smache discussed to decompose the attacks by intrusion detection system. In [86] Zhao delineated solution of IoT threats IPV security channel, cryptography technology scheme, physical security schemes, security algorithm and routing protocols to protect IoT security and privacy. In [87] Y. Zhang adopted internal and external isolation of network to achieve the deep defense. In [89] Andrea stated that it is very hard to implement cryptography and trust management systems in IoT systems because both consume lot of power. New algorithm and protocols should be defined which consume less in protection of IoT systems. In [91] Yaseen introduced real time detection in IoT environment against collusion attacks. In [94] HU described that the NE of static game is deduced and its existence is proved. NE shows that attackers do not attack frequently when playing hybrid strategy games, and defenders can adjust detection strategies to improve security based on the knowledge of system expertise. In [95] Elwray defined intrusion detection system for IoT environment to lessen the gravity of threats and vulnerabilities. In [98] Ko proposed a platform to prevent cyber-attacks with information on fragile devices connected to the Internet. In [99] Ferreira demonstrated (UIOT) uniform and transparent internet of things based on existing technologies in IoT to provide privacy, integrity, confidentiality and authenticity for data exchange in between parties. In [100] Yan presented a survey from (2000-2014) in which characterized IoT by words. IoT security has 56.6 share in data. In [103] Taunja defined IDS to prevent from routing attack in IoT. In [104] Raza explain generic scheme in RPL for authenticity of topology. In [105] Pongel expressed single gateway and hope for IoT consists upon node registration scheme. In [107] Ashraf elucidated Dos detection for 6lowpan based upon IoT. In [110] Hamoud also described importance of security for IoT.

VI. Conclusion and Future Discussion

In this paper, we discussed pervious published work related with internet of things security and privacy architecture, layers threats, common threats and their prospective solutions through existing literature to validate our suggested model and found that Privacy and Security layers did not find significant importance as separate layers. Privacy and Security can be described the most sensitive concern. So, billions of people are affiliated with internet of things through smart developments and deployments. After the maturity of IoT, there will be massive escalation in number of devices which is expected in trillions, definitely the number of threats will be increased and criminal activities will go through the roof. Either market share of IoT maybe decreased or people can be avoided to use it frequently. So, we suggested two layers addition for it on the basis of previous published work. Countries and organizations are paying fruitful attention to IoT security. They must consider a standard model or architecture for IoT to minimize privacy breaches, internal and external security threats. So, the more work, energies, efforts and considerations are required to establish this kind of stand-alone model.

Acknowledgment

This work was supported by the National Natural Science Foundation of China under Grant No. 51577046, the State Key Program of National Natural Science Foundation of China under Grant No. 51637004, the national key research and development plan "important scientific instruments and equipment development Grant No.2016YFF0102200, Equipment research project in advance Grant No.41402040301.

References

[1] A. Ghaffarian-Hoseini *et al*., "The essence of future smart houses: From embeddingict to adapting to sustainability principles," *Renewable SustainableEnergy Rev.*, vol. 24, no. 1, pp. 593–607, 2013.
[2] S. Greengard, "Smart transportation networks drive gains," *Commun. ACM*, vol. 58, no. 1, pp. 25–27, 2015.
[3] G. Pan *et al*., "Trace analysis and mining for smart cities: Issues, methods, and applications," *IEEE Commun. Mag.*, vol. 121, no. 6, pp. 120–126, 2015.
[4] M. Amin and W. Bruce, "Toward a smart grid: Power delivery for the 21st century," *IEEE Power Energ. Mag*., vol. 3, no. 5, pp. 34–41, 2005.
[5] D. X. Li, W. He, and S. Li, "Internet of things in industries: A survey," *IEEE Trans. Ind.Inf*., vol. 10, no. 4, pp. 2233–2243, 2014.
[6] J. Gubbi *et al*., "Internet of Things (iot): A vision, architectural elements, andfuture directions," *Future Gener. Comput. Syst*., vol. 29, no. 7, pp. 1645–1660, 2013.
[7] Z. Liu, K. K. R. Choo, and M. Zhao, "Practical-oriented protocols forprivacy-preserving outsourced big data analysis: Challenges and future research directions," *Comput. Secur*., vol. 69, pp. 97–113, 2017.
[8] A. L. L. Atzori and G. Morabito, "The internet of things: A survey," *Comput. Netw*., vol. 54, no. 15, pp. 2787–2805, 2010.
[9] L. Li, "Study on security architecture in the Internet of Things," in P*roc. 2012 International Conference on Measurement, Information and Control*, 2012, pp.374-377.
[10] A. M. C. Souza and J. R. A. Amazonas, "An outlier detect algorithm using big data processing and internet of things architecture," *Procedia Computer Science*, vol. 52, pp. 1010-1015, 2015.
[11] S. Vashi, J. Ram, J. Modi, S. Verma, and C. Prakash, "Internet of Things (IoT): A vision, architectural elements, and security issues," in *Proc. 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*, 2017, pp. 492-496.
[12] R. Kanagavelu and K. M. M. Aung, "A survey on SDN based security in Internet of Things," in *Advances in Information and Communication Networks*, vol. 887, K. Arai, S. Kapoor, and R. Bhatia, Eds. Cham: Springer, 2019.
[13] G. P. Dai and Y. Wang, *XML-Based Structural Representing Method for Information of Things in Internet of Things*, Heidelberg, New York: Springer.
[14] S. Yang, X. Wen, W. Zheng, and Z. Lu, "Convergence architecture of Internet of Things and 3GPP LTE-A network based on IMS," in *Proc. 2011 Global Mobile Congress*, 2011, pp. 1-7.
[15] S. K. Lee, M. Bae, and H. Kim, "Future of IoT networks: A survey," *Applied Sciences (Switzerland)*, vol. 7, no. 10, 2017.
[16] V. Tyagi and A. Kumar, "Internet of Things and social networks: A survey," in *Proc. 2017 International Conference on Computing, Communication and Automation (ICCCA)*, 2017, pp. 1268-1270.
[17] P. V. Paul and R. Saraswathi, "The Internet of Things — A comprehensive survey," in *Proc. 2017 International Conference on Computation of Power, Energy Information and Communication (ICCPEIC)*, 2017, pp. 421-426.
[18] N. Miloslays and A. Tolstoy, "Internet of Things: information security challenges and solutions," *Cluster Comput.*, vol. 22, no. 1, pp. 103-119, 2019.

[19] H. Derhamy, J. Eliasson, J. Delsing and P. Priller, "A survey of commercial frameworks for the Internet of Things," in *Proc. 2015 IEEE 20th Conference on Emerging Technologies & Factory Automation (ETFA)*, 2015, pp. 1-8.

[20] S. Kraijak and P. Tuwanut, "A survey on internet of things architecture, protocols, possible applications, security, privacy, real-world implementation and future trends," in *Proc. 2015 IEEE 16th International Conference on Communication Technology (ICCT)*, 2015, pp. 26-31.

[21] U. Banerjee, C. Juvekar, S. H. Fuller, and A. P. Chandrakasan, "eeDTLS: Energy-efficient datagram transport layer security for the Internet of Things," in *Proc. GLOBECOM 2017 - 2017 IEEE Global Communications Conference*, 2017, pp. 1-6.

[22] R. Kanagavelu and K. M. M. Aung, "A survey on SDN based security in Internet of Things," in *Advances in Information and Communication Networks*, vol. 887, K. Arai, S. Kapoor, and R. Bhatia, Eds. Cham: Springer, 2019.

[23] A. M. C. Souza nd J. R. A. Amazonas, "An outlier detect algorithm using big data processing and Internet of Things architecture," *Procedia Computer Science*, vol. 52, pp. 1010-1015, 2015.

[24] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of Things: A survey on enabling technologies, protocols, and applications," *IEEE Comlamunications Surveys & Tutorials*, vol. 17, no. 4, pp. 2347-2376, 2015.

[25] Z. Yang, Y. Yue, Y. Yang, Y. Peng, X. Wang, and W. Liu, "Study and application on the architecture and key technologies for IOT," in *Proc. 2011 International Conference on Multimedia Technology (ICMT)*, 2011, pp. 747–751.

[26] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A survey," *Comput. Networks*, vol. 54, no. 15, pp. 2787–2805, 2010.

[27] R. Khan, S. U. Khan, R. Zaheer, and S. Khan, "Future internet: The Internet of Things architecture, possible applications and key challenges," in *Proc. 2012 10th International Conference on Frontiers of Information Technology (FIT)*, 2012, pp. 257–260.

[28] L. Nastase, "Security in the Internet of Things: A Survey on application layer protocols," in *Proc. 2017 21st International Conference on Control Systems and Computer Science (CSCS)*, 2017, pp. 659-666.

[29] S. Deshmukh and S. S. Sonavane, "Security protocols for Internet of Things: A survey," in *Proc. 2017 International Conference on Nextgen Electronic Technologies: Silicon to Software (ICNETS2)*, 2017, pp. 71-74.

[30] I. Andrea, C. Chrysostomou, and G. Hadjichristofi, "Internet of Things: Security vulnerabilities and challenges," in *Proc. IEEE Symp. Comput. Commun. (ISCC)*, Jul. 2015, pp. 180-187.

[31] Y. Yang, L. Wu, G. Yin, L. Li, and H. Zhao, "A survey on security and privacy issues in Internet-of-Things," *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1250-1258, 2017.

[32] S. Deshmukh and S. S. Sonavane, "Security protocols for Internet of Things: A survey," in *Proc. 2017 International Conference on Nextgen Electronic Technologies: Silicon to Software (ICNETS2)*, 2017, pp. 71-74.

[33] M. Amadeo *et al*., "Information-centric networking for the internet of things: challenges and opportunities," *IEEE Network*, vol. 30, no. 2, pp. 92-100, 2016.

[34] K. Sha, W. Wei, A. Yang, and W. Shi, "Security in Internet of Things: Opportunitiesand challenges," in *Proc. International Conference on Identification, Information & Knowledge in the Internet of Things (IIKI 2016)*, 2016.

[35] C. Lin and G. Wu, "Enhancing the attacking efficiency of the node capture attack in WSN: A matrix approach," *J. Supercomput.*, vol. 66, no. 2, pp. 989–1007, 2013.

[36] I. Rouf *et al*., "Neighborhood watch: Security and privacy analysis of automaticmeter reading systems," in *Proc. the 2012 ACM Conference onComputer and Communications Security*, 2012.

[37] X. Pan, Z. Ling, A. Pingley, W. Yu, K. Ren, N. Zhang, and X. Fu, "How privacy leaks from bluetooth mouse?" *IEEE Trans. Dependable Secure Comput.*, vol. 13, no.4, pp. 461–473, 2016.

[38] A. Molina-Markham *et al*., "Private memoirs of a smart meter," in *Proc. the Second ACM Workshop on Embedded Sensing Systems for Energy-Efficiency in Buildings*, 2010.

[39] J. Lin, W. Yu, and X. Yang, "On false data injection attack against multistep electricity price in electricity market in smart grid," *IEEE Trans. Parallel Distrib. Syst.*, vol. 27, no. 1, pp. 286–302, 2016.

[40] Q. Yang, J. Yang, W. Yu, D. An, N. Zhang, and W. Zhao, "On false data-injection attacks against power system state estimation: Modeling and countermeasures," I*EEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 3, pp. 717–729, 2014.

[41] X. Yang, J. Lin, W. Yu, P. Moulema, X. Fu, and W. Zhao, "A novel en-route filtering scheme against false data injection attacks in cyber-physical networked systems, *IEEE Trans. Comput.*, vol. 64, no. 1, pp. 4–18, 2015.

[42] Q. Yang, D. An, R. Min, W. Yu, X. Yang, and W. Zhao, "On optimal pmu placement based defense against data integrity attacks in smart grid," *IEEE Trans. Inf.Forensics Secur.*, vol. 12, no. 7, pp. 1735–1750, 2017.

[43] X. Zhang, X. Yang, J. Lin, G. Xu, and W. Yu, "On data integrity attacks against realtime pricing in energy-based cyber-physical systems," *IEEE Trans. Parallel Distrib. Syst*., vol. 28, no. 1, pp. 170–187, 2017.

[44] Y. Chahid, M. Benabdellah, and A. Azizi, "Internet of things security," in *Proc. 2017 International Conference on Wireless Technologies, Embedded and Intelligent Systems (WITS)*, 2017, pp. 1-6.

[45] Z. Ling, J. Luo, Y. Xu, C. Gao, K. Wu, and X. Fu, "Security vulnerabilities of Internet of Things: A case study of the smart plug system," *IIEEE Int.-of-Things (IoT) J*., vol. 1, no.1, p. 99, 2017.

[46] C. D'Orazio, K. K. R. Choo, and L. T. Yang, "Data exfiltration from Internet of Things devices: IoS devices as case studies," *IEEE Internet Things J*., vol. 4, no. 1, pp. 524–535, 2017.

[47] C. D'Orazio and K. K. R. Choo, "A technique to circumvent ssl/tls validations on iosdevices," *Future Gener. Comput. Syst*., vol. 74, pp. 366–374, 2017.

[48] C. J. D'Orazio, R. Lu, K. K. R. Choo, and A. V. Vasilakos, "A Markov adversary modelto detect vulnerable IOS devices and vulnerabilities in IOS apps," *Appl. Math.Comput*., vol. 293, pp. 523–544, 2017.

[49] C. D'Orazio and K. K. R. Choo, "Circumventing IOS security mechanisms for apt forensic investigations: A security taxonomy for cloud apps," *Future Gener.Comput. Syst*., vol. 79, pp. 247–261, 2018.

[50] Q. Do, B. Martini, and K. K. R. Choo, "Is the data on your wearable device secure? An Android wear smartwatch case study," *Softw. Pract. Exper*., vol. 47, no. 3, pp. 391–403, 2017.

[51] Q. Do, B. Martini, and K. K. R. Choo, "A data exfiltration and remote exploitation attack on consumer 3d printers," *IEEE Trans. Inf. Forensics Secur*., vol. 11, no. 10, pp. 2174–2186, 2016.

[52] Q. Do, B. Martini, and K. K. R. Choo, "Exfiltrating data from android devices," *Comput. Secur*., vol. 48, pp. 74–91, 2015.

[53] J. Holdsworth, W. B. Glisson, and K. K. R. Choo, "Medical device vulnerability mitigation effort gapanalysis taxonomy," *Smart Health*, vol. 12, pp. 82-98, 2019.

[54] A. Anjum *et al*., "An efficient privacy mechanism for electronic healthrecords," *Comput. Secu*r., vol. 72, pp. 196–211, 2018.

[55] V. Casola, A. Castiglione, K. K. R. Choo, and C. Esposito, "Healthcare-related data inthe cloud: Challenges and opportunities," *IEEE Cloud Comput*., vol. 3, no. 6, pp. 10–14, 2016.

[57] Z. K. Zhang, M. C. Y. Cho, C. W. Wang, C. W. Hsu, C. K. Chen, and S. Shieh, "Iot security: Ongoing challenges and research opportunities," in *Proc. 2014 IEEE 7th International Conference on Service-Oriented Computing and Applications*, 2014, pp. 230-234.

[58] R. Putthacharoen and P. Bunyatnoparat, "Protecting cookies from cross site script attacks using dynamic cookies rewriting technique," in *Proc. 13th International Conference on Advanced Communication Technology (ICACT2011)*, 2011, pp. 1090-1094.

[59] H. Takahashi, K. Yasunaga, M. Mambo, K. Kim, and H. Y. Youm, "Preventing abuse of cookies stolen by XSS," in *Proc. 2013 Eighth Asia Joint Conference on Information Security*, 2013, pp. 85-89.

[60] A. Aladeokin, P. Zavarsky, and N. Memon, "Analysis and compliance evaluation of cookies-setting websites with privacy protection laws," in *Proc. 2017 Twelfth International Conference on Digital Information Management (ICDIM)*, 2017, pp. 121-126.

[61] A. Juels, M. Jakobsson, and T. N. Jagatic, "Cache cookies for browser authentication," in *Proc. 2006 IEEE Symposium on Security and Privacy (S&P'06)*, 2006, pp. 5-305.

[62] M. Casado, P. Cao, A. Akella, and N. Provos, "Flow-cookies: Using bandwidth amplification to defend against DDoS flooding attacks," in *Proc. 2006 14th IEEE International Workshop on Quality of Service*, 2006, pp. 286-287.

[63] C. Smith and A. Matrawy, "Comparison of operating system implementations of SYN flood defenses (Cookies)," in *Proc. 2008 24th Biennial Symposium on Communications*, 2008, pp. 243-246.

[64] P. Paul *et al*., "Using browser cookies for event monitoring and user verification of an account," in *Proc. 2018 IEEE 9th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON)*, 2018, pp. 455-460.

[65] K. Nirmal, B. Janet, and R. Kumar, "It's more than stealing cookies - Exploitability of XSS," in *Proc. 2018 Second International Conference on Intelligent Computing and Control Systems (ICICCS)*, 2018, pp. 490-493.

[66] M. Conti, A. Gangwal, S. P. Gochhayat, and G. Tolomei, "Spot the difference: Your bucket is leaking: A novel methodology to expose

A/B testing effortlessly," in *Proc. 2018 IEEE Conference on Communications and Network Security (CNS)*, 2018, pp. 1-7.
[67] L. Li, "Study on security architecture in the Internet of Things," in *Proc. 2012 International Conference on Measurement, Information and Control*, 2012, pp. 374-377.
[68] P. Yu, "Privacy security in mobile RFID networks," *Journal of Chongqing College of Electronic Engineering*, no. 19, pp. 91-92, 2010.
[69] X. Xingmei, Z. Jing, and W. He, "Research on the basic characteristics, the key technologies, the network architecture and security problems of the Internet of things," in *Proc. 2013 3rd International Conference on Computer Science and Network Technology*, 2013, pp. 825-828.
[70] S. A. Hinai and A. V. Singh, "Internet of things: Architecture, security challenges and solutions," in *Proc. 2017 International Conference on Infocom Technologies and Unmanned Systems (Trends and Future Directions) (ICTUS)*, 2017, pp. 1-4.
[71] T. Kothmayr, C. Schmitt, W. Hu, M. Brünig, and G. Carle, "A DTLS based end-to-end security architecture for the Internet of Things with two-way authentication," in *Proc. 37th Annual IEEE Conference on Local Computer Networks - Workshops*, 2012, pp. 956-963.
[72] A. M. C. Souza and J. R. A. Amazonas, "An outlier detect algorithm using big data processing and Internet of Things architecture," *Procedia Computer Science*, vol. 52, pp. 1010-1015, 2015.
[73] N. W. Bergmann and P. J. Robinson, "Server-based Internet of Things architecture," in *Proc. 2012 IEEE Consumer Communications and Networking Conference (CCNC)*, 2012, pp. 360-361.
[74] H. F. Sun *et al*., "A security scheme research of the Internet of Things based on the SA/NIA architecture," *Advanced Materials Research*, vol. 320, pp. 291-296, 2011.
[75] S. Vashi, J. Ram, J. Modi, S. Verma, and C. Prakash, "Internet of Things (IoT): A vision, architectural elements, and security issues," in *Proc. 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*, 2017, pp. 492-496.
[76] Isha, A. K. Luhach, and S. Kumar, "Layer based security in Internet of Things: Current mechanisms, prospective attacks, and future orientation," in *Smart Trends in Information Technology and Computer Communications*, vol. 628, A. Unal, M. Nayak, D. Mishra, D. Singh, and A. Joshi, Eds. Singapore: Springer, 2016
[77] M. U. Farooq and M. Waseem, "A critical analysis on the security concerns of internet of things (IoT)," *Int. J. Comput. Appl.*, vol. III, no. 7, pp. 1-6, 2015.
[78] R. Roman, P. Najera, and J. Lopez, "Securing the internet of things," *IEEE Computer*, vol. 44, pp. 51-58, 2011.
[79] R. Roman, J. Zhou, and J. Lopez, "On the features and challenges of security and privacy in distributed Internet of Things," *Comput. Netw.*, vol. 57, no. 10, pp. 2266-2279, 2013.
[80] K. Singh and D. D. Singh Tomar, "Architecture, enabling technologies, Security and privacy, and applications of Internet of Things: A survey," in *Proc. 2018 2nd International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*, 2018, pp. 642-646.
[81] Z. Qi, P. SilpaChaitanya, and T. Sudhir, "Spoofing attack detection wireless networks using advanced KNN," *International Journal of Smart Device and Appliance*, vol. 4, no. 1, pp. 1-8, 2016.
[82] H. Li and X. Zhou, "Study on security architecture for Internet of Things," in *Applied Informatics and Communication*, vol. 224, D. Zeng, Ed. Heidelberg, Berlin: Springer, 2011.
[83] P. Rughoobur and L. Nagowah, "A lightweight replay attack detection framework for battery depended IoT devices designed for healthcare," in *Proc. 2017 International Conference on Infocom Technologies and Unmanned Systems (Trends and Future Directions) (ICTUS)*, 2017, pp. 811-817.
[84] M. Smache, N. E. Mrabet, J. Gilquijano, A. Tria, E. Riou, and C. Gregory, "Modeling a node capture attack in a secure wireless sensor networks," in *Proc. 2016 IEEE 3rd World Forum on Internet of Things (WF-IoT)*, 2016, pp. 188-193.
[85] K. Zhao and L. Ge, "A survey on the Internet of Things security," in *Proc. 2013 Ninth International Conference on Computational Intelligence and Security*, 2013, pp. 663-667.
[86] Y. Zhang, W. Zou, X. Chen, C. Yang, and J. Cao, "The security for power Internet of Things: Framework, policies, and countermeasures," in *Proc. 2014 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery*, 2014, pp.139-142.
[87] A. Perrig, J. Stankovic, and D. Wagner,"Security in wireless sensor networks," *Communications of the ACM*, vol. 47, no. 6, pp. 53-57, 2004.
[88] I. Andrea, C. Chrysostomou, and G. Hadjichristofi, "Internet of Things: Security vulnerabilities and challenges," in *Proc. 2015 IEEE Symposium on Computers and Communication (ISCC)*, 2015, pp. 180-187.
[89] B. Bostami, M. Ahmed, and S. Choudhury, "False data injection attacks in Internet of Things," in *Performability in Internet of Things*, F. Al-Turjman, Ed. Cham: Springer, 2019.
[90] H. Xu, D. Sgandurra, K. Mayes, P. Li, and R. Wang, "Analyzing the resilience of the Internet of Things against physical and proximity attacks," *Lecture Notes in Computer Science*, vol 10658, 2017.
[91] Q. Yaseen, M. Aldwairi, Y. Jararweh *et al*., "Collusion attacks mitigation in Internet of Things: A fog based model," *Multimedia Tools and Applications*, vol. 77, no. 14, pp. 18249-18268, 2018.
[92] I. Sahmi, T. Mazri, and N. Hmina, "Security study of different threats in Internet of Things," *Lecture Notes in Intelligent Transportation and Infrastructure*, 2019.
[93] A. Al-Gburi, A. Al-Hasnawi, and L. Lilien, "Differentiating security from privacy in Internet of Things: A survey of selected threats and controls," *Computer and Network Security Essentials*, 2018.
[94] Q. Hu, S. Lv, Z. Shi, L. Sun, and L. Xiao, "Defense against advanced persistent threats with expert system for Internet of Things," *Lecture Notes in Computer Science*, vol 10251, 2017.
[95] M. Elrawy, A. Awad, and H. Hamed, "Intrusion detection systems for IoT-based smart environments: A survey," *Journal of Cloud Computing*, vol. 7, p. 21, 2018
[96] A. A. Zaidan, B. B. Zaidan, M. Y. Qahtan *et al*., "A survey on communication components for IoT-based technologies in smart homes," Telecommunication Systems, vol. 69, no. 1, pp. 1–25, 2018.
[97] S. A. Alabady, F. Al-Turjman, and S. Din, "A novel security model for cooperative virtual networks in the IoT era," *International Journal of Parallel Programming*, pp. 1–16, 2018
[98] E. Ko, T. Kim, and H. Kim, "Management platform of threats information in IoT environment," *Journal of Ambient Intelligence and Humanized Computing*, vol. 9, no. 4, pp. 1167-1176, 2018.
[99] H. G. C. Ferreira and R. T. S. Junior, "Security analysis of a proposed internet of things middleware," *Cluster Computing*, vol. 20, no. 1, pp. 651-660, 2017.
[100] B. N. Yan, T. S. Lee, and T. P. Lee, "Mapping the intellectual structure of the Internet of Things (IoT) field (2000–2014): A co-word analysis," *Scientometrics*, vol. 105, no. 2, pp. 1285-1300, 2015.
[101] M. Aly, F. Khomh, M. Haoues, A. Quintero, and S. Yacout, "Enforcing security in Internet of Things frameworks: A Systematic literature review," *Internet of Things*, vol. 6, 2019.
[102] N. N. Srinidhi, S. M. D. Kumar, and K. R. Venugopal, "Network optimizations in the Internet of Things: A review," *International Journal of Engineering Science and Technology*, vo. 22, issue 1, pp. 1-21, 2019.
[103] R. Tanuja, Y. Shruthi, S. Manjula, K. Venugopal, and L. Patnaik, "Token based privacy preserving access control in wireless sensor networks," in *Proc. International Conference on Advanced Computing and Communications(ADCOM)*, 2015, pp. 45–50.
[104] S. Raza, L. Wallgren, and T. Voigt, "SVELTE: real-time intrusion detection in the Internet of Things," *Ad Hoc Networks*, vol. 11, no. 8, pp. 2661–2674, 2013.
[105] H. Perrey, M. Landsmann, O. Ugus, T. C. Schmidt, and M. Wahlisch, "TRAIL: Topologyauthentication in RPL," arXiv:1312.0984, 2016.
[106] P. Pongle and G. Chavan, "Real time intrusion and wormhole attack detection in Internet of things," *Int. J. Comput. Appl*., vol. 9, p. 121, 2015.
[107] Q. M. Ashraf, M. H. Habaebi, G. R. Sinniah, and J. Chebil, *Broadcast Based Registration Technique for heterogenous Nodes in the IoT*, 2014.
[108] P. Kasinathan, C. Pastrone, M. A. Spirito, and M. Vinkovits, "Denial-of-servicedetection in 6lowpan based Internet of Things," in *Proc. IEEE 9th International Conference on Wireless and Mobile Computing, Networking andCommunications (WiMob)*, 2013, pp. 600–607.
[109] D. Yin, L. Zhang, and K. Yang, "A DDoS attack detection and mitigation with software-defined Internet of Things framework," *IEEE Access,* vol. 6, pp. 24694-24705, 2018.
[110] G. L. Santos, V. T. Guimarães, G. C. Rodrigues, L. Z. Granville, and L. M. R. Tarouco, "A DTLS-based security architecture for the Internet of Things," in *Proc. 2015 IEEE Symposium on Computers and Communication (ISCC)*, 2015, pp. 809-815.
[111] D. Singh, G. Tripathi, and A. Jara, "Secure layers based architecture for Internet of Things," in *Proc. 2015 IEEE 2nd World Forum on Internet of Things (WF-IoT)*, 2015, pp. 321-326.
[112] J. Qian, H. Xu, and P. Li, "A novel secure architecture for the Internet of Things," in *Proc. 2016 International Conference on Intelligent Networking and Collaborative Systems (INCoS)*, 2016, pp. 398-401.

[113] W. Zhang, B. Qu, "Security architecture of the Internet of Things oriented to perceptual layer," *International Journal on Computer Consumer and Control (IJ3C)*, vol. 2, no. 2, 2013.
[114] Y. Huang, Y. He, Q. Luo, L. Shi, and Y. Wu, "Channel estimation in MIMO–OFDM systems based on a new adaptive greedy algorithm," *IEEE Wireless Communications Letters*, vol. 8, no. 1, pp. 29-32, 2019.
[115] A. Farhan and Y. He, "Spectrum for next generation technologies," in *Proc. the 2019 8th International Conference on Software and Information Engineering (ICSIE '19)*, 2019, pp. 188-191.
[116] T. Cheng, Y. He, L. Shi, Y. Wu, Y. Huang, and Y. Sui, "A novel adaptive hybrid truncation precoding strategy in massive MIMO," *IEEE Communications Letters*, vol. 22, no. 11, pp. 2298-2301, November 2018.
[117] R. Atta, S. Kiran, D. Sujata, and K. M. Aftab, "Management of resource USAGE in mobile cloud computing," *International Journal of Pure and Applied Mathematics*, vol. 119, pp. 255-261.
[118] R. Atta, D. Sujata, K. Mahi, A. Areej, A. Atheer, M. Heba, A. Nadeen, A. Wejdan, and S. Kiran, "A comprehensive study of mobile computing in telemedicine," in *Proc. International Conference on Advanced Informatics for Computing Research*, 2018.
[119] Sujata, B. Sitanath, B. Debajit, and R. Atta, "Edge and FOG computing in healthcare – A review," *Scalable Computing: Practice and Experience*, vol. 20, pp. 191-206, 2019.

Farhan Ali received his BS (electronics and communication) and MS (electrical and electronics systems) from the University of Lahore, Pakistan in 2012 and 2016 respectively. From 2016-2017, Ali worked as C.E.O of Aqua Clean, Pakistan. Ali is currently pursuing his PhD degree in School of Electrical Engineering and Automation, Hefei University of Technology, Hefei, China. His research interests include 5G, wireless communication, Internet of Things, future generation spectrum, standardization and channel modeling. He is the recipient of the CSC scholarship and two best performance of the year awards.

He Yigang received the M.Sc. degree in electrical engineering from Hunan University, Changsha, China, in 1992 and the Ph.D. degree in electrical engineering from Xi'an Jiaotong University, Xi'an, China, in 1996. In 1990, he joined the College of Electrical and Information Engineering, Hunan University and was promoted to associate professor, professor in 1996, 1999, respectively. From 2006 to 2011, he worked as the director of the Institute of Testing Technology for Circuits and Systems, Hunan University. He was a senior visiting scholar with the University of Hertfordshire, Hatfield, U.K., in 2002. In 2011, he joined the Hefei University of Technology, China, and currently works as the head of School of Electrical Engineering and Automation, Hefei University of Technology. His teaching and research interests are in the areas of power electronic circuit theory and its applications, testing and fault diagnosis of analog and mixed-signal circuits, electrical signal detection, smart grid, satellite communication monitoring, sensor design and intelligent signal processing. On the above research areas, he has presided over a number of state-level projects research such as the National Natural Science Foundation of China, the State Key Program of National Natural Science Foundation of China the national key research and development plan "important scientific instruments and equipment development", the National High Technology Research and Development Program of China, the Major State Basic Research Development Program of China, etc. He has published over 300 journal and conference papers which was included more than 1000 times in Science Citation Index of American Institute for Scientific Information in the aforementioned areas and several chapters in edited books. Dr. He has been on the Technical Program Committees of a number of international conferences. He was the recipient of a number of national and international awards, prizes, and honors. For example, he was the winner of national outstanding youth science fund, China national excellent science and technology worker.

Yi Ruan was born in 1996. He graduated in 2017 with a bachelor degree of engineering from Hefei University of Technology. Currently, he is pursuing his PhD degree from same university. His present research interests include reliability analysis, fault diagnosis and residual life prediction of micro-electro-mechanical systems and new electronic components.