IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received January 19, 2019, accepted March 8, 2019, date of current version May 10, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2907793

Application Specific Internet of Things (ASIoTs): Taxonomy, Applications, Use Case and Future Directions

KENNETH LI-MINN ANG, (Senior Member, IEEE), AND JASMINE KAH PHOOI SENG, (Member, IEEE)
[1]School of Information Communication & Technology, Griffith University, Gold Coast, QLD 4215, Australia
[2]School of Engineering & IT, University of New South Wales, Canberra, ACT 2600, Australia

Corresponding author: Kenneth Li-Minn Ang (kenneth.ang@gmail.com)

ABSTRACT As more and more applications are deployed using the Internet of Things (IoT) technologies, the fragmentation of general purpose IoT technologies to target particular sectors with different requirements is becoming necessary. In this paper, we summarize the latest developments of application-specific IoTs (ASIoTs) (a term to conceptualize the development of IoTs targeted toward specific domains, communications mediums, and industry sectors) in eight representative studies (Internet of Battlefield Things (IoBT), Internet of Medical Things (IoMT), Internet of Animal Things (IoAT), Internet of Waste Things (IoWT), Internet of Underwater Things (IoUWT), Internet of Underground Things (IoUGT), Internet of Nano Things (IoNT), and Internet of Mobile Things (IoMobT) such as the Internet of Vehicles). The paper gives contributions to ASIoTs from three perspectives: First, we offer a basic classification taxonomy for ASIoTs and discuss various representative studies and applications which can be found in the literature; Second, we discuss a use case for a biometrics-based ASIoT (termed IoBioT) for illustration and experiments of face-based biometric recognition on IoBioT are also performed; and Third, we give discussions and future directions for ASIoTs. An objective of this paper is to spur researchers and facilitate the development of ASIoTs for the different user-defined domains, communication mediums, and technology constrained platforms.

INDEX TERMS Application specific Internet-of-Things (ASIoT), Internet-of-Things (IoT), biometrics ASIoT, big data.

I. INTRODUCTION

Internet-of-Things (IoT) which combines advancements in sensing, mobile computing and cloud server technologies and platforms have in recent years become highly important and ubiquitous in the modern world [1], [2]. As more and more applications are deployed using IoT technologies, the fragmentation of general purpose IoT technologies to target particular sectors with different requirements is becoming necessary. For example, a customized IoT for environmental water monitoring would have different requirements from a customized IoT for medical patient monitoring. The latter IoT application would require much higher and stringent requirements for real-time data transfer and security. This leads to the emergence and development of IoTs to realize specific requirements for various domains, communications mediums and industry sectors which for convenience we term as application specific IoTs (ASIoTs).

On observation, the development of ASIoTs is mirroring the development of application specific integrated circuits (ASICs) in digital electronics technology with the realization that different application domains (e.g. high speed logic processing, implementation on low power devices) required different design parameters to be optimized. In the case of ASICs, some requirements and parameters to be customized include clock speed, chip area, power consumption, etc [3]. For ASIoTs, some parameters and requirements to be customized include the end-to-end delay or network data latency, robustness of the network towards node failures, node power consumption, security aspects, etc.

The associate editor coordinating the review of this manuscript and approving it for publication was Usama Mir.

Although ASIoTs are an emerging research area, some examples of IoTs for customized and specific applications can be found in the literature. The authors in [4] proposed the medical Internet of Things which they termed mIoT. Further examples of ASIoTs are the Internet of Underwater Things (IoUWT) [5] as a network of smart interconnected underwater objects, the Internet of Battlefield Things (IoBT) [6] worn by military personnel and embedded within military equipment, the Internet of Nano Things [7] and the Internet of Vehicles (IoV) [8], [22] which utilizes vehicles on highways as mobile nodes and roadside sensing and computational infrastructure for intelligent transportation and safety applications. The design of the different ASIoTs will prioritize meeting different design factors. Some design factors will remain common towards most ASIoTs whereas others may only apply towards ASIoTs in particular domains.

A common requirement for many ASIoTs is the requirement for low power and low complexity implementation in battery-powered sensor nodes or devices. Many IoT devices cannot afford resource demanding algorithms (e.g. cryptographic & video [9] protocols) to be implemented within the hardware constrained devices. For example, a medical sensor device to be authenticated with fingerprint recognition technology would need the biometric traits to be encrypted before transmission to the cloud server. This encryption would need to be performed on the device itself which would have severe constraints on computational power, memory storage and power consumption while still ensuring the requirements are met for secure communications. However, this requirement for low power consumption is not required in IoV applications as the chemical or electric batteries in vehicles can provide ample power for sensing, communications and information processing. In the case for IoV networks, the requirement is geared towards very low network latency and fast response time to meet the safety requirements for intelligent transportation. Here, we see a contrast between the design factors and tradeoffs (e.g. power consumption vs network response time) for different ASIoTs.

This paper aims to spur researchers and facilitate the development of ASIoTs for different user-defined domains, communication mediums and technology constrained platforms. It gives contributions for ASIoTs from three perspective. First, a basic classification taxonomy for ASIoTs is presented. This is followed by the discussion on various representative studies and applications which can be found in the literature. Second, we present a use case for a biometrics-based ASIoT (termed IoBioT) for illustration. A case study of face-based biometric recognition and experiments is included to confirm our approach in the Big biometrics data computation layer of IoBioT. Third, the discussions and future directions for ASIoTs are presented. The paper is organized as follows: Section II discusses a basic classification taxonomy and several representative studies and applications for ASIoTs which can be found in the literature. A focus here is to identify some important design parameters and challenges to be addressed in these ASIoTs. A use case study for a biometric-based ASIoT (IoBioT) is discussed in Section III to illustrate some design parameters and customizations for security, key management and Big data information processing. Experiments are also included. Section IV gives future directions and discussions to spur researchers and facilitate the development of ASIoTs for different user domains, communication mediums and technology constrained platforms. Section IV concludes the paper.

II. STUDIES IN ASIOT RESEARCH

This section surveys advancements made in the developments and applications of ASIoTs in eight representative studies (Internet of Battlefield Things, Internet of Medical Things, Internet of Animal Things, Internet of Waste Things, Internet of Underwater Things, Internet of Underground Things, Internet of Nano Things, and Internet of Mobile Things). An important focus is the identification of the various design factors and challenges to be prioritized for the different ASIoTs. We also offer a basic taxonomy and classification of ASIoTs into three categories: (1) User domain-driven; (2) Communications medium-driven; and (3) Technology constraint-driven. The design parameters for user domain-driven ASIoTs are optimized for parameters defined by the specific user domain.

Examples of user domain-driven ASIoTs would be the Internet of Battlefield Things, Internet of Medical Things, Internet of Animal Things and Internet of Waste Things. The design of communications medium-driven ASIoTs are dominated by the network communications in the medium (e.g. terrestrial, underwater, underground mediums) with different properties and characteristics. Examples of these classes of ASIoTs are the Internet of Underwater Things and the Internet of Underground Things. The third classification for ASIoTs are the technology constraint-driven ASIoTs. An example of this class is the Internet of Nano Things where the constraints of the nanotechnology implementation drives the design factors for the ASIoT. Table 1 shows a summary of the different types of ASIoTs and its taxonomy classification, the smart things or objects in the ASIoT, the challenges and the design parameters to be prioritized and optimized, and some representative works discussed in this section. The lessons learnt from the case studies and the important factors and future directions for designing and building ASIoTs are discussed in Section IV.

A. INTERNET OF BATTLEFIELD THINGS (IoBT)

The Internet of Battle Things or also known as the Internet of Battlefield Things (IoBT) [6], [10], [11], [12] is an illustrative example of an ASIoT which has been designed for military and defense applications. The design of the IoBT would be strongly influenced by two technologies (machine intelligence and networked communications). The ‘‘smart things’’ in the IoBT would include sensors, munitions, weapons, vehicles, robots, and human-wearable devices which are capable of collecting and processing information, acting as agents to support decision making and situational awareness,

TABLE 1. Summary of ASIoTs characteristics and its taxonomy classification.

Application Specific IoT (ASIoT)	Smart things and objects in ASIoT	Design challenges and optimization parameters	Ref.
User domain-driven ASIoTs			
Internet of Battlefield Things (IoBT)	Sensors, munitions, weapons, vehicles, human-wearable devices	Fast adaptive robust network communications, real-time information processing, high security for IoBT functioning	[6], [10], [11], [12]
Internet of Medical Things (IoMT)	Medical wearables (Parkinson, multiple sclerosis, diabetes, heart rate, ECG), smart things (insulin and inhalers)	Interoperability between manufacturers, simple connectivity and device management, security and privacy concerns	[4], [13], [14]
Internet of Animal Things (IoAT)	Smart cattle collars (rumination, activity temperature), RFID ear tags, sound analyzers	Energy efficiency for on-animal measuring devices, indoor wireless channel characterizations	[15], [16], [26]
Internet of Waste Things (IoWasteT)	Smart garbage bins (SGBs), RFID tags, cameras, actuators	Energy efficient large scale data collection, integration with IoV, data MULEs	[17], [18], [19]
Communications medium-driven ASIoTs			
Internet of Underwater Things (IoUWT)	Underwater sensors, smart buoys, AUVs, ships	Long propagation delays, high error rates, short bandwidth, difficulty to recharge devices	[5], [23], [24], [25]
Internet of Underground Things (IoUGT)	Buried soil sensors, seismometers, mobile sinks on field vehicles/machinery	Power conservation, network topology design, antenna design, environmental extremes	[27], [28], [29]
Technology constraint-driven ASIoTs			
Internet of Nano Things (IoNT)	Nano-sensors and actuators, nano-routers, nano-micro interfaces, bioFETs	Nanomaterial properties (e.g. graphene nanoribbon (GNR), carbon nanotube (CNT) for communications	[7], [30], [31], [32]
Internet of Mobile Things (IoMobT)	Mobile personal devices (tablets, smartphones), robots, vehicles	Dynamic network topology, unpredictability, direct energy exchange among smart objects	[33], [34], [35]

undertaking coordinated defensive actions, and unleashing a variety of effects on the adversary [6].

The IoBT can be seen as a user defined-domain ASIoT with extremely stringent requirements for fast and adaptively robust network communications, rapid real-time information processing to deal with a large volume and complexity of information for human decision-making and requiring very high security. As remarked by the authors in [6], the IoBT will itself become a battleground, as the adversary will attempt to take control and subvert the IoBT for its own ends. The authors identified three security challenges for the IoBT to be addressed: (1) Physical survival and functioning of IoBT from kinetic, directed-energy and electronic attacks against its things, jamming the RF channels, destroying fiber channels and by depriving IoBT of its power sources; (2) Threats to the confidentiality, integrity, availability of the information within IoBT, by electronic eavesdropping, and by deploying malware into IoBT; and (3) Human deceptions and loss of confidence that the information in the IoBT is trustworthy or that some elements of IoBT are being controlled by the adversary.

Other authors have proposed various improvements to address the challenges faced by the IoBT. A significant challenge for the IoBT compared with other IoTs is the need for information dissemination in the presence of adversaries. The authors in [10] studied the problem of network connectivity for the IoBT in which an attacker aims at disrupting the connectivity of the network by choosing to compromise one of the IoBT nodes at each time epoch. The authors formulate the scenario as a dynamic multistage Stackelberg connectivity game that explicitly takes into account the characteristics and requirements of the IoBT network such as the IoBT latency and the sum of weights of disconnected nodes at each stage of the game. Their results showed that the expected number of disconnected sensors using the feedback Stackelberg equilibrium (FSE) decreased up to 46% compared to a baseline equal probability policy. Another approach for secure information dissemination in the presence of adversaries was proposed by [11]. In this work, the authors used stochastic geometry (SG) based models to characterize the connectivity of IoBT networks in terms of the degree distribution and employed epidemic spreading models to model data dissemination among different types of battlefield devices according to the assigned missions. Their results showed that the objectives of the battlefield mission could be achieved by either changing the deployment of the combat units or by changing their transmission power. The authors in [12] investigated the problem of detecting malware in the IoBT. Their approach employed eigenspace learning and deep learning methods to detect IoBT malware using the operational code sequences (OpCode) of the devices. The authors showed that their approach achieved an accuracy rate of 98.37%, a precision rate of 98.59% and also had the capability to mitigate against junk code insertion attacks.

B. INTERNET OF MEDICAL THINGS (IoMT)

The Internet of Medical Things (IoMT) is another example of a customized user domain-driven ASIoT for healthcare and patient monitoring with its own specific requirements and challenges. Examples of "smart things" in the IoMT would include sensor wearables (e.g. for Parkinson's disease, multiple sclerosis), sensors and devices for diabetes, heart rate and electrocardiogram (ECG), and smart things for insulin and inhalers. The authors in [4] identified the requirement of interoperability as a major challenge for the IoMT. This important issue deals with the need for proprietary protocols from medical sensors/devices and smart things from one manufacturer to be able to communicate with devices and servers from other manufacturers in order that the collected data can be utilized fully for the diagnosis and health applications and not marooned on separate data islands. Other challenges identified by the authors for the IoMT include: (1) Simple connectivity for the smart things and devices to connect to and access the cloud-based services; (2) Easy device management for improved device availability and reduced maintenance; and (3) Informative analytics to gain insight from huge volumes of medical and healthcare data for better decision-making.

Although the security requirements for the IoMT may not be as stringent as for the IoBT, the security and privacy of the patients' records also require protection from unauthorized access. The privacy of patients' can be breached if the personal and medical information are posted in the public domain or otherwise used without their consent. Similarly, attacks can be made to interfere with the proper functioning of essential medical devices such as pacemakers. The authors in [13] proposed authentication mechanisms for ECG monitoring signals from IoT devices using watermarking techniques. In their approach, a watermark is introduced into the ECG signal on the client side which is then authenticated on the cloud server. Their watermarking approach is based on dividing the ECG signal into a number of beats and applying the discrete wavelet transform singular value decomposition (DWT-SVD) on each beat. On the cloud side, seven features (heartbeat rate, P wave duration, PR interval, QRS complex, QT interval, shape and T wave) are extracted from the ECG signal and the classification is performed using a one-class support vector machine (OCSVM).

The authors in [14] proposed the Wearable IoT (WIoT) for person-centered healthcare. The architectural composition of the WIoT includes three elements: (1) Wearable body area sensors (WBAS); (2) Internet-connected gateways; and (3) Cloud and Big data support. The WBAS serves as the frontend for the WIoT ecosystem and performs two functions: (1) Data collection from the body through contact sensors or peripheral sensors; and (2) Data preparation for onboard device analysis or remote transmission for comprehensive analysis and decision support. The Internet-connected gateways serves to exchange data with the wearable sensor devices via short range communication technology (e.g Bluetooth) and transmit the data to the cloud via heterogeneous networks communication technology (e.g. WiFi and GSM). The Cloud and Big data support provides the computing infrastructure for large-scale and advanced functionalities for medical data analytics, machine learning and data mining.

C. INTERNET OF ANIMAL THINGS (IoAT)

The Internet of Animal Things (IoAT) [15] is as an example of an ASIoT where the smart objects and devices are used to monitor living creatures (e.g. livestock such as dairy cows, sheep, cattle) within the IoT. The IoAT would have significant advantages for monitoring the health of livestock for smart farming applications. Examples of smart things in the IoAT would include smart cattle collars to monitor rumination, temperature and activity movements, RFID ear tags and sound analyzers for early detection of respiratory diseases [16]. A recent work by the authors in [26] proposed a method to detect and classify the screams of pigs for indications of stressful situations. Their approach used classification of sound spectrograms and achieved results of 71.83% sensitivity, 91.43% specificity and 83.61% precision. Some challenges for the IoAT include energy efficiency for the on-animal measuring devices. The authors in [15] proposed the use of sub-GHz long range (LoRA) for use in animal monitoring and characterized the off-body wireless channel in indoor (barn) environments at 868 MHz using LoRa nodes.

D. INTERNET OF WASTE THINGS (IoWasteT)

The Internet of Waste Things (or also known as the Internet of Bins [17]) is a very useful application for deployment in smart cities [18], [20]. The smart things and objects in the IoWasteT include smart garbage bins (SGBs) [19], RFID tags, sensors, cameras and actuators. The IoT-based smart garbage system (SGS) proposed in [19] was operated as a pilot project in Seoul for a one-year period. The battery-based SGBs communicated information with each other using wireless mesh networks and a router and server collected and analyzed the information for service provisioning. A header SGB (HSGB) located within each region was used to analyze and manage the other SGBs within its region after collecting their information. Their approach included a cooperation-based operation to increase the battery lifetime in the IoT for energy-efficient operations of the SGBs where the HSGB was adaptively selected according to the battery and memory status of each SGB in the region. An important challenge for the IoWasteT is the large scale data collection and delivery to thousands of sensors and actuators integrated within the smart objects. A potential solution is to use the Internet of Vehicles (IoV) to serve as data MULES (Mobile Ubiquitous LAN Extensions) [21] in smart city environments as a cost effective approach for the large scale data collection, transportation and information processing from smart objects within the smart city environment [22].

E. INTERNET OF UNDERWATER THINGS (IoUWT)

The Internet of Underwater Things (IoUWT) is an example of a communications medium driven ASIoT targeted for application in oceans and other water-based domains. The "smart things" in the IoUWT would include underwater sensors, smart buoys, autonomous underwater vehicles (AUVs) and ships. The design of the IoUWT would be strongly influenced by the unique factors for network communications in the water-based medium compared to communications in a traditional terrestrial medium. The network communications in the IoUWT would employ acoustic links compared to radio waves for a terrestrial-based IoT. The acoustic medium for network communications would suffer from long propagation delays, high bit error rates and short network bandwidth [5]. The authors in [23] identified some further challenges for the IoUWT: (1) Energy efficiency and difficulty to recharge. Due to the high deployment costs of the underwater sensors and the difficulty to recharge the devices, energy efficiency is an important challenge for the IoUWT; (2) Changes to network topology due to movement of the underwater sensors; and (3) Unstable and low reliability due to transmission loss of the acoustic signals being absorbed by the water environment.

Two approaches for energy efficient medium access control (MAC) and routing protocols for the IoUWT can be found in the works by [24], [25]. Medium access control (MAC) protocols developed for terrestrial IoTs such as carrier-sense multiple access (CSMA) or time-division multiple access (TDMA) do not perform well underwater. The authors in [24] proposed an energy efficient MAC protocol for underwater sensor networks termed EE-MAC. The EE-MAC protocol achieves the energy efficiency by minimizing the idle listening period and reduces the energy loss due to packet collisions. The authors in [25] proposed an energy efficient routing protocol which is efficient in packet forwarding and energy consumption for the IoUWT termed E-CARP. The E-CARP protocol uses a greedy routing strategy to deliver packets hop-by-hop and reduces the number of control packets to lower the energy consumption and increase the lifetime of the sensor nodes in the IoUWT.

F. INTERNET OF UNDERGROUND THINGS (IoUGT)

The Internet of Underground Things (IoUGT) [27], [28] is another example of a communications medium-driven ASIoT targeted in this case for underground network communications. The IoUGT is particularly useful for applications in environmental monitoring, landslide and earthquake monitoring and precision agriculture (e.g. for real-time soil sensing and monitoring [27]). The smart things in the IoUGT include underground (UG) objects (e.g. buried soil sensors for temperature, moisture, pH sensing, buried seismometers), above ground (AG) smart objects (e.g. base stations and mobile sinks), smart interfaces for field machinery and irrigation systems. Being a communications-medium driven ASIoT, the design of the IoUGT would be influenced by the underground network communications (in this case through electromagnetic (EM) wave propagation through a dense substance such as soil or rock). The authors in [28] identified four design challenges for wireless sensor communications in underground channels: (1) Power conservation and recharge ability – The IoUGT faces similar challenges to the IoUWT for recharging or replacing the deployed smart devices (in this case, the smart devices would be buried underground with difficulty to access physically).

The factors which affect communication with EM waves in underground environments include path loss due to material absorption, reflection/refraction, multi-path fading, reduced propagation velocity and noise [28]; (2) Topology design – The topology and deployment of the sink/relay objects could be completely underground or utilize a hybrid structure where field vehicles or machinery function as mobile sinks for data collection from the underground sensors; (3) Antenna design – some challenges include antenna size and directionality (e.g. using a single omni-directional or a group of independent directional antennas); and (4) Environmental extremes – threats from extreme temperatures, water, animals and insects. A recent work by the authors in [29] performed a comprehensive connectivity analysis of underground sensors in wireless underground sensor networks for the effects of environment parameters such as soil moisture and composition, and for system parameters such as node density and propagation techniques. The authors remarked that their connectivity analysis can be used as a framework when considering the connectivity of wireless underground sensor nodes with other kinds of environment and system parameters.

G. INTERNET OF NANO THINGS (IoNT)

The Internet of Nano Things (IoNT) [7], [30] serves as an example of an ASIoT which is targeted towards realization for a specific technology constraint-domain (in this case nanotechnology) and the design parameters are strongly influenced by what communications and information processing can be performed in this (nanotechnology) domain. Communications on the nanoscale can take two forms: (1) Molecular communication – utilizing the transmission and reception of information encoded in molecules; and (2) Nano-electromagnetic communication – utilizing the transmission and reception of EM radiation based on novel nanomaterials [7]. The smart things in the nanotechnology domain include nano-sensors, nano-actuators, nano-nodes, nano-routers, nano-micro interface and gateways (e.g. smartphones) to connect the IoNT to the global Internet. The design challenges for the IoNT stems from the properties of the nanomaterials used (e.g. graphene nanoribbon (GNR) or carbon nanotube (CNT)). The works in [30] and [31] extended the concept of the IoNT to the Internet of Multimedia Nano Things (IoMNT) and the Internet of Bio Nano Things (IoBNT). The IoBNT requires the development of connections between the biochemical domain of molecular nanonetworks and the electrical domain of electromagnetic networks with the promise of continuous health monitoring and bacterial sensor-actuator networks inside the human body. The authors in [32] proposed the use of field effect transistor based biosensors (bioFETs) to construct a molecular antenna capable of transducing molecular messages into electrical signals.

H. INTERNET OF MOBILE THINGS

In the traditional IoT, the sensor nodes and devices are mostly static within the network. The Internet of Mobile Things (IoMobT) [33] represents an ASIoT where the smart things can move independently and remain accessible within the network. The ‘‘smart things’’ in the IoMobT would include mobile personal devices (e.g. smartphones, tablets), mobile robots and vehicles on highways. The Internet of Vehicles (IoV) is a good example of the IoMobT. The authors in [33] identified four challenges to be addressed for the IoMobT: (1) Mobile Data Collection – Movement of the smart objects within the network generates unpredictability and an increased number of faults and disruptions for data collection; (2) Mobile Data Analytics – Characterizing and utilizing learnt mobility patterns of the smart objects to improve data analysis tasks; (3) Energy Management – Allowing the direct energy exchange among the different smart objects (e.g. an electric vehicle within the IoV can transfer available energy to another vehicle or to the smart grid (i.e. V2G technology)); and (4) Security and Privacy – Authenticating new smart devices and objects and preserving

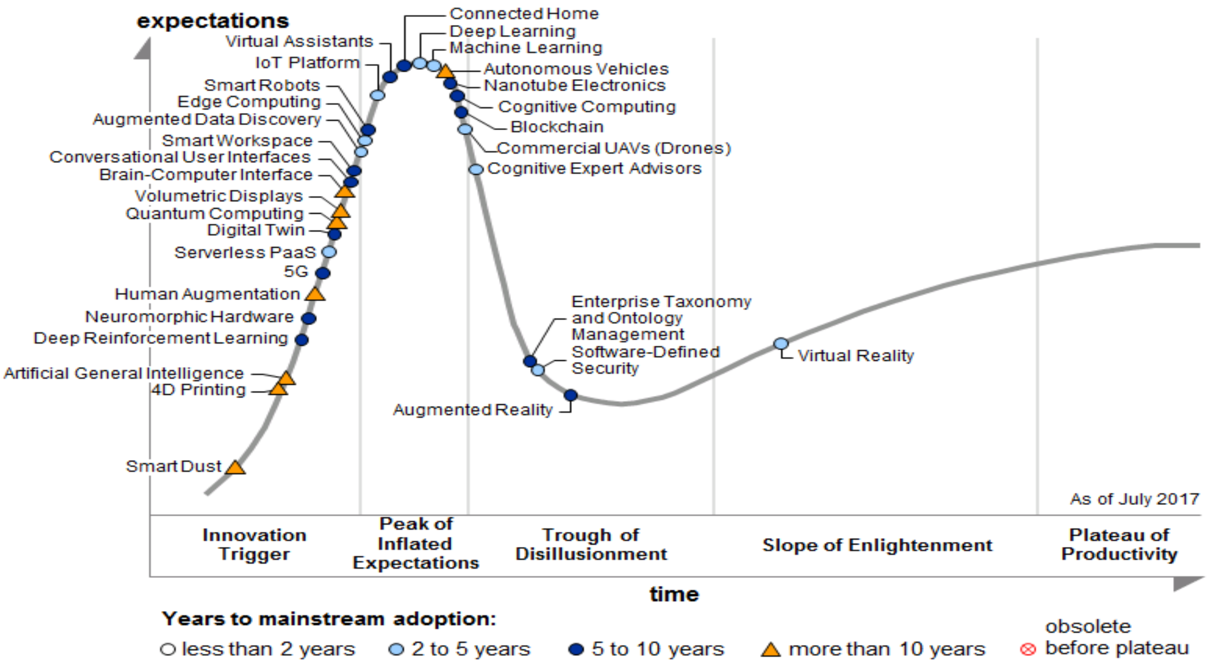


FIGURE 1. Gartner 2017 Hype Cycle for Emerging Technologies showing IoT and edge computing technologies [36].

location privacy of the objects. The works in [34], [35] further proposed improvements towards the IoMobT. The authors in [34] proposed a middleware concept termed *Mobile Hub* for the IoMobT which allows the smart objects in the IoMobT to move autonomously and remain remotely accessible over the Internet. The authors in [35] proposed a platform as a service (PaaS) fog computing model termed *Mobile Fog* for the IoMobT that has the advantages of being geospatially distributed, large-scale and latency-sensitive.

III. USE CASE FOR A BIOMETRICS-BASED ASIoT

This section gives an illustration for a user domain-driven ASIoT for biometrics termed IoBioT. The section first gives an introduction to biometric systems for the IoT. We then give discussions for a layer architecture for the IoBioT, and some design parameters and customizations for security, key management and Big data information processing.

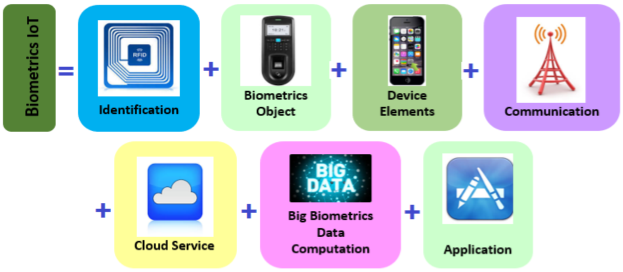
A. BIOMETRICS AND IoT SYSTEMS

Biometric systems are becoming essential for authentication purposes particularly for usage in embedded devices such as the IoT. In 2000, the Gartner Group remarked that biometric identification (e.g. fingerprints, face and voice) will emerge as the only way to truly authenticate an individual, which will become increasingly important as security and privacy concerns grow. Initial systems for biometrics applications used standalone devices connected to a central server which performed the information processing and authentication tasks. With the rapid proliferation and increasing processing capability of smartphone and IoT devices, together with wide-scale network connectivity, distributed approaches where the processing tasks are performed at the edge of the network (or termed as edge or fog computing techniques) are becoming popular. Fig. 1 shows the Hype Cycle for Emerging Technologies from Gartner in 2017 [36].

An interesting observation as shown in Fig. 1 is the closeness for the technology trends for edge computing and IoT. This also motivates the development of the biometrics ASIoT (IoBioT) which requires fast response times to perform the authentication tasks. In the IoBioT, this can be achieved by performing the information processing on the IoT devices instead of having to transmit the biometrics data across the IoT network and waiting for the response from the central server. Some examples of works for implementing biometrics on the IoT or embedded devices can be found in [37], [38]. These works used the Raspberry Pi as the IoT device for implementation. Compared to the works in [37], [38] which focused the discussion on implementation in embedded devices, this section takes a broader perspective for the IoBioT to serve as an illustration for developing domain-driven IoT technologies and aims to spur researchers towards developing ASIoTs for different domains and platforms in general, and towards the development of the IoBioT specifically.

B. BIOMETRICS ASIoT LAYER ARCHITECTURE

This section introduces the major elements in the Biometrics ASIoT (IoBIoT) infrastructure. Fig. 2 shows a diagram of the Biometrics ASIoT elements and the building blocks components in its layers. Fig. 3 shows an overview of the IoBioT layer architecture. There are seven core layers within this architecture (Identification Layer, Biometrics Object Layer,



(a)

Biometrics ASIoT	Components	
Identification Layer	Name/Object ID (e.g. EPC, uCode)	
	Addressing (e.g. IPv4, IPv6)	
Biometrics Object Layer	Scalar Object (single modality object e.g. image from visual sensor)	
	Multimedia Object	Single modality object (e.g. image data)
		Multimodalities object (e.g. video data with image and speech modalities)
Device Layer	Device Elements (e.g. motes, body sensor nodes, wearable devices)	
	Device-Object Security (e.g. pairing-based, identity-based, hop-based)	
Communication Layer	Link (e.g. IEEE 802.15.4)	
	Network (e.g. IP, RPL)	
	Transport (e.g. UDP (User Datagram Protocol), TCP (Transmission Control Protocol))	
Cloud Services Layer	Private cloud, Public cloud (e.g. Amazon EC2, Microsoft Azure)	
	Device-Cloud Security	
Big Biometrics Data Computation Layer	Hardware (e.g. data centers, GPUs, parallel platforms)	
	Software (RTOS e.g. TinyOS, Contiki)	
	Big Biometrics Data Analytics (Divide and Conquer paradigm)	
Application Layer	e.g. CoAP (Constrained Application Protocol), XMPP (Extensible Messaging and Presence Protocol), DDS (Data Distribution Services)	

(b)

FIGURE 2. Elements and components in the Biometrics ASIoT (IoBIoT) layers. (a) Biometrics ASIoT elements. (b) IoBIoT components.

Device Layer, Communication Layer, Cloud Services Layer, Big Biometrics Data Computation Layer and Application layer). We will give particular focus for two customizations which are important for the biometrics IoT domain: (1) End-to-end security and key management; and (2) Big data information processing using divide-and-conquer approaches. The layer customizations for end-to-end security and key management for the IoBioT will be discussed in Section III-(C). As shown in Fig. 3, the Big Biometrics Data Computation Layer is designed specifically for biometrics processing and contains dedicated computational units for data centralization, data aggregation, divide and conquer feature extraction, data fusion and decision making. This customized layer for Big data information processing will be discussed further in Section III-(D).

The first layer in the IoBioT is the Identification (ID) Layer. The ID layer functions to uniquely identify the smart things and objects within the IoBioT. Examples of ID codes are electronic product codes (EPC), uCodes and IP addresses (e.g. IPv6 addresses can be used to uniquely identify billions of objects and devices). The second layer (Biometrics Object Layer) functions to gather data from multiple biometrics sensors (e.g. face, fingerprint, voice/speech, iris and palm data) or objects from users within the network, and transmits the data to a central cloud for further processing. The biometric data can be collected from various locations (e.g. smartphones, smart cars, smart devices, smart appliances and smart homes). Some biometrics data are not scalar data and may involve different types of sensors. Multi-biometrics authentications would require data from multiple modalities to be collected from various biometrics sensors. The Device Layer in the IoBioT consists of components (e.g. wearable devices, body sensor nodes, wireless motes, etc.) to transmit the sensed biometrics data to the higher layers of the IoBioT. An important issue in this layer is to secure the biometric data before an attacker can get hold of it. Security issues and challenges in this layer include the need to avoid resource-demanding cryptographic protocols to meet the hardware-constrained (e.g. low computational power, memory and limited energy resources) requirements for IoT devices. Lightweight cryptography protocols [39], [40] which are suitable for implementation on hardware-constrained devices can be utilized in this layer. Security issues for the IoBioT nodes in this layer include attacks from an adversary to deplete the energy resources of the nodes by repeatedly making excessive requests or transmissions so that the nodes would have to make unnecessary transmissions.

The fourth layer (Communication Layer) in the IoBioT serves the same function as that within the conventional IoT with three sub-layers or components: (1) Link sub-layer – responsible for the MAC protocols to be used within the IoBioT; (2) Network sub-layer – responsible for connectivity and routing decisions within the IoBioT (e.g. can utilize RPL protocol for routing over low Power and lossy networks [41]); and (3) Transport sub-layer – responsible for end-to-end communications by providing flow and congestion control mechanisms (e.g. can utilize UDP or TCP protocols). The Cloud Services Layer provides the core hardware infrastructure, servers, platform and storage and gives flexibility and scalability for the IoBioT applications. Using virtualization technology, it provides a system architecture with distributed parallel environments which can run multiple computational units to give fast computational response and high reliability. The elements in the IoBioT cloud could be formed from the private cloud within an organization or the public cloud (e.g. can utilize Amazon EC2 or Microsoft Azure). The Big Biometrics Data Computation Layer functions as a customized processing layer in the IoBioT to serve the need for Big data information processing. It contains the hardware components (e.g. data centers, GPUs, parallel platforms, FPGAs, SOCs) and software components (e.g. MapReduce, Hadoop, Spark) to perform computations in the IoT. For the IoBioT, we also include a software component to perform the multimodal Big data analytics using a divide and conquer paradigm which

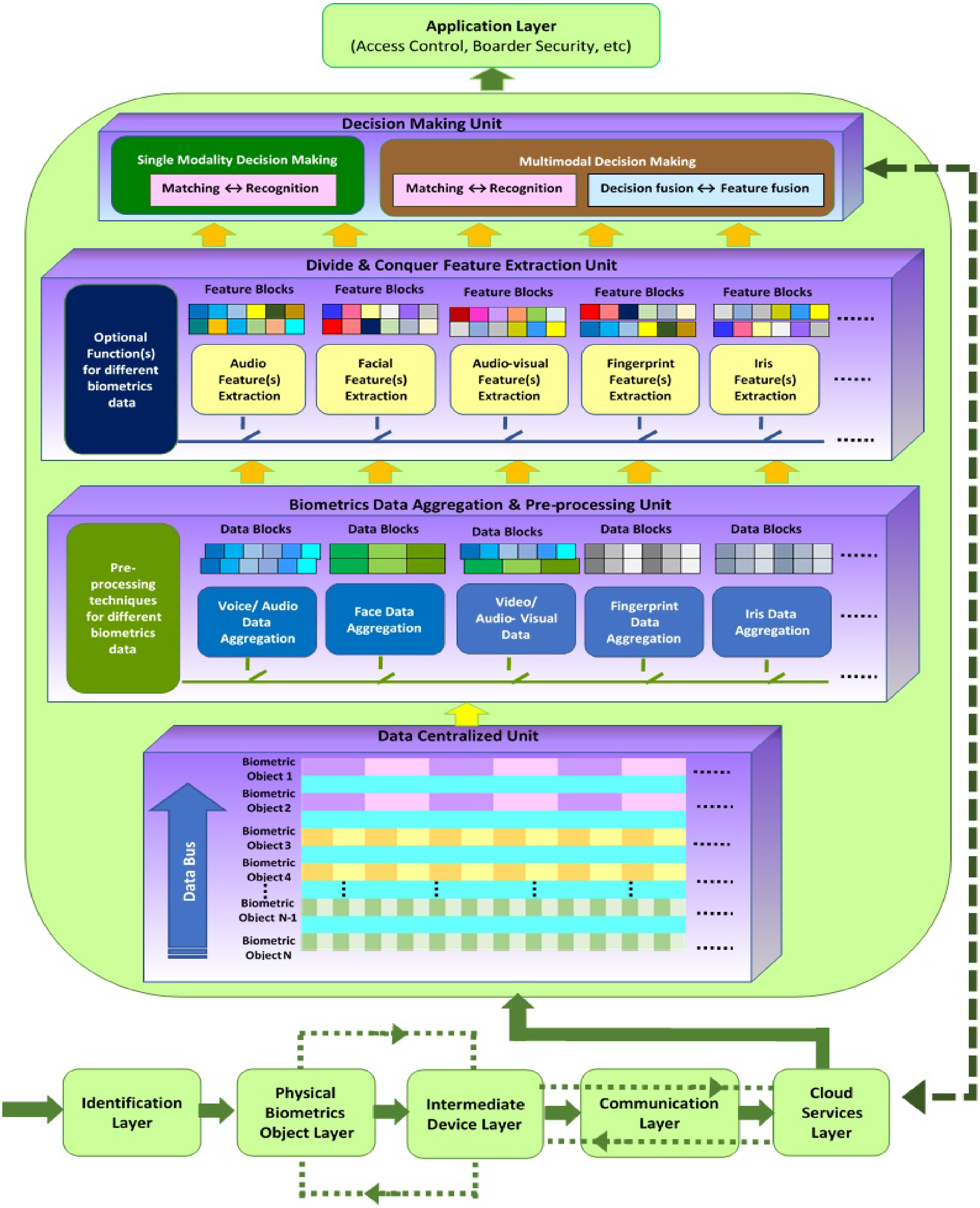

Application Layer
(Access Control, Boarder Security, etc)
Decision Making Unit
Single Modality Decision Making
Matching ↔ Recognition
Multimodal Decision Making
Matching ↔ Recognition
Decision fusion ↔ Feature fusion
Divide & Conquer Feature Extraction Unit
Optional Function(s) for different biometrics data
Feature Blocks
Audio Feature(s) Extraction
Facial Feature(s) Extraction
Audio-visual Feature(s) Extraction
Fingerprint Feature(s) Extraction
Iris Feature(s) Extraction
Biometrics Data Aggregation & Pre-processing Unit
Pre-processing techniques for different biometrics data
Data Blocks
Voice/ Audio Data Aggregation
Face Data Aggregation
Video/ Audio- Visual Data
Fingerprint Data Aggregation
Iris Data Aggregation
Data Centralized Unit
Data Bus
Biometric Object 1
Biometric Object 2
Biometric Object 3
Biometric Object 4
Biometric Object N-1
Biometric Object N
Identification Layer
Physical Biometrics Object Layer
Intermediate Device Layer
Communication Layer
Cloud Services Layer

FIGURE 3. The proposed Biometric ASIoT (IoBioT) architecture.

is discussed in Section III-(D). The smart objects send their data to the cloud for processing in real-time and then deliver results to end users from the extracted Big data.

The final layer (Application Layer) in the IoBioT is responsible for providing services and determines a set of protocols for message passing. The IEEE 802.15.4 proposes the

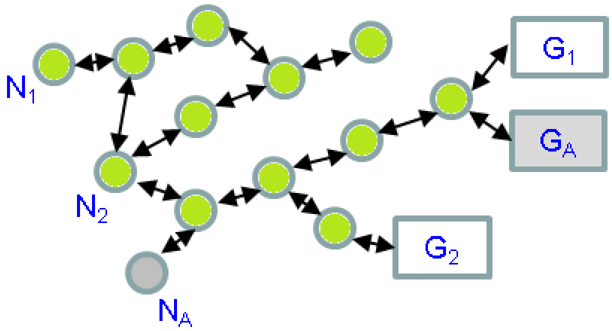


FIGURE 4. Adversary or imposter nodes and gateways in the IoBioT.

CoAP [42] as a key component for the low power IoT to reduce overheads and enhance packet delivery. The CoAP has two layers where the first layer is the messaging layer and the second layer is the request/response layer. The CoAP protocol uses the Datagram Transport-Layer Security (DTLS) to secure the CoAP messages. The authors in [43] proposed a fully implemented end-to-end application layer security architecture for the IoT based on existing Internet standards and communication stacks that use UDP/IPv6 networking for Low Power Wireless Personal Area Networks (6LoWPANs).

C. IoBioT CUSTOMIZATIONS FOR SECURITY AND KEY MANAGEMENT

This section gives some customizations for end-to-end security and key management for the IoBioT for securing the biometrics data from the device to the central collector (e.g. gateway) at the edge of the wireless network. The gateway provides the nodes in the IoBioT access to the global Internet. As in wireless sensor networks, messages are relayed from node to node until it reaches the gateway. There is also no requirement that all nodes in the network are under control or there may be imposter nodes as shown in Fig. 4. Thus, end-to-end security is essential to ensure that messages cannot be intercepted on the route from the sending IoBioT node to the gateway.

The authors in [44] identified a security issue to be addressed when a malicious compromised node forges a communication message and transmits to the gateway. The issue of forged nodes or gateways is highly important for the IoBioT especially for biometrics applications requiring high security such as hospital and medical monitoring systems. We consider the scenario when both malicious adversary nodes (N$_A$) and gateways (G$_A$) are forged and inserted into the IoBioT as shown in Fig. 4. Thus, there is a need to authenticate a new IoBioT node to the gateway, as well as to authenticate the gateway to an IoBioT node. We assume the presence of a Trusted Authority (*TA*) in the network for the following approach to authenticate IoBioT node i ($IoBioT_i$) to Gateway j (G_j) and vice versa. The secure data transfer from node to gateway can then take place using a shared key (K_{ij}) after successful authentication. Initally, the *TA* generates a master secret key (*sk*) and public key (*pk*). The *pk*is made available to all devices on the network. When a new IoBioT node is added to the network, it first needs to authenticate itself to G_j. The node sends to *TA* its node identity ($IoBioT_i$), G_j and the current timestamp (T_c) all encrypted by *pk*.

$$IoBioT_i \rightarrow TA : \{IoBioT_i, G_j, T_c\}pk \tag{1}$$

The *TA* checks the timestamp, and if valid sends back to $IoBioT_i$ the shared key (Kij), a nonce (N_1), the timestamp and a message encrypted with sk_{Gj} all encrypted by the public key of the node.

$$TA \rightarrow IoBioT_i : \{K_{ij}, N_1, T_c, \{K_{ij}, pk\}sk_{Gj}\}pk_{IoBioTi} \tag{2}$$

$IoBioT_i$ checks T_c and $N_1$and if valid sends to G_j the shared key (K_{ij}), a new nonce (N_2), the timestamp and the secret message for G_j received from the *TA* all encrypted by the public key of G_j.

$$IoBioT_i \rightarrow G_j : \{K_{ij}, N_2, T_c, \{K_{ij}, pk\}sk_{Gj}\}pk_{Gj} \tag{3}$$

$G_j$checks T_c and if valid decrypts the message encrypted with sk_{Gj} from the *TA* and retrieves the shared key (K_{ij}). $G_j$then replies to $IoBioT_i$ with N_2 and another new nonce (N_3) encrypted by the public key of $IoBioT_i$ all encrypted by the shared key K_{ij}.

$$G_j \rightarrow IoBioT_i : \{\{N_2, N_3\}pk_{IoBioTi}, T_c\}K_{ij} \tag{4}$$

$IoBioT_i$ checks T_c and $N_2$and if valid, it is assured that G_j is authenticated with the *TA*. $IoBioT_i$ sends to $G_jN_3$and the timestamp all encrypted by the shared key K_{ij}.

$$IoBioT_i \rightarrow G_j : \{N_3, T_c\}K_{ij} \tag{5}$$

G_j checks T_c and $N_3$and if valid, it is assured that $IoBioT_i$ is authenticated with the *TA*. $IoBioT_i$ and G_j can then communicate securely using the shared key K_{ij} and be assured that they are communicating with legitimate and not forged entities within the IoBioT. These security and key management customizations would enable the realization for biometrics applications requiring high security. The generation of the *sk* and *pk* could use low complexity elliptic curve techniques [45].

D. IoBioT CUSTOMIZATIONS FOR BIG DATA PROCESSING

This section gives some customizations for Big data information processing and analytics for the IoBioT. This is performed in the Big Biometrics Data Computation Layer as shown in Fig. 3. The processing layer caters for all kinds of biometric data. It also allows the multi-modalities fusion and decision making at the final stage. The divide and conquer feature extraction mechanism is presented to process these data blocks to obtain the feature blocks. The proposed structure of this layer is composed of four units: (1) Biometrics Data Centralized Unit (Bio_Data_CU); (2) Biometrics Data Aggregation & Pre-processing Unit (Bio_Data_APU);

(3) Divide & Conquer Biometrics Feature Extraction Unit (D&C_Bio_FEU); and (4) Biometrics Decision Making Unit (Bio_DMU).

The Bio_Data_CU is the first component in the Computation Layer and processes the raw data from various biometrics objects or devices with their own identity. The data from these objects can be video, images, voice, etc. This unit is also responsible for combining the objects data with their unique identity. This process of the Bio_Data_CU is illustrated in Fig. 3. After the raw data pre-processing in Bio_Data_CU has been completed, the processed data is passed to the Bio_Data_APU. This unit is responsible to perform data aggregation and arranges the data into blocks for the same object source based on its identity and biometrics modality and tries to create equal sizes of data blocks. In this unit, the aggregation and compilation service is supported by various algorithms that compile, organize, store and transmit the results. It also has some pre-processing functions for different modalities of biometrics data before performing the data analytics in the next units. The Bio_Data_CU and the Bio_Data_APU serves different functions in the Big Biometrics Data Computation Layer for the IoBioT. As illustrated in Fig. 3, The focus of the Bio_Data_CU is towards data arrangement and processing for biometric objects, whereas the focus of the Bio_Data_APU is towards data arrangement and processing for the different modalities (e.g. face, fingerprint, iris, etc.) found in multimodal biometrics data.

The D&C_Bio_FEU is the third component in the layer. The divide and conquer mechanism in this unit plays an important role to enhance the scalability of the IoBioT architecture and improve the computational efficiency of the processing. The divide and conquer mechanism with their own servers processes the data of each biometrics modality efficiently for performing the parallel processing or tasks. The deployment of the specific feature extraction function depends on the biometrics data and its modality to extract the target features (e.g. ridge features for fingerprints, visual features for face biometrics and audio features for audio signal/speech). Fig. 5 shows the flow chart of the proposed divide and conquer mechanism for the aggregated biometrics data blocks.

The type of biometrics data of the aggregated data blocks decides which feature function for the divide and conquer mechanism in the D&C_Bio_FEU is to be deployed. There are three main functions in the general mechanism: (1) Divide function; (2) Conquer function; and (3) Customized feature extraction function to target the specific feature. The divide function is responsible for divisions of block recursively until the block size reaches its threshold. The function takes the aggregated data block and divides the incoming block into two equal parts or sub-blocks (e.g. horizontally or vertically) recursively until it reaches to the block size threshold. Then the target feature extraction function is called for each divided or sub-block to extract the local features. The type and number of features vary and depends on the need of the biometrics application (e.g. minutiae for fingerprint features, spectral, mel-frequency cepstral coefficients (MFCC), zero-crossing rate (ZCR), linear prediction coefficients (LPC) for audio or speech features, optical flows and motion patterns for gait features). Other biometric features include hand geometry, palm print, knuckle print, vein patterns, etc. These features are extracted from the sub-blocks during the divide and conquer mechanism. The conquer function then is initiated to combine and process the features in reverse order by taking each two neighbors' sub-blocks local features. These feature blocks will be sent to the next stage of Bio_DMU for combination or fusion of feature blocks before decision making. Some examples for divide and conquer approaches for feature processing can be found in the works by [46], [47].

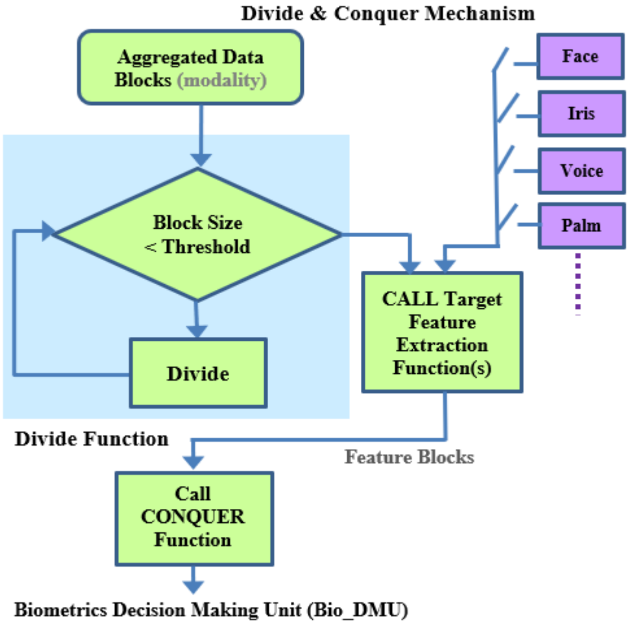

Divide & Conquer Mechanism
Aggregated Data Blocks (modality)
Block Size < Threshold
Divide
Divide Function
CALL Target Feature Extraction Function(s)
Face
Iris
Voice
Palm
Feature Blocks
Call CONQUER Function
Biometrics Decision Making Unit (Bio_DMU)

FIGURE 5. Customized divide and conquer mechanism to extract important features of different biometric data.

The Bio_DMU is the final stage of the computation layer. It contains fundamental support components (e.g. features/results storage devices, decision-making servers and communications infrastructure). The servers are supported by various algorithms that organize, store, and transmit the features/results with the intention that the data can be used by any server for its processing at any time. The algorithms to be used depend on the user domain biometric requirements. The Decision Making Server is also supported by various algorithms in order to make decisions for different scenarios and requirements. The decision making algorithm should be intelligent and efficient enough to efficiently produce a good decision. After the decision has been made, Bio_DMU returns the final desired output so that any application can utilize these decisions at real-time or offline for their respective requirements. The decision-making in the Bio_DMU depends on the data modality of the biometrics data: (1) Single modality; and (2) Multi-modality.

The feature blocks of biometrics data with single modality are sent to the Single Modality Decision Making module in the Bio_DMU. The decision making process is straightforward. There is a customized design of decision mechanism for the single modality and also specific applications. This unit can operate in two modes with built-in functionalities: (1) Verification; and (2) Identification. The verification process is described as a 1–to–1 matching system because the system tries to match the biometric presented by the individual against a specific biometric already in the database. The identification process is described as a 1-to-*n* matching system, where *n* is the total number of biometric templates in the database. Biometrics templates stored in the database can be obtained from the cloud and this computation layer also provides the access to the cloud database in the previous cloud services as illustrated in Fig. 3. The decision making for the modality can be made using machine learning techniques such as supervised learning, unsupervised learning or reinforcement learning. If the decision involves more than one type/modality of biometrics data, the sets of multimodal features blocks for each input multimodal partitioned data block are sent to the Multimodal Decision Making module in Bio_DMU.

The final process is required to integrate and perform fusion of the features from different modalities in order to make the decision. Two scenarios need to be considered: (1) Decision Level Fusion; and (2) Feature Level Fusion. For decision level fusion and decision making, the target analysis first provides the local decisions based on individual modality feature blocks. The local decisions are then combined using a final decision fusion module to make a fused decision vector that is analyzed further to obtain a final decision. For feature level fusion and decision making, the feature blocks are first combined and then sent as input to the feature fusion module which merges the sets of features blocks from different modalities before the decision making.

E. BIOMETRICS FACE RECOGNITION AND EXPERIMENTS

Sections III(B)–(D) have proposed the architecture of Biometrics ASIoT (IoBIoT) and customizations for Big Data Processing. One of the main components in the proposed architecture is the Biometrics Data Divide & Conquer Feature Extraction Unit which consists of the divide and conquer subsystems. This section provides a case study of biometrics face recognition where the single modality is the face image. In many biometrics applications, principal component analysis (PCA) and linear discriminant analysis (LDA) are two well-known and widely used feature extraction techniques. PCA and LDA are normally used together in a cascade operation to extract features in biometrics. The original versions of PCA, LDA or PCA-LDA (Fisherface technique) and their current extensions were not designed for Big data computation and do not scale well for Big data applications. To conduct the experiments for biometrics face recognition in Big biometric data computation layer in IoBIoT, our previous research work on divide-and-conquer approaches [55], Divide and Conquer PCA (DC-PCA) and Divide and Conquer LDA (DC-LDA) for Big data information processing are applied as shown in Fig. 6.

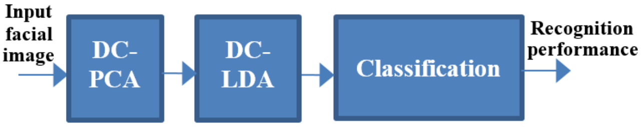


FIGURE 6. Experimental approach of Biometrics Face Recognition.

TABLE 2. Summary of the performance comparisons for ORL and Yale datasets.

Dataset	PCA	Fisherface	DC-PCA+LDA
ORL [56]	71%	83%	86%
Yale [57]	18%	60%	62%

Experimental results using the ORL [56] and Yale [57] datasets containing real-world variations for face recognition are presented to validate the approach and comparisons are given for the classification performance of the approach versus other traditional techniques which do not use the divide and conquer approach. The ORL dataset contains 400 images of 40 people containing 10 samples for each person with variations such as facial expressions and appearance. The experiments used five samples for each person for training and the remaining samples were used for testing. The Yale face database demonstrate variations in lighting conditions, facial expressions and facial details. The database contains 11 different images for each of 15 people. The experiments used 90 samples from the 15 people for training and the remaining samples were used for testing. Table 2. shows a summary of the performance comparisons. For the ORL dataset, the DC-PCA+LDA gave a recognition rate of 86% compared to 71% and 83% for PCA and Fisherface respectively, while for the Yale dataset, the DC-PCA+LDA gave a recognition rate of 62% compared to 18% and 60% for PCA and Fisherface respectively. The results validated the performance efficacy of the DC-PCA+LDA compared with the traditional PCA and Fisherface methods. Although the experimental objectives were to validate the divide and conquer feature extraction approach for Big data computation, the results for DC-PCA+LDA gave better performance than the established Fisherface approach.

IV. FUTURE DIRECTIONS AND RESEARCH FOR ASIoTs

This section discusses lessons learnt from the use case studies and some important challenges and future directions for designing and building ASIoTs. From the discussions in Section III and the observations in Table 1, we identify four areas and perspectives towards future research for ASIoTs: (1) Interoperability among ASIoTs; (2) Energy efficient operation in ASIoTs; (3) Edge and fog machine learning models for ASIoTs; and (4) Security and privacy challenges for ASIoTs.

A. INTEROPERABILITY AMONG ASIoTs

ASIoTs may contain a wide range of sensors, smart objects/devices and platforms from different manufacturers and vendors to be deployed within a specific domain. To achieve deployment of the ASIoT on a large-scale, these smart objects which may come from different manufacturers and vendors require the capabilities to interoperate and communicate with other smart objects within the IoT. The authors in [48] discuss a useful taxonomy for interoperability in IoT from five perspectives: (1) Device interoperability – mechanisms for integrating new devices into the IoT and message exchange among heterogeneous communication protocols within devices; (2) Network interoperability – mechanisms for end to end communication through diverse (wireless and wired) and heterogeneous communication networks; (3) Syntactical interoperability – interoperation of the data structure, format and interface for information exchange among the IoT entities; (4) Semantic interoperability – data and information models to allow IoT systems, services and applications to exchange information, data and knowledge in a meaningful way; and (5) Platform interoperability – mechanisms for information exchange across cross-platforms and cross-domains IoTs with diverse operating systems, architectures, access mechanisms for smart objects and data. The authors in [49] proposed a novel interoperability deployment for the industrial IoT domain using software-defined networks (SDNs) to manage different types of physical devices (industrial robot, automated guided vehicle, RFID reader, etc.), industrial wireless networks and cloud services and provide an interface for information exchange.

B. ENERGY EFFICIENT OPERATION IN ASIoTs

Many smart objects and devices in ASIoTs may rely on battery-powered sources with limited energy and/or may not be easily accessible for recharging purposes (e.g. in communications medium-driven IoUGTs and IoUWTs). Similar as for WSNs, the energy efficient operation and the need to optimize the network lifetime remains a critical challenge for ASIoTs. Novel and customized solutions for energy efficiency can be designed for different ASIoTs based on their specific deployment environment and requirements. The energy efficient solution used for one ASIoT may be different from solutions for other ASIoTs. The authors in [50] give an illustrative example of analyzing and designing an energy efficient ASIoT for the user domain of heritage artwork conservation. Their design considered the measurement requirements (e.g. sampling rate), aspects of the node design (e.g. sleep modes), gateway design, cloud infrastructure and user interface to determine the energy efficient requirements of the IoT operation. Using a small 1.7 mAh lithium-thionyl battery, their design was able to achieve a node lifespan of over twenty years by utilizing LoRa technology without the need for battery replacement.

C. EDGE AND FOG MACHINE LEARNING MODELS FOR ASIoTs

The authors in [51] remarked on the importance of cross-domain and multimodal inference and analytics for large-scale networked sensor systems which is also applicable towards ASIoTs where data is collected from a variety of sensing sources and domains. It is expected that new machine learning algorithms, data science and analytics will play a key role to extract value from the next generation of IoTs. A recent survey of machine learning techniques for the IoT can be found in [52]. A critical challenge for IoTs is to implement the machine learning algorithms (which can be computationally and/or storage intensive) on the resource-constrained smart objects or devices itself (or termed as edge or fog computing models). The authors in [53] remarked that the implementation of machine learning inference analytics on edge devices has huge potential and is still in its early stages. They also demonstrated the feasibility and effectiveness of implementing and testing three machine learning algorithms (random forests, support vector machine and multi-layer perceptron) on the Raspberry Pi to profile their performance in terms of speed, accuracy and power consumption. The implementation of new machine learning algorithms such as deep learning techniques and convolutional neural networks on edge devices remain a significant challenge to be addressed.

D. SECURITY AND PRIVACY CHALLENGES FOR ASIoTs

The security requirements for different ASIoTs may vary considerably and this gives opportunities for cost-effective and energy efficient customizations (e.g. the requirements for the IoBT would be much stringent and higher than for the IoAT). The IoAT can be deployed with less stringent and computationally lower (or no) cryptographic protocols to reduce the power consumption requirements for the sensor nodes. Similarly, the security and privacy requirements for an IoT-based smart home would be different from that for an IoT to be deployed in a manufacturing environment. The number of potential threats, vulnerabilities and attacks towards an IoT is wide ranging due to the large number of attack surfaces and domains. The authors in [54] give a survey of potential security attacks and countermeasures in three IoT domains: (1) Sensing domain (e.g. jamming, vampire, selective forwarding, sinkhole attacks); (2) Cloud domain (e.g. hidden channel, VM escape, theft of service, VM migration, insider attacks); and (3) Fog domain (e.g. authentication and trust issues, privacy issues, denial-of-service (DoS) attacks). The privacy issues in the fog domain occur because fog devices will be able to infer the location of all the smart objects that are connected to the fog device and by extension track the location of users that are operating the devices.

V. CONCLUSION

This paper has reviewed and summarized the emerging area of application specific Internet of Things (ASIoTs) and given a basic taxonomy into three categories (user domain-driven, communications medium-driven, and technology constraint-driven ASIoTs). Several representative examples of the different classes of ASIoTs have been drawn from the literature for illustration of the challenges and design parameters to be optimized for the various ASIoTs. The design parameters for user domain-driven ASIoTs will require optimization for parameters defined by the specific user domain. The design parameters for communications medium-driven ASIoTs wil require optimization for the network communications in the medium (e.g. terrestrial, underwater, underground mediums) with different properties and characteristics. The design parameters for technology-driven ASIoTs will require optimization to meet the constraints of the technology implementation. The paper has also given a use case illustration for a biometrics-based ASIoT (IoBioT) and some layer customizations for security, key management and Big data information processing. Experiments on face-based biometrics have been performed to validate the Big biometric data computation layer in the IoBioT. Finally, perspectives and directions have also been discussed for future research covering interoperability, energy efficient operation, edge/fog machine learning models, and security/privacy challenges for ASIoTs.

REFERENCES

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

[2] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions," *Future Gener. Comput. Syst.*, vol. 29, no. 7, pp. 1645–1660, 2013.

[3] M. J. S. Smith, *Application Specific Integrated Circuits*. Reading, MA, USA: Addison-Wesley, 1997.

[4] D. V. Dimitrov, "Medical Internet of Things and big data in healthcare," *Healthcare Inform. Res.*, vol. 22, no. 3, pp. 156–163, 2016.

[5] M. C. Domingo, "An overview of the Internet of underwater things," *J. Netw. Comput. Appl.*, vol. 35, no. 6, pp. 1879–1890, 2012.

[6] A. Kott, A. Swami, and B. J. West, "The Internet of battle things," *Computer*, vol. 49, no. 12, pp. 70–75, Dec. 2016.

[7] I. F. Akyildiz and J. M. Jornet, "The Internet of nano-things," *IEEE Wireless Commun.*, vol. 17, no. 6, pp. 58–63, Dec. 2010.

[8] O. Kaiwartya *et al.*, "Internet of vehicles: Motivation, layered architecture, network model, challenges, and future aspects," *IEEE Access*, vol. 4, pp. 5356–5373, 2016.

[9] L. W. Chew, W. Chia, L. M. Ang, and K. P. Seng, "Low-memory video compression architecture using strip-based processing for implementation in wireless multimedia sensor networks," *Int. J. Sensor Netw.*, vol. 11, no. 1, pp. 33–47, 2012.

[10] N. Abuzainab and W. Saad, "Dynamic connectivity game for adversarial Internet of battlefield things systems," *IEEE Internet Things J.*, vol. 5, no. 1, pp. 378–390, Feb. 2018.

[11] M. J. Farooq and Q. Zhu, "Secure and reconfigurable network design for critical information dissemination in the Internet of battlefield things (IoBT)," in *Proc. 15th Int. Symp. Modeling Optim. Mobile, Ad Hoc, Wireless Netw.*, May 2017, pp. 1–8.

[12] A. Azmoodeh, A. Dehghantanha, and K.-K. R. Choo, "Robust malware detection for Internet of (battlefield) things devices using deep Eigenspace learning," *IEEE Trans. Sustain. Comput.*, vol. 4, no. 1, pp. 88–95, Jan./Mar. 2019.

[13] M. S. Hossain and G. Muhammad, "Cloud-assisted industrial Internet of Things (IIoT)—Enabled framework for health monitoring," *Comput. Netw.*, vol. 101, pp. 192–202, Jun. 2016.

[14] S. Hiremath, G. Yang, and K. Mankodiya, "Wearable Internet of Things: Concept, architectural components and promises for person-centered healthcare," in *Proc. 4th Int. Conf. Wireless Mobile Commun. Healthcare*, Nov. 2014, pp. 304–307.

[15] S. Benaissa *et al.*, "Internet of animals: Characterisation of LoRa sub-GHz off-body wireless channel in dairy barns," *Electron. Lett.*, vol. 53, no. 18, pp. 1281–1283, Aug. 2017.

[16] S. Neethirajan, "Recent advances in wearable sensors for animal health management," *Sens. Bio-Sens. Res.*, vol. 12, pp. 15–29, Feb. 2017.

[17] B. Keerthana, S. M. Raghavendran, S. Kalyani, P. Suja, and V. K. G. Kalaiselvi, "Internet of bins: Trash management in India," in *Proc. 2nd Int. Conf. Comput. Commun. Technol.*, Feb. 2017, pp. 248–251.

[18] A. Medvedev, P. Fedchenkov, A. Zaslavsky, T. Anagnostopoulos, and S. Khoruzhnikov, "Waste management as an IoT-enabled service in smart cities," in *Proc. Int. Conf. Next Gener. Wired/Wireless Netw.*, 2015, pp. 104–115.

[19] I. Hong, S. Park, B. Lee, J. Lee, D. Jeong, and S. Park, "IoT-based smart garbage system for efficient food waste management," *Sci. World J.*, vol. 2014, Aug. 2014, Art. no. 646953.

[20] L.-M. Ang, K. P. Seng, A. M. Zungeru, and G. K. Ijemaru, "Big sensor data systems for smart cities," *IEEE Internet Things J.*, vol. 4, no. 5, pp. 1259–1271, Oct. 2017.

[21] R. C. Shah, S. Roy, S. Jain, and W. Brunette, "Data MULEs: Modeling a three-tier architecture for sparse sensor networks," in *Proc. IEEE SNPA Workshop*, May 2003, pp. 30–41.

[22] L.-M. Ang, K. P. Seng, G. K. Ijemaru, and A. M. Zungeru, "Deployment of IoV for smart cities: Applications, architecture, and challenges," *IEEE Access*, vol. 7, pp. 6473–6492, 2018.

[23] C.-C. Kao, Y.-S. Lin, G.-D. Wu, and C.-J. Huang, "A comprehensive study on the Internet of underwater things: Applications, challenges, and channel models," *Sensors*, vol. 17, no. 7, p. 1477, 2017.

[24] V. Rodoplu and M. K. Park, "An energy-efficient MAC protocol for underwater wireless acoustic networks," in *Proc. OCEANS MTS/IEEE*, Sep. 2005, pp. 1–6.

[25] Z. Zhou, B. Yao, R. Xing, L. Shu, and S. Bu, "E-CARP: An energy efficient routing protocol for UWSNs in the Internet of underwater things," *IEEE Sensors J.*, vol. 16, no. 11, pp. 4072–4082, Jun. 2016.

[26] J. Vandermeulen *et al.*, "Discerning pig screams in production environments," *PLoS ONE*, vol. 10, no. 4, 2015, Art. no. e0123111.

[27] M. C. Vuran, A. Salam, R. Wong, and S. Irmak, "Internet of underground things in precision agriculture: Architecture and technology aspects," *Ad Hoc Netw.*, vol. 81, pp. 160–173, Dec. 2018.

[28] I. F. Akyildiz and E. P. Stuntebeck, "Wireless underground sensor networks: Research challenges," *Ad Hoc Netw.*, vol. 4, no. 6, pp. 669–686, Nov. 2006.

[29] H. T. H. Trang, L. T. Dung, and S. O. Hwang, "Connectivity analysis of underground sensors in wireless underground sensor networks," *Ad Hoc Netw.*, vol. 71, pp. 104–116, Mar. 2018.

[30] J. M. Jornet and I. F. Akyildiz, "The Internet of multimedia nano-things," *Nano Commun. Netw.*, vol. 3, no. 4, pp. 242–251, 2012.

[31] I. F. Akyildiz, M. Pierobon, S. Balasubramaniam, and Y. Koucheryavy, "The Internet of bio-nano things," *IEEE Commun. Mag.*, vol. 53, no. 3, pp. 32–40, Mar. 2015.

[32] M. Kuscu and O. B. Akan, "Modeling and analysis of SiNW BioFET as molecular antenna for bio-cyber interfaces towards the Internet of bio-nanothings," in *Proc. IEEE 2nd World Forum Internet Things (WF-IoT)*, Dec. 2015, pp. 669–674.

[33] K. Nahrstedt, H. Li, P. Nguyen, S. Chang, and L. Vu, "Internet of mobile things: Mobility-driven challenges, designs and implementations," in *Proc. IEEE 1st Int. Conf. Internet-Things Design Implement.*, Apr. 2016, pp. 25–36.

[34] L. E. Talavera, M. Endler, I. Vasconcelos, R. Vasconcelos, M. Cunha, and F. J. da Silva e Silva, "The mobile hub concept: Enabling applications for the Internet of mobile things," in *Proc. IEEE Int. Conf. Pervasive Comput. Commun. Workshops*, Mar. 2015, pp. 123–128.

[35] K. Hong, D. Lillethun, U. Ramachandran, B. Ottenwälder, and B. Koldehofe, "Mobile fog: A programming model for large-scale applications on the Internet of Things," in *Proc. 2nd ACM SIGCOMM Workshop Mobile Cloud Comput.*, 2013, pp. 15–20.

[36] Accessed: Mar. 31, 2019. [Online]. Available: http://www.gartner.com and https://www.gartner.com/smarterwithgartner/top-trends-in-the-gartner-hype-cycle-for-emerging-technologies-2017/

[37] D. Shah and V. Haradi, "IoT based biometrics implementation on Raspberry Pi," *Procedia Comput. Sci.*, vol. 79, pp. 328–336, 2016.

[38] R. I. S. Pereira, I. M. Dupont, P. C. M. Carvalho, and S. C. S. Jucá, "IoT embedded linux system based on Raspberry Pi applied to real-time cloud monitoring of a decentralized photovoltaic plant," *Measurement*, vol. 114, pp. 286–297, Jan. 2018.

[39] E. R. Naru, H. Saini, and M. Sharma, "A recent review on lightweight cryptography in IoT," in *Proc. Int. Conf. I-SMAC (IoT Social, Mobile, Anal. Cloud)*, Feb. 2017, pp. 887–890.

[40] J. H. Kong, L.-M. Ang, and K. P. Seng, "A comprehensive survey of modern symmetric cryptographic solutions for resource constrained environments," *J. Netw. Comput. Appl.*, vol. 49, pp. 15–50, Mar. 2015.

[41] O. Iova, P. Picco, T. Istomin, and C. Kiraly, "RPL: The routing standard for the Internet of Things... Or is it?" *IEEE Commun. Mag.*, vol. 54, no. 12, pp. 16–22, Dec. 2016.

[42] L. Coetzee, D. Oosthuizen, and B. Mkhize, "An analysis of CoAP as transport in an Internet of Things environment," in *Proc. IST-Afr. Week Conf. (IST-Africa)*, May 2018, pp. 1–7.

[43] 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 Annu. IEEE Conf. Local Comput. Netw.-Workshops*, Oct. 2012, pp. 956–963.

[44] R. J. Hwang and Y. Z. Huang, "Secure data collection scheme for wireless sensor networks," in *Proc. 31st Int. Conf. Adv. Inf. Netw. Appl. Workshops*, Mar. 2017, pp. 553–558.

[45] I. Blake, G. Seroussi, N. Smart, and J. W. S. Cassels, "Advances in elliptic curve cryptography," in *London Mathematical Society Lecture Note Series*. Cambridge, U.K.: Cambridge Univ. Press, 2005.

[46] Q. Guo *et al.*, "Efficient divide-and-conquer classification based on parallel feature-space decomposition for distributed systems," *IEEE Syst. J.*, vol. 12, no. 2, pp. 1492–1498, Jun. 2018.

[47] J. K. P. Seng and K. L.-M. Ang, "Big feature data analytics: Split and combine linear discriminant analysis (SC-LDA) for integration towards decision making analytics," *IEEE Access*, vol. 5, pp. 14056–14065, 2017.

[48] M. Noura, M. Atiquzzaman, and M. Gaedke, "Interoperability in Internet of Things: Taxonomies and open challenges," *Mobile Netw. Appl.*, pp. 1–14, Jul. 2018.

[49] J. Wan *et al.*, "Software-defined industrial Internet of Things in the context of industry 4.0," *IEEE Sensors J.*, vol. 16, no. 20, pp. 7373–7380, Oct. 2016.

[50] A. Perles *et al.*, "An energy-efficient internet of things (IoT) architecture for preventive conservation of cultural heritage," *Future Gener. Comput. Syst.*, vol. 81, pp. 566–581, Apr. 2018.

[51] L.-M. Ang and K. P. Seng, "Big sensor data applications in urban environments," *Big Data Res.*, vol. 4, pp. 1–12, Jun. 2016.

[52] M. S. Mahdavinejad, M. Rezvan, M. Barekatain, P. Adibi, P. Barnaghi, and A. P. Sheth, "Machine learning for Internet of Things data analysis: A survey," *Digit. Commun. Netw.*, vol. 4, no. 3, pp. 161–175, 2018.

[53] M. T. Yazici, S. Basurra, and M. M. Gaber, "Edge machine learning: Enabling smart Internet of Things applications," *Big Data Cognit. Computing*, vol. 2, no. 3, p. 26, 2018.

[54] M. Dabbagh and A. Rayes, "Internet of things security and privacy," in *Internet of Things-From Hype to Reality*, A. Rayes and S. Salam, Eds. Springer, 2017.

[55] K. P. Seng and L.-M. Ang, "A big data layered architecture and functional units for the multimedia Internet of Things," *IEEE Trans. Multi-Scale Comput. Syst.*, vol. 4, no. 4, pp. 500–512, Oct./Dec. 2018.

[56] F. S. Samaria and A. C. Harter, "Parameterisation of a stochastic model for human face identification," in *Proc. IEEE Workshop Appl. Comput. Vis.*, Dec. 1994, pp. 138–142.

[57] Accessed: Mar. 31, 2019. [Online]. Available: http://vision.ucsd.edu/content/yale-face-database

KENNETH LI-MINN ANG received the B.Eng. (Hons.) and Ph.D. degrees from Edith Cowan University, Australia. He was an Associate Professor and the Head of the Research Division, Nottingham University, before returning to Australia. He was the Associate Professor with the School of Computing & Mathematics, Charles Sturt University (CSU), Australia, and the Leader of the Intelligent Analytics and Sensing (IAS) Research Group, CSU. He is currently an Associate Professor with the School of Information Communication Technology (ICT), Griffith University. He has published over a 100 papers in journals and conferences. His research interests include real-world computer systems and networks, reconfigurable computing and embedded systems, big data and analytics for multimedia sensor networks, and the IoT. He is a Senior Member of the IEEE and a Fellow of the Higher Education Academy, U.K.

JASMINE KAH PHOOI SENG received the B.Eng. (Hons.) and Ph.D. degrees from the University of Tasmania, Australia. She was an Associate Professor with the School of Electrical and Electronic Engineering, Nottingham University. She was a Professor and the Head of the Department of Computer Science and Networked Systems, Sunway University. She was an Adjunct Professor with Charles Sturt University and Edith Cowan University, Australia. She is currently an Adjunct Professor with the School of Engineering and IT, University of New South Wales (UNSW). She has published over 230 papers in journals, book chapters and refereed conferences. Her research interests include machine learning, AI and intelligent systems, big data analytics, the Internet of Things, affective computing, and software design and development.