DEVICE CLASSIFICATION IN ROBOT ASSISTED SURGERY: A REVIEW

Meghana P. Lokhande

Department of Computer Engineering, Pimpri Chinchwad College of Engineering,Pune.
Research Scholar, Smt. Kashibai Navale College of Engineering, Pune, India.
meghna.ingole1983@gmail.com

Dipti Durgesh Patil

Department of Information Technology,
MKSSS's Cummins College of Engineering for Women, Pune, India
diptivt@gmail.com

Abstract: Internet of Things (IoT) domain gradually growing in information technology and telecommunications systems area considering its size and complexity. It is recognized as potential domain in IoT applications. New technologies need to anticipate this sharp increase in the number of varying smart devices. In current perspective, the IOT environment, which allows a huge network of things to communicate with each other, may face a number of technical and application problems, such as privacy concerns, security, sensor anonymity, decision support, a variety of device applications, and so on. In this review paper, goal is to study various frameworks for IoT device classification possible in Tele robotic surgery and summarizes the classification algorithm. Tele robotic surgery needs robust and beneficiary control techniques for providing efficient and precise alternative for medical surgeries. Time delays over network severely impact the stability in the surgery and eventually affect the performance of expert doctors. Also we analyze the problems encountered with the M2M connectivity of network devices.

Keywords: Device classification, Internet of Things (IoT), IoT challenges, M2M communication**.**

1. Introduction

Advances in communication technology will create an Internet of Things (IoT) environment. In IOT era, it has transformed the lives of many automated internet connected devices, from machines to machines (M2M) communications to decision-making to coordinate the use of interconnected intelligent devices [1]. M2M communication has emerged to provide device connectivity. It combines low-cost, reliable and scalable technologies with interconnected networks and remote controllable mechanical and electrical networks. Market condition and recent forecasts confirms that M2M adoption is rapidly increased. It needs to automate the monitoring and management processes in real life, also provide smart applications to improve live-work style [2].

M2M communication provides various applications such as monitoring the environment, security, energy and smart grid, building automation and home networks [1][4]. These applications create new business opportunities and features of M2M somewhat different than those of traditional networks [1][3]. To ensure communication between a large numbers of machines, the cost of the machines as well as connection must be low. Since most machines run on batteries, in which energy-saving methods are difficult task. When a machine receives data from another machine or perceives data from a physical environment (such as a sensor or a mobile device), M2M establishes communication without human intervention. As overall traffic per machine is more so maintaining an established connection is a difficult task.

IoT provided by the interrelated objects creates serious problems like data exchange security, privacy, devices heterogeneous sensors anonymity, decision support, etc. The fundamental problem with M2M communication is IoT devices are constantly increasing. Based on Ericsson, IoT study says in 2020 nearly 50 billion devices will be connected shown in Fig. 1. This creates serious problems in M2M communication in point of view of data security, and privacy [1] [4].

As more IoT devices are deployed, more information will be at risk. The rapid growth of IoT devices creates vulnerability which causes security attacks. The network of IoT is different in terms of devices, and services. Heterogeneity problems created due to the variety of data generated during M2M communications. Decision Support Systems is still the main problem of the inter-machine network, i.e. the IoT, because they are largely aimed at human intervention to reduce their communication time.

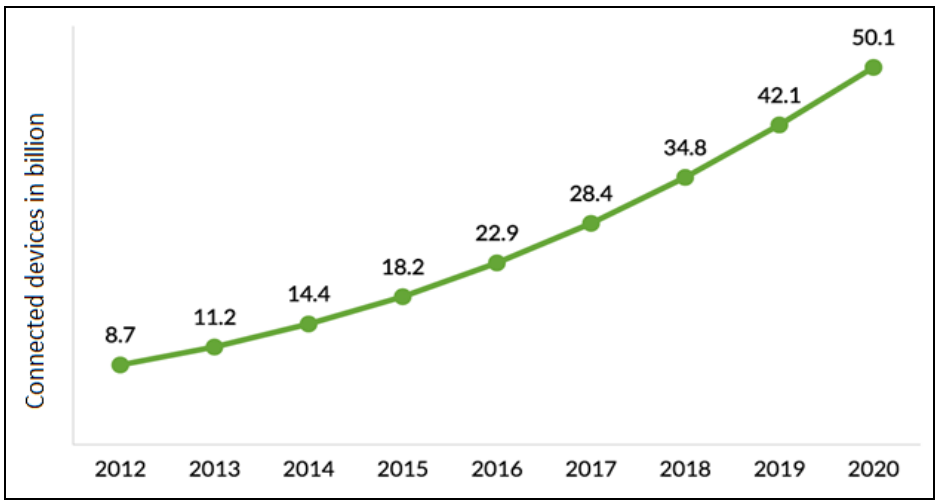

Fig. 1. Growth in Internet of Things Devices [1][4]

Autonomous M2M communication plays a crucial role in fulfilling this intelligent machine control mission [5]. The capability of M2M wireless communication can be used in tele robotics. Typical communication options possible are the service robot can be controlled inside a rescue robot [6] or a housing robot with potential access to a dedicated network. Tele-robotics is an integral part of the broader field of telemedicine. The main aim is to provide medical care for long distances and removes the need for both the doctor and the patient to be physically present in the same place. Consultation by far the possibility of diagnosis and treatment can greatly affect the life of patients with limited access to specialist health services [7]. Tele-robotics is practically lead by special doctors where there are no medical institutions or specialists. In addition to medical isolation, Tele-robotic is very important in eliminating medical issues in building countries, disaster places, and war areas where ongoing medical care's are not available or do not have time to shift the patient to the hospital [8].
Several researchers described IoT technology in Tele robotic surgery in different aspects. Using these facts, this study provides an analysis of some problems and certain technologies to overcome the problems encountered in related field.

1.1 IOT Devices Classification Based on Machine Learning

In today's scenario, more number of devices connecting to the internet. Tens of billions of devices work independently and communicates with servers on the internet [9]. IoT device classification can also be used to identify attackers and perform vulnerable IoT devices to analyze passive traffic networks in a wireless IoT network, even if the network is secured, to find the device type. The classification of the device also has some privacy issues. Once the device is identified, the current state of the device can be determined [10]. The IoT device classification makes use of header information. The function related classification is shown in [11]. In [12], an experiment was created to determine the type of device, which appears on a white list that it is not authorized. A data set that captures multi-day Internet of things traffic, analyzed network and published its own data set [13]. The automatic classification of devices from network traffic streams using learning algorithms discussed in[14]. In [15], a feature of the proposed approach for analyzing traffic networks using typical modes of operation, including IoT devices are developing a classification method. They also identified specific IOT devices with 95% accuracy. The Weka relies on a large number of algorithms for classification (to label the data set) that can be used as tool, and the RF algorithm reaches a high accuracy of more than 95%. In [16], a unified system of fundamental statistical tests for ranking features was developed. They use classification Trees, Random forests, and Bagging classifiers. They show that bagging algorithm with eight features show 95% of accuracy. The random forest performance is unstable.
The author in [17] discussed four classification algorithms that are used, such as KNN, NB, SVM, RF are applied to a data set containing the specifications of known devices for classification. They compare the classifiers using performance metrics and shows that the KNN is the best classifier. Researcher [18] provides a way of automatic classification of devices on the Internet of things to identify new, invisible devices. This abundance of information is driven by the movement of the internet, which is also a typical attribute of the network. In this article, they first determine the set of features that distinguish it from the RAW network traffic flow, and then propose LSTM-CNN model for classification of devices. It shows the 99.7 % accuracy.
In [19] presented development of a reliable framework basis for classifying devices of the IoT using characteristics of traffic received at the network layer. They first instrumented live lab device with 28 IoT

devices in smart environment emulation mode. The authors develop a multistage classification algorithm based on machine learning for classifying specific IOT devices. The system architecture of the multi-stage classifier for IoT device classification shows in Fig. 2. This architecture first feeds each multivalued attribute to the corresponding stage-0 classifier as a "word bag". A word packet is a matrix in which a row is labeled as an instance and a column is a unique word. As shown in the figure, 356, 421, and 54 unique words were observed for domain names, remote port numbers, and cipher suite strings. The stage 0 is analyzes each packet using a Naive Bayes polynomial classifier and sent to the stage 1 classifier for production of final output. Training instances are distributed in various classes, that time Naïve Bayes algorithm is very useful [20].

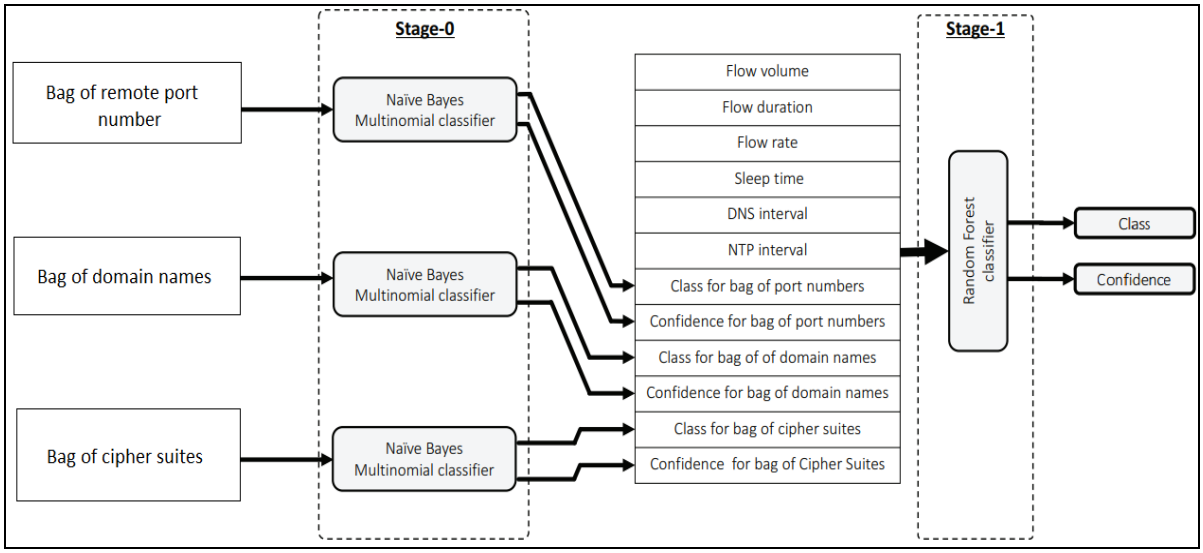

Fig. 2. Multi-stage classifier for IoT device classification [15]

Stage 1 classifier, which accepts all quantitative attributes and the product pair of each stage 1 classifier. Since the Stage-1 attribute cannot be separated linearly and the output of the stage-0 classifier is rated, a random Forest classifier stage-1 is used. Another reason for choosing a random forest is that it is very resistant to reconstruction compared to other decision tree classifiers. The proposed method in [21] recognizes network traffic data by analyzing IoT devices. To describe behavior of the network, the features set, which selected the effectiveness of the use-type indication for visualization, differ depending on the occurrence of the Traffic Network. Classification and network traffic using different machine learning algorithms such as RF, DT, SVM, KNN, ANN, and GNB. They compare the entire algorithm 99% shows an RF classifier. We have reviewed the paper for classifying the IoT devices using various machine learning classifiers shows in Fig 3.

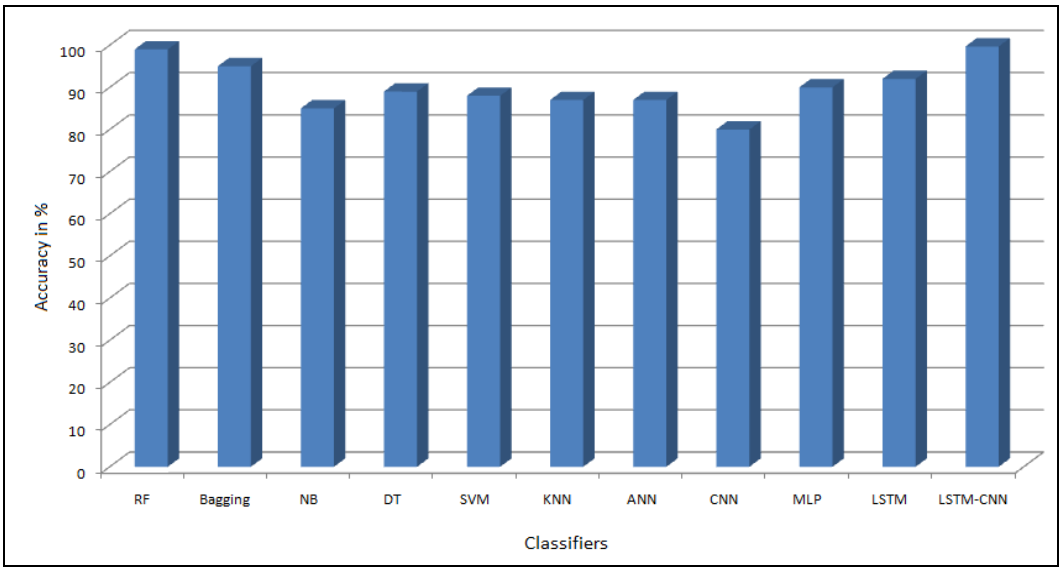

Fig. 3. Accuracy of classifying the IoT devices

The author uses RF [15, 16, 17, 19, 21], Bagging [15], NB [17, 19], DT [21], SVM [17, 21], KNN [17, 21], ANN [21], CNN [21], MLP [18], LSTM [18], and LSTM-CNN [18] classifiers. Fig. 4 shows that the RF (99%) and LSTM-CNN (99.7%) classifiers accuracy of classifying the IoT devices is more than other classifiers.

1.2 Machine to Machine Communication Architecture in IoT

Network of M2M contain various nodes communication which involves basic entity as a machine (device). Energy efficiency is main problem because several devices work with batteries. These several devices produce a big data with different format, size and periods. Communication is done without human interference, and it requires stability of network.

Tele-presence assumes that all information of the remote environment is inherently provided by the operator [22]. The main connection is created in master and slave communication to called M2M communication through the internet. The length of nodes from each other is vast; the data transfer delay may disturb the system and ultimately affect the performance of the healthcare professional. The communication quality and performance metrics are important in telerobotic M2M communication. Security and privacy are very important aspects of any communication. Network performance is reduced if a malicious node is present in the network. The incorrect behavior of the node presents malicious packet drop attacks which disturb the routing rules, data transmission is corrupted, packets are dropped and data is lost. So the presented systems provide a low delay and secure communication for the telerobotic community and data security.

In 2009, the European telecommunications standards institute (ETSI) established the M2M technical Committee to develop M2M communications architecture in IoT in Fig. 4 [2][4]. The M2M domain connects a several node and gateway (GW), allowing for a variety of automated services. Each node includes a variety of functions such as data preprocessing, data acquisition; communication interfaces unique addresses, data storage, and power supplies.

They can make smart decisions and transfer data to GW in single-jump or multi-jump mode. Embedded nodes gathering packets and it can manage packages intelligently, and to provide effective ways in packages sent to remote server through networks. Network consists of heterogeneous attachment points. Here, a convergent heterogeneous network provides optimal probing packets for effective and reliable channel transfer in M2M application areas.

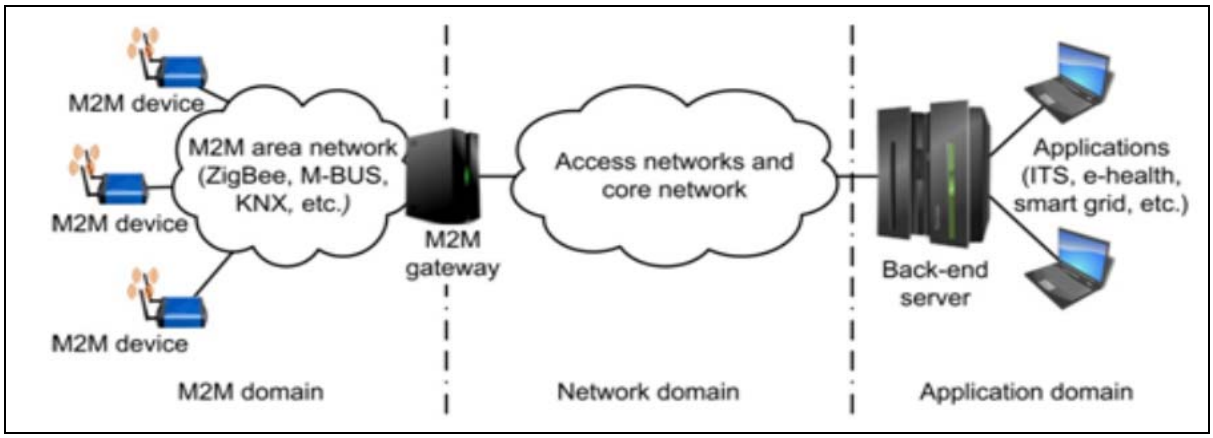

Fig. 4. Machine to machine communication architecture in IoT [4]

Finally, the application area classified into transportation, business, real-time services, home, remote management, logistics, remote monitoring, etc. The important component of M2M communication is back-end server. To all devices the integrated point is created for data collection. M2M devices may be stationary, such as household appliances or mobile devices. Devices are connected to main network using Access network. A wired solution capable of the highest data transfer speed, reliability, security, and low latency, but all M2M connections as a result of it can be lost. However, low data transfer rates, weak security, and serious interference mentioned in the universal infrastructure create limitations on the use of M2M.

2. Related Work

This research aims to examine the literature, identify current trends, and describe challenges that threaten the spread of IoT, presents open research challenges and future directions. IoT requires ubiquitous connectivity to

all devisees but due to access protocols and heterogeneity the IoT network became a very large, so it is difficult to manage. Comparative study on device classification used in Tele robotic surgery shown in table 1. In [23], constructed a network based on Software Defined Network (SDN). In [24] propose a scheme for allocation of the resources in D2D communication. Author in [25] provides the cutting edge of cognitive M2M communication in terms of protocol stacks. In [26], implements M2M gateway SCL (GSCL) and application, and the decision in the development process were evaluated experimentally on the performance of the smart phone in different configurations. The application developers are the ones that use the libraries that they have developed for M2M applications. Also, M2M network application (NAs) is used to show how the operation is performed in M2M GWs.

Table 1 Comparative study on device classification used in Tele robotic surgery

Sr. No.	Author Name	Method	Limitation
1	Huand and L. Zang [23]	Managing devices and dynamically constructing networks based on Software Defined Network (SDN).	Not focuses on distributed devices.
2	Huang. J, Yan. H Yin. Y, and Duan, Q [24]	Propose a allocation resource scheme intercell D2D communication.	The resource is assigned at a limited range.
3	C. Pereira, A. Pinto and A. Aguiar [26]	Implement M2M gateway, SCL and application in Smartphone.	Poor battery life and GIP support for few types of legacy devices.
4	A. Nessa, and M. Kadoch [27]	A set of common network source encoding systems for reliable data transfer between M2M and eNB devices is presented.	Lack of central administrative control, mobility of the nodes and error-prone.
5	H. Jin, B. jung, J. Seo, and W. Toor [29]	Proposes an ABC algorithm for solving the congestion problem of large M2M communication in the LTE system	Early convergence in the later search period and sometimes cannot meet the requirements of the optimum value of accuracy.
6	J. Mass, S. srirama and C. Chang [30]	Implement D2D-based business process execution.	It fails to manage integrated information systems in IoT.
7	Azariadi. D, Tsoutsouras. S, Soudris. V, Xydis. D [31]	IoT based embedded system is proposed.	Signal to noise ratio is poor.
8	J. Huang, C. xing, and F. Hen [28-33]	Present M2M communication access control model.	The starvation of the low priority flow, and delay.
9	Liu. X, and Ansari. N [34]	Proposed dual-battery architecture for MTDs will meet the needs for green energy harvesting and IoT capabilities.	Infrastructure is thinly spread.
10	Z. li and J.Gui [35]	Proposes a hybrid TDMA-NOMA and an energy-efficient resource allocation scheme for LTE-a compatible M2M networks.	Receiver complexity and error propagation are high.
11	H.Zang, B. Di, K. Bian and Z. Han [36],	Cycle-based mechanism for fair unlicensed frequency distribution and optimized the minimum transmission energy consumption	A limitation is the cost of licensed spectrum resources.
12	N. Shahin, R. ali, and Y.kim [38]	Propose a hybrid-slot CSMA/CA time-division multi-way access (TDMA) (HSCT) media access control (MAC) protocol.	Overlap of spectrum sensing and analysis with actual device IOT transmission.

13	Chae. S, Cho. S, Kim. S, and Rim. M [39]	Improved random access performance with coded random sampling technology with several numbers of copies per packet.	Couldn't find the optimal number of copies.
14	Panigrahi. B, Rath. H, and Sinha. A [40],	Proposes M2M devices to bypass gateway nodes and use proximity M2M devices.	Signaling and security limitations in device link analysis.
15	M. Elsaadany, and W. Hamouda [41],	Release 13 (Rel-13) provides an overview of LTE-A CAT-M. New specifications for various physical channels.	Hardware limitation and they operate only single channel.
16	J. Lianghai, B. Han, and M. Liu [42]	The proposed network control side link communication for cellular network is assisted by the mMTC service.	Challenging to control level of interference.

In [27] examines heterogeneous M2M networks wherein clustered CHs are sent directly to eNB with the help of relays, to address the harmful effects of radio Fading Channels. In [28] proposed protocol-protected repeater interface for D2D communication between LTE-in the UEs.

Researchers in [29], proposed to use two Bayes-ACB algorithms to find active devices. A commercial LTE system, eNodeB can immediately detect whether a given introduction is sent, but idles BS in each slot immediately.

Author in [30], proposes system design for a D2D-based business process. They apply this plan in the field of intelligent logistics to enable the control of intelligent products. Presented product tracking solution reacts to events as soon as an event occurs and produces traces of tracked execution history. Healthcare is rapidly increased in Information Technology Application. The IoT allow patients to be remotely monitored. The author in [31] suggested a much-immersed system. They're developing algorithms for ECG analysis and classification of heart rate diagnosis.

The reliable, efficient and scalable M2M communication is an important factor in IoT network. In paper [32] examines and presents the studies of M2M communication based on energy collection and assuming bond flaws, and determines energy collection and storage properties. In [33] proposes access control algorithm for system model through which access collisions are prevented, and the quality of the service was improved. In [34] author offers dual-battery architecture to extend the capabilities of MTDs while simultaneously collecting green energy and IoT features. In [35], proposes a hybrid TDMA-NOMA and an energy-efficient resource allocation scheme for LTE-a compatible M2M networks.

Author in [36] presented the design of duty cycle based on the mechanism for the fair permission to obtain spectrum sharing, optimal minimum transmission of energy consumption and scheduled IoT devices. The network is ad hoc in nature [37], allowing easily "connecting & transmitting" processes of the device. Given the centralized computing storage server, the user sets up devices and they provide most up-to-date data. They create the current registered living ecosystem for the built ecosystem. In [38] suggests hybrid-slot CSMA / CA time-division multi-way access (TDMA -) (HSCT) MAC (media access control) protocol for efficient and large - scale registration of IoT devices (up to 8000) in M2M networks.

In [39] processed to improve performance random access using encoded random access technology when MTC devices use different package lengths according to channel conditions. In [40], describe how M2M devices bypass gateway nodes. In [41], the 3GPP standard LTE-A has recently been included in a new category, user equipment support MTC. They offer minimum cost and energy. In [42] proposed scheme of the network control side link communication that can be applied to mMTC service for the support by the cellular network and the context recognition algorithm. In [43], proposes AKA protocol for use of terminal equipment for M2M data transfer. Authors in [44], propose a AUD scheme for performance improvement of NOMA system to utilize the data measurements.

In [39] processed to improve performance random access using encoded random access technology when MTC devices use different package lengths according to channel conditions. In [40], describe how M2M devices bypass gateway nodes. In [41], the 3GPP standard LTE-A has recently been included in a new category, user equipment support MTC. They offer minimum cost and energy. In [42] proposed scheme of the network control side link communication that can be applied to mMTC service for the support by the cellular network and the context recognition algorithm. In [43], proposes AKA protocol for use of terminal equipment for M2M data transfer. Authors in [44], propose a AUD scheme for performance improvement of NOMA system to utilize the data measurements. In the industrial IOT era, it is important to create an industrial IOT environment in which

sensors; actuators, gateways, and other devices can autonomously exchange information without human intervention.

In article [45], propose to simplify the authentication scheme of this machine, the authorization limited resources to provide IoT solutions for safe integration into future production engines. In [46], author summarizes access control approaches for accessing resources of authenticated devices.

3. The Security, Challenges, and Attacks in IOT

In IoT based applications important part is security. This is why computer-aided design (CAD) technology adopts to a lower cost solution compared to other technology [47]. Security goal of IoT devices is the integrity and availability of confidentiality [48][49]. New technology will be used for comprehensive security and privacy management.

Main challenge of security is a secure health system and relocation system to save lives and prevent financial losses. IoT layer builds all aspects of security-related issues with long-term security attacks. Security requirements vary by Application. Other network layer problems include denial of Service (DoS), espionage, middleman, heterogeneity, node jamming. The lowest layer in IOT architecture facing a security challenge in cyber attacks. Researchers believe that the IoT architecture layer, which has a large impact on security attacks, can be used to harden nodes, embed malicious codebases, fake nodes, network problems, data access, and so on [49][50]. The security of the Internet of things depends on: data confidentiality, privacy, and trust. The objectives illustrated in table 2 the three IoT security challenges that need to be achieved better if the three issues mentioned above are used effectively and reliably [51].

The possibility of surgeons violating the surgical system complicates the issue of legal liability follow during the procedure. In the event of an attack like changing intentions or manipulation, the robots are not directly accessed by surgeons; they operate robots based on data received. Tactile feedbacks are altered which can harm patient health. It can be argued surgeons need to be aware that tactile feedback has been fixed, and then the result of a lawsuit regarding negligence may be amplified. The threat to the security of telerobotic is a growing concern for the surgical community, as an installed attack can cause the robot to break or damage.

In [52][53] side-channel attacks are being investigated in 3D printers. The researcher's examine the 3D printing mechanism, searched the side channels through the Smartphone, and compared the 3D printer to the side-channel attack. In [54] node tempering attack all sensor networks are physically access and control all over the sensor nodes. Software modification attack [54], attackers manipulate the software's. Attack node generates false distorted information that violates the integrity of the data. The Hardware Trojans attack [55], of the Integrated Circuit device performs malicious monitoring function. Destruction of M2M devices attacks [56] when used in inaccessible locations, M2M devices can be easily stolen or damaged.

In [57] spooling an attack, the attacker can impersonate the network member and control the network's operations. For example, an opponent who manages to falsify an intellectual ID can force their owner to pay the opponent's costs. Even worse it appears as a server, because it can trigger a launch attack [58]. The attackers make an unauthorized M2M device. DoS [59] the attacker wants to make computer or network resources available to the intended users. Jammers can always send a radio signal to prevent legitimate access to the channel. In [60] the relay attack, attacker passed the message so that the sender would believe it was near the transmitter. Routing protocols [61] affect destination routing decisions.

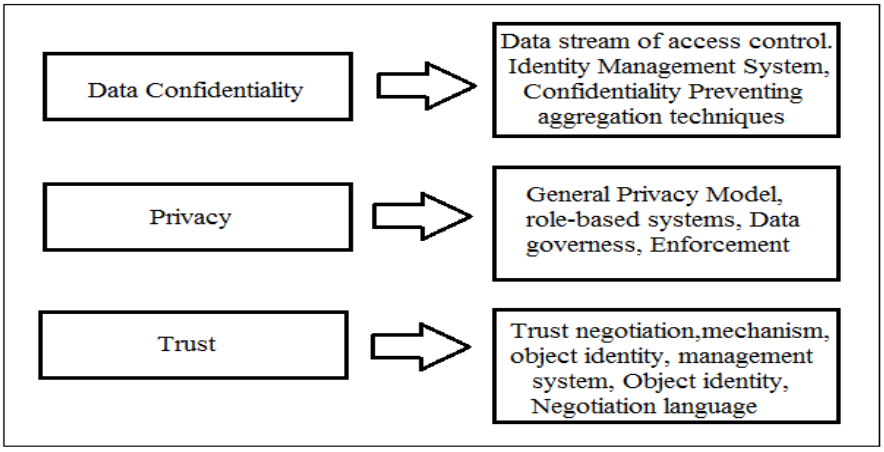

Fig. 5. Security challenges of IoT [46]

Data attacks are aimed at exchanging information. Most attacks are eavesdropping attacks [62], the network to obtain information about the data that the attacker sent on hearing the target communication channel. A malicious attacker could compromise the user's privacy and infer the user's habits, health, etc. In a traffic analysis attack [63], the attacker passively monitors the transmission of the communication patterns and participants to identify the purpose.

Table 2 The attacks, vulnerabilities, and requirement for security in IoT

Attacks	Vulnerability	Requirement of security
Node tampering	WC, PS, RC	C, AU
Denial of Service (DoS)	WC, RC, S	A
Destruction of M2M device	PS	I, A
Side-channel attacks	PS	C
Software modification	PS,RC,S	A, I, AU
Relay attacks	WC,S,RC,DS	I, AU
Selective forwarding	GC,DS,S	I, AU, A
Hardware Trojans	PS	C, I
Eavesdropping	WC, RC, GC	C
Traffic Analysis	WC	C
Routing protocol attacks	RC,DS,S	A, I
Spoofing	WC, RC, S, GC,OSP	AU
Integrity attack	RC, WC	I

This attack is increased because of wireless and internet-based communication in M2M devices. In the integrity of the attack, data is leaked during the transmission or storage of the device memory on the application server. In [64] authors discussed security issues and attack scenario on devices in Internet of Things. In [65] the Selective forwarding attack is discussed, in this attack the receiver drops some received packets. Table 2 lists the Attacks, vulnerabilities and requirements of security. The vulnerabilities are Wireless communication (WC), Resource constraint (RC), Software (S), Physical security (PS), Global Connection (GC), Open Standard Protocol (OSP), and Delay sensitive (DS). The security requirements are Confidentiality (C), Integrity (I), Authentication (AU), and Availability (A). That provides a secure M2M communication environment that requires a security mechanism to counter security threats.

4. Conclusion

The Internet of things is the world's current trend technology, which combine Information Technology and real-life things. IoT is technology that makes human activities better and more convenient. Research focused on the classification of IOT devices in Tele robotic surgery and summarizes the classification algorithm. The entire wireless telerobotic information system includes computing for robotic operation and M2M communication for two-way purposes, robotic control, and communication with the environment. Also the multi-stage machine learning based classification framework for IOT device classification is discussed. M2M communication is mainly handled in connection with objects in IoT. In this article security threats to M2M networks based on these vulnerabilities are classified. In addition, the vulnerabilities used in each attack were identified, as well as security requirements to combat them. Our future work will be focused on building highly feasible IoT architectures for tele robotic surgery, generating effective device classification and M2M communication between highly connected physical objects, and integrating all the beneficial mechanisms provided to overcome IoT problems, providing upgraded neural analysis and high-level communication between interconnected devices.

5. References

[1] Kim Thuat Nguyen; Maryline Laurent; Nouha Oualha;(2015): Survey on Secure communication protocols for the Internet of Things.Elsevier Adhoc Networks. Volume 32 Issue C, 17-31.
[2] Dohler M.; Swetina J.; Alexiou A.; Wang C.; Martigne P.; Zheng K. (2014) : Machine-to Machine Technologies & Architectures. 1-3 doi:10.1109/SURV.2014.012114.00000.
[3] Zhao M.; Kumar A.; Ristaniemi T. ; Chong P. H. J.(2017) : Machine to Machine communication and research challenges: A survey. Wireless Personal Communications 97 (3), 3569–3585.
[4] Kim, J.; et al.(2014) : M2M Services Platforms: Survey, Issues, and Enabling Technologies. IEEE Communications Surveys & Tutorials. 16 (1), 61-76.
[5] Kaur, T.; Kumar, D.(2019): Computational intelligence-based energy efficient routing protocols with QoS assurance for wireless sensor networks: a survey. Int. J. Wireless and Mobile Computing. Vol. 16, No. 2, pp.172–193.

[6] Tin-Yu Wu ; Yu-Wei Wu.(2020): An energy-efficient low-SAR path finding mechanism for WBAN. International Journal of Ad Hoc and Ubiquitous Computing. vol. 34, Issue 4, pp. 199-207.
[7] Yang, G.Z. ; Cambias, J. ; Cleary, K. ; Daimler, E.; Drake, J. ; Dupont, P. E.; Hata, N. ; Kazanzides, P. ; Martel, S. ; Patel R. V. ; et al.(2017): Medical robotics regulatory . Science Robotics. vol. 2, no. 4, p. 8638.
[8] Litjens, G. ; Kooi, T. ;. Bejnordi, B. E ;. Setio, A. A. A; Ciompi, F. ; Ghafoorian, M. ; Van Der Laak, J. A. ; Van Ginneken, B. ; Sanchez, C. I. (2017): A survey on deep learning in medical image analysis. Medical Image Analysis. vol. 42, pp. 60–88.
[9] Popular Internet of Things forecast of 50 billion devices by 2020. https://goo.gl/6wSUkk.
[10] Acar; Fereidooni, H. ; Abera, T. ; Sikder, A. K. ; Miettinen, M. ; Aksu, H. ; Conti, M. ; Sadeghi, A.R. ; Uluagac, A. S. (2018): Peek-a-boo: I see your smart home activities, even encrypted! CoRR.
[11] Miettinen, M.; Marchal, S. ; Hafeez, I. ; Asokan, N. ; Sadeghi, A.R. ; Tarkoma, S. (2017) : Iot sentinel: Automated device-type identification for security enforcement in iot. in Distributed Computing Systems (ICDCS) IEEE 37th International Conference on. IEEE. pp. 2177– 2184.
[12] Meidan, Y.; Bohadana, M.; Shabtai, A.;Ochoa, M.; Tippenhauer, N. O.; Guarnizo, J. D.; Elovici, Y.(2017): Detection of unauthorized *IOT* devices using machine learning techniques. CoRR. vol. abs/1709.04647, http://arxiv.org/abs/1709.04647.
[13] Sivanathan; Sherratt, D.; Gharakheili, H. H. ; Radford, A. ; Wijenayake, C. ; Vishwanath, A. ; Sivaraman, V.(2017) Characterizing and classifying iot traffic in smart cities and campuses. in Computer Communications Workshops (INFOCOM WKSHPS) IEEE Conference on. IEEE. pp. 559–564.
[14] Bai, L. ; Yao, L. ; Kanhere, S. S. ; Wang, X. ; Yang, Z.(2018) : Automatic device classification from network traffic streams of internet of things. arXiv preprint arXiv:1812.0988.
[15] Sivanathan, A. ; et al. (2017) :Characterizing and classifying IoT traffic in smart cities and campuses. IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS). pp. 559-564, doi: 10.1109/INFCOMW.2017.8116438.
[16] Desai, B. A. ; Divakaran, D. M. ; Nevat, I. ; Peter G. W. ; Gurusamy, M. (2019) : A feature-ranking framework for IoT device classification. 11th International Conference on Communication Systems & Networks (COMSNETS). pp. 64-71, doi: 10.1109/COMSNETS.2019.8711210.
[17] Mavrogiorgou A.; Kiourtis A.; Kyriazis D. (2017): A Comparative Study of Classification Techniques for Managing IoT Devices of Common Specifications. In: Pham C., Altmann J., Bañares J. (eds) Economics of Grids, Clouds, Systems, and Services. GECON. Lecture Notes in Computer Science, vol 10537.
[18] Bai, L.; Yao, L. ; Kanhere, S. S. ; Wang X. ; Yang, Z.(2018) : Automatic Device Classification from Network Traffic Streams of Internet of Things. IEEE 43rd Conference on Local Computer Networks (LCN). pp. 1-9, doi: 10.1109/LCN.2018.8638232.
[19] Sivanathan; et al.(2019) : Classifying IoT Devices in Smart Environments Using Network Traffic Characteristics. in IEEE Transactions on Mobile Computing. vol. 18, no. 8, pp. 1745-1759, doi: 10.1109/TMC.2018.2866249.
[20] McCallum ; Nigam, K. (1998) : A Comparison of Event Models for Naive Bayes Text Classification. AAAI/ICML-98 Workshop on Learning for Text Categorization. pp. 41–48.
[21] Shahid, M. R. ; Blanc, G. ; Zhang Z. ; Debar, H.(2018): IoT Devices Recognition Through Network Traffic Analysis. IEEE International Conference on Big Data (Big Data), Seattle, WA, USA. pp. 5187-5192, doi: 10.1109/BigData.2018.8622243.
[22] Shvets, A. A. ; Rakhlin,A.; Kalinin,A.A.; Iglovikov,V.I.(2018): Automatic instrument segmentation in robot-assisted surgery using deep learning. in Proceedings of IEEE International Conference on Machine Learning and Applications (ICMLA). IEEE. pp. 624–628
[23] Huang,H.; Zhu J.; Zhang, L.(2014): An SDN_based management framework for IoT devices. 25th IET Irish Signals & Systems Conference 2014 and 2014 China-Ireland International Conference on Information and Communications Technologies (ISSC 2014/CIICT 2014). pp. 175-179, doi: 10.1049/cp.2014.0680.
[24] Huang,J.; Yin,Y.; Duan,Q.; Yan,H.(2015): A Game-Theoretic Analysis on Context-Aware Resource Allocation for Device-to-Device Communications in Cloud-Centric Internet of Things. 3rd International Conference on Future Internet of Things and Cloud. pp. 80-86, doi: 10.1109/FiCloud.2015.125.
[25] Aijaz A.; Aghvami, A.H. (2015): Cognitive Machine-to-Machine Communications for Internet-of-Things: A Protocol Stack Perspective. in IEEE Internet of Things Journal. vol. 2, no. 2, pp. 103-112, doi: 10.1109/JIOT.2015.2390775.
[26] Pereira,C.;Pinto,A.; Aguiar,A.; Rocha,P.;Santiago F.; Sousa,J.(2016): IoT interoperability for actuating applications through standardized M2M communications. IEEE 17th International Symposium on A World of Wireless, Mobile and Multimedia Networks (WoWMoM). pp. 1-6, doi: 10.1109/WoWMoM.2016.7523564.
[27] Nessa, A.; Kadoch,M. (2016) : Joint Network Channel Fountain Schemes for Machine-Type Communications Over LTE-Advanced. in IEEE Internet of Things Journal. vol. 3, no. 3, pp. 418-427, doi: 10.1109/JIOT.2015.2497311.
[28] Steri,G.; Baldini,G.; Fovino,I.N.; Neisse,R.; Goratti, L.(2016): A novel multi-hop secure LTE-D2D communication protocol for IoT scenarios. 23rd International Conference on Telecommunications (ICT). pp. 1-6, doi: 10.1109/ICT.2016.7500356.
[29] Jin,H.; Toor,W.T.; Jung B.C.; Seo, J.(2017): Recursive Pseudo-Bayesian Access Class Barring for M2M Communications in LTE Systems. in IEEE Transactions on Vehicular Technology. vol. 66, no. 9, pp. 8595-8599, doi: 10.1109/TVT.2017.2681206.
[30] Mass,J.; Chang, C.; Srirama, S.N.(2016) : WiseWare: A Device-to-Device-Based Business Process Management System for Industrial Internet of Things. IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data. pp. 269-275, doi: 10.1109/iThings-GreenCom-CPSCom-SmartData.2016.69.
[31] Azariadi; Dimitra; et al.(2016): ECG signal analysis and arrhythmia detection on IoT wearable medical devices. 5th International Conference on Modern Circuits and Systems Technologies (MOCAST) IEEE . 1-4.
[32] Rinne, J. ; Keskinen, J. ; Berger, P. R. ; Lupo, D. ; Valkama,M.(2016): Feasibility and fundamental limits of energy-harvesting based M2M communications. IEEE 27th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC). pp. 1-6, doi: 10.1109/PIMRC.2016.7794605.
[33] Huang,J.; Xing,C.; Shin,S.Y.; Hou,F.; Hsu,C.(2018): Optimizing M2M Communications and Quality of Services in the IoT for Sustainable Smart Cities. in IEEE Transactions on Sustainable Computing. vol. 3, no. 1, pp. 4-15, doi: 10.1109/TSUSC.2017.2702589.
[34] Liu, X.; Ansari, N.;(2018) : Dual-Battery Enabled Green Proximal M2M Communications in LPWA for IoT. IEEE International Conference on Communications (ICC). pp. 1-6, doi: 10.1109/ICC.2018.8422203.
[35] Li, Z.; Gui, J.; (2019): Energy-Efficient Resource Allocation With Hybrid TDMA–NOMA for Cellular-Enabled Machine-to-Machine Communications. in IEEE Access. vol. 7, pp. 105800-105815, doi: 10.1109/ACCESS.2019.2931657.
[36] Zhang,H.;Di,B.; Bian,K.;Song,L.(2019): IoT-U: Cellular Internet-of-Things Networks Over Unlicensed Spectrum. in IEEE Transactions on Wireless Communications. vol. 18, no. 5, pp. 2477-2492, doi: 10.1109/TWC.2019.2904269.
[37] Das,D.; Sarkar, S.(2018): Machine-to-Machine Learning based framework for ad-hoc IOT ecosystems. International Conference on Computational Techniques, Electronics and Mechanical Systems (CTEMS).pp. 431-436, doi: 10.1109/CTEMS.2018.8769148.

[38] Shahin,N.; Ali, R.;Kim,Y.(2018): Hybrid Slotted-CSMA/CA-TDMA for Efficient Massive Registration of IoT Devices. in IEEE Access. vol. 6, pp. 18366-18382; doi: 10.1109/ACCESS.2018.2815990.
[39] Chae,S.;Cho,S.;Kim,S.;Rim,M.(2016): Coded random access with multiple coverage classes for massive machine type communication. International Conference on Information and Communication Technology Convergence (ICTC). pp. 882-886, doi: 10.1109/ICTC.2016.7763321.
[40] Panigrahi,B.;Rath,H.K.; Ramamohan, R.; Simha,A.(2016): Energy and spectral efficient direct Machine-to-Machine (M2M) communication for cellular Internet of Things (IoT) networks. International Conference on Internet of Things and Applications (IOTA). pp. 337-342, doi: 10.1109/IOTA.2016.7562748.
[41] Elsaadany,M.;Hamouda, w.(2017): The new enhancements in LTE-A Rel-13 for reliable machine type communications. IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC). Montreal. QC. pp. 1-5, doi: 10.1109/PIMRC.2017.8292399.
[42] Lianghai,J.; Han,B.; Liu,M.; Schotten,H.D.(2017): Applying Device-to-Device Communication to Enhance IoT Services. in IEEE Communications Standards Magazine. vol. 1, no. 2, pp. 85-91, doi: 10.1109/MCOMSTD.2017.1700031.
[43] Parne,B.L.; Gupta, S.; Chaudhari,N.S.(2018): SEGB: Security Enhanced Group Based AKA Protocol for M2M Communication in an IoT Enabled LTE/LTE-A Network. in IEEE Access. vol. 6, pp. 3668-3684, doi: 10.1109/ACCESS.2017.2788919.
[44] Lim,G.;Ji,H.;Shim,B.(2018): Hybrid Active User Detection for Massive Machine-type Communications in IoT. International Conference on Information and Communication Technology Convergence (ICTC). pp. 1049-1052, doi: 10.1109/ICTC.2018.8539661.
[45] Esfahani,A.; et al.(2019): A Lightweight Authentication Mechanism for M2M Communications in Industrial IoT Environment. in IEEE Internet of Things Journal. vol. 6, no. 1, pp. 288-296, doi: 10.1109/JIOT.2017.2737630.
[46] Lokhande, M.; Patil,D.(2019): Access control approaches in Internet of Things. International Journal of Computer Science and Engineering. Vol. 7, Issue 5, E-ISSN: 2347-269.
[47] Silva,B.N.; Khan,M.; Han,K.(2017): Internet of Things: A Comprehensive Review of Enabling Technologies, Architecture, and Challenges. IETE Technical Review. pp. 1- 16.
[48] Farooq,M.;Waseem,M.; Khairi,A.;Mazhar,S.(2015): A critical analysis on the security concerns of internet of things (IoT). International Journal of Computer Applications. vol. 111.
[49] Lin,J.; Yu,W.; Zhang,N.;Yang,X.;Zhang,H.; Zhao,W.(2017): A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications. IEEE Internet of Things Journal.
[50] Ali,I.; Sabir,S.; Ullah,Z.(2016):. Internet of Things Security, Device Authentication and Access Control: A Review. International Journal of Computer Science and Information Security. vol. 14, p. 456.
[51] Miorandi,D.; Sicari,S.;. De Pellegrini,F.; Chlamtac,I.(2012): Internet of things: Vision, applications and research challenges. Ad Hoc Networks. vol. 10, pp. 1497-1516.
[52] Faruque,A.; Abdullah,M.; Chhetri,S.R.;Canedo,A.; Wan,J.(2016): Acoustic side channel attacks on additive manufacturing systems. in Proceedings of the 7th International Conference on Cyber-Physical Systems. p. 19.
[53] Song,C.; Lin,F.; Ba,Z.; Ren,K.; Zhou,C.; Xu,W.(2016): My Smartphone Knows What You Print: Exploring Smartphone-based Side-channel Attacks Against 3D Printers. in Proceedings of the ACM SIGSAC Conference on Computer and Communications Security. pp. 895-907.
[54] Qabulio,M.; Malkani,Y.A.; Keerio,A.(2016): A framework for securing mobile wireless sensor networks against physical attacks. International Conference on Emerging Technologies (ICET). pp. 1-6.
[55] Jalalitabar,M.; Valero,M.;Bourgeois, A.G.(2015): Demonstrating the Threat of Hardware Trojans in Wireless Sensor Networks. 24th International Conference on Computer Communication and Networks (ICCCN), Las Vegas. pp. 1-8.
[56] Finogeev,A.; Finogeev,A.(2017): Information attacks and security in wireless sensor networks of industrial SCADA systems. Journal of Industrial Information Integration. vol. 5, pp. 6-16.
[57] Barki,A.;Bouabdallah,A.; Gharout,S.; Traor,J.(2016): M2M Security: Challenges and Solutions. IEEE Communications Surveys and Tutorials. vol. 18, no. 2, pp. 1241-1254.
[58] Zhao,C.; Huang,L.; Zhao,Y.; Du,X.(2017): Secure Machine-Type Communications toward LTE Heterogeneous Networks. IEEE Wireless Communications. vol. 24, no. 1, pp. 82-87.
[59] Hancke,G.P.; Mayes,K.E.; Markantonakis,K.(2009): Confidence in smart token proximity: Relay attacks revisited. Computers & Security. vol. 28, no. 7 pp. 615-627.
[60] Dong,W.; Liu,X.(2015): Robust and Secure Time-Synchronization Against Sybil Attacks for Sensor Networks. IEEE Transactions on Industrial Informatics. vol. 11, no. 6, pp. 1482-149.
[61] Sridhar,S.; Hahn,A.; Govindarasu,M.(2012): Cyberphysical system security for the electric power grid. Proc. IEEE. vol. 100, no. 1, pp. 210224.
[62] Ren,W.; Yu,L.;Ma,L.; Ren,Y.(2013): RISE: A RelIable and SEcure scheme for wireless Machine to Machine communications. Tsinghua Science and Technology. vol. 18, no. 1, pp. 100-117.
[63] He,D.; Chan,S.; Qiao,Y.; Guizani,N.(2018): Imminent Communication Security for Smart Communities. IEEE Communications Magazine. vol. 56, no. 1, pp. 99-103.
[64] Lokhande,M.; Patil,D.(2020): Security Threats In M2M Framework Of Iot. International Journal of Advanced Science and Technology. vol. 29, No. 8, pp. 1809-1823.
[65] Jhaveri,R.H.;Patel, S.J.; Jinwala,D.C.(2012): DoS Attacks in Mobile Ad Hoc Networks: A Survey. Second International Conference on Advanced Computing & Communication Technologies. Rohtak. Haryana. pp. 535-541.

Author's Profile

Meghana P. Lokhande is Assistant Professor in Computer Engineering Department at Pimpri Chinchwad College of Engineering, Pune. She earned her MTech degree from Bharati Vidyapeeth Deemed University College of Engineering, Pune. Now she is doing PhD in Computer engineering. She has published papers in International and National journals.

Dr. Dipti D. Patil is Associate Professor in Information Technology Department at MKSSS's Cummins College of Engineering for Women, Pune. She earned her doctorate in the year 2014 from Sant Gadgebaba Amravati University in Computer Science and Engineering. She pursued her UG and PG Computer Engineering from Thadomal Shahani Engineering College, Bandra of Mumbai University in 2002 and 2008 respectively. She has authored books in areas of Data Structures and Mobile healthcare. Dr. Dipti has published many research articles, which are published in various national and international Journals and conferences. She is involved in developing healthcare system prototypes and for which she has filed various national and international patents. She is contributing as editor, reviewer, Session Chair & committee member to various International conferences and Journals. Her areas of special interest include mobile healthcare, analytics, data science, artificial intelligence and Internet of Things.