IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received December 2, 2020, accepted December 24, 2020, date of publication December 30, 2020,
date of current version January 12, 2021.

Digital Object Identifier 10.1109/ACCESS.2020.3048192

Lightweight KPABE Architecture Enabled in Mesh Networked Resource-Constrained IoT Devices

ULA HIJAWI[1], DEVRIM UNAL[2], (Senior Member, IEEE), RIDHA HAMILA[1], (Senior Member, IEEE), ADEL GASTLI[1], (Senior Member, IEEE), AND OMAR ELLABBAN[3], (Senior Member, IEEE)

[1]Department of Electrical Engineering, Qatar University, Doha, Qatar
[2]KINDI Center for Computing Research, Qatar University, Doha, Qatar
[3]CSA Catapult Innovation Centre, Newport NP10 8BE, U.K.

Corresponding author: Ula Hijawi (ula.hijawi@qu.edu.qa)

This work was supported in part by the National Priority Research Program (NPRP) from the Qatar National Research Fund (a member of Qatar Foundation) under Grant NPRP10-1203-160008 and in part by the IBERDROLA QSTP LLC. The publication of this article was funded by the Qatar National Library.

ABSTRACT Internet of Things (IoT) environments are widely employed in industrial applications including intelligent transportation systems, healthcare systems, and building energy management systems. For such environments of highly sensitive data, adapting scalable and flexible communication with efficient security is vital. Research investigated wireless Ad-hoc/mesh networking, while Attribute Based Encryption (ABE) schemes have been highly recommended for IoT. However, a combined implementation of both mesh networking and Key-Policy Attribute Based Encryption (KPABE) on resource-constrained devices has been rarely addressed. Hence, in this work, an integrated system that deploys a lightweight KPABE security built on wireless mesh networking is proposed. Implementation results show that the proposed system ensures flexibility and scalability of self-forming and cooperative mesh networking in addition to a fine-grained security access structure for IoT nodes. Moreover, the work introduces a case study of an enabled scenario at a school building for optimizing energy efficiency, in which the proposed integrated system architecture is deployed on IoT sensing and actuating devices. Therefore, the encryption attributes and access policy are well-defined, and can be adopted in relevant IoT applications.

INDEX TERMS Attribute based encryption, constrained-resources, cybersecurity, elliptic curves cryptography, Internet of Things, mesh networking.

I. INTRODUCTION

Recent research has greatly shed light on lightweight deployments, in which Internet of Things (IoT) devices are employed. IoT solutions have been developed for a wide range of applications, such as Vehicular Ad-hoc networks (VANETs) for intelligent transportation systems [1]–[3], medical sensor networks for healthcare systems [4], and building energy management systems [5]. Such networks collect sensitive information over time that represent users' behavioral patterns necessitating the need for safe data communication. Consequently, different flexible and scalable communication and cryptographic mechanisms have been proposed to overcome challenges accompanied with resource-constrained IoT devices. These challenges include limitations in computational and storage capabilities in addition to restricted battery lifetime affecting deployment scalability [6], [7].

The literature has defined resource-constrained devices as of devices limited capabilities in terms of computational power and memory, or unable to perform costly operations, such as encryption operations [7], [8]. Similarly, Kirilline *et al.* [9] have defined resource-constrained devices as devices of restricted memory, processing power, and/or graphical capabilities. Examples include mobile devices, pagers, and personal digital assistants. Sudharsan *et al.* [10], amongst many others, have particularly specified Microcontroller Units (MCUs) as resource-constrained devices due to their limited memory footprint, fewer computation cores, and low clock speeds. Their work considered the ESP32 MCU as an example. In this work, ESP32 MCUs, widely known in IoT development frameworks, are

The associate editor coordinating the review of this manuscript and approving it for publication was Tawfik Al-Hadhrami.

leveraged as resource-constrained devices with a dual-core of 240 MHz MCU, 520 KB of SRAM, and 448 KB of programmable ROM.

In a traditional Wi-Fi network, every single node, or device, is connected directly to a single Access Point (AP) for data transmission to the cloud. However, this requires every device to be within a certain range to connect to the AP; a disadvantage to the network when devices suffer from limited coverage as in distributed IoT environments. One of the widely adopted solutions is mesh networking for data transmission, which is a local network topology such that nodes link directly to as many other nodes as possible, and collaborate with each other to effectively route data between network nodes [11].

On another hand, according to the National Institute of Standards and Technology (NIST) [12], resource-constrained devices encounter challenges, such as inefficient computing performance and computational complexity that are not incurred by conventional cryptography in computer environments. Fig. 1 summarizes various challenges from the device and network perspectives in terms of device computational power capabilities, connection coverage, and security schemes compatibility.

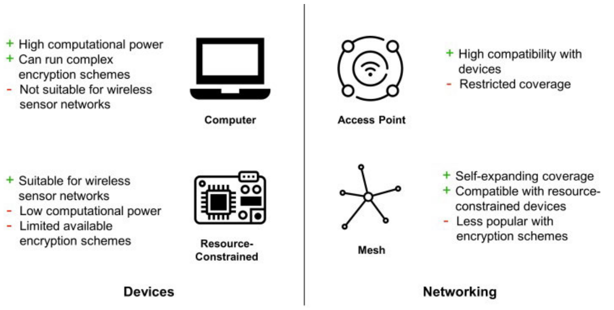
+ High computational power
+ Can run complex encryption schemes
- Not suitable for wireless sensor networks
Computer
Access Point
+ High compatibility with devices
- Restricted coverage
+ Suitable for wireless sensor networks
- Low computational power
- Limited available encryption schemes
Resource-Constrained
Mesh
+ Self-expanding coverage
+ Compatible with resource-constrained devices
- Less popular with encryption schemes
Devices
Networking

FIGURE 1. **Challenges encountered in secure and interconnected IoT devices.**

Attribute Based Encryption (ABE) has been designed as a reliable solution offering expressive and flexible fine-grained access control based on attributes to identify each authorized user [13]. There are two major types of ABE schemes that are widely investigated, and still under continuous development.

The first is the Cipher-text Policy Attribute Based Encryption (CPABE) [14], in which an encrypted cipher-text is associated with an access policy that should be satisfied by a set of attributes associated within the private key of the decrypting entity. The second type is the Key-Policy Attribute Based Encryption (KPABE) [15], in which a decrypting entity can successfully decrypt data when the access policy embedded in its private key is satisfied by the set of attributes associated with the cipher-text. In both ways, the access policy is needed to be satisfied by a set of intrinsic attributes for successful data recovery.

Tan *et al.* [16] compared between CPABE and KPABE schemes in terms of encryption efficiency, employment of attribute and access policy, access control, and hardware deployment. They concluded that KPABE is more promising for resource-constrained devices, as encryption associated with attributes performed on these devices is of less computational power when compared against encryption associated with an access policy. Therefore, KPABE provides efficient and lightweight security in IoT.

In conjunction, Elliptic Curve Cryptography (ECC) is widely known for computationally efficient implementations, as it produces much smaller key bit sizes when compared to other cryptosystems, such as Rivest–Shamir–Adleman (RSA) at the same security level. The arithmetic definition of an elliptic curve E defined over a finite prime field F_P is given by satisfying the equation $y^2 = x^3 + ax + b$, where $4a^3 + 27b^2 \neq 0$, and determined by a set of domain parameters that are common between the involved communicating parties. Although the performance is not affected by key size, key size can be costly when it comes to storing security keys [17].

The KPABE security scheme has been originally devised by Goyal *et al.* [15], however, it was not applied to mesh communication networks, which are defined as wireless devices organized in a mesh topology. In this article, a practical solution is proposed for resource-constrained devices that collect, transmit, and receive data in IoT-based applications. Explicitly, the main contributions of this article are:

- Effectively deploying an integrated system of a self-organizing and cooperative mesh network with lightweight and no-pairing ECC-based KPABE security scheme.
- Developing an integrated, full architecture specifically for resource-constrained IoT devices for distributed areas. This is a novel contribution compared to other works that implement the cybersecurity scheme on a single/standalone device, rather than a complete system as in a multi-device mesh network.
- Presenting an ambitious case study in a school building, in which the proposed mesh network integrated with the KPABE architecture are deployed for resource-constrained devices.
- Benchmarking the proposed system from a communications, security, and performance standpoints in contrast to state-of-the-art.

The remainder of this article is organized into six sections: Section II presents related work, Section III describes the proposed mesh communication architecture, Section IV describes the proposed ECC-based and no-pairing KPABE security architecture, and Section V presents a case study of Qatar Greener Schools scenario, in which the proposed mesh and security architectures are integrated and deployed. Section VI discusses the implementation results, and Section VII concludes the paper.

II. RELATED WORK

To facilitate continuous connection and exchanging content data, Sudarsono and Nakanishi [18] have deployed wireless Delay Tolerant Networks (DTNs) that are secured based on ABE. In this work, rather than focusing on the security of content data as in existing ABE schemes, the ABE-based security of routing messages, which are important to update the routing table of all nodes in the DTN, is addressed. Routing messages are authenticated using Advanced Encryption Standard (AES). Nevertheless, this work has been implemented in laptop PCs environment, and not on resource-constrained devices.

Another work by Kang *et al.* [1] introduces VANETs in a security architecture addressing confidentiality, authentication, and access control for specific vehicles. In vehicular communication, messages are authenticated by adopting Identity-Based Signature (IBS), and messages confidentiality is preserved by deploying the CPABE scheme.

Rao and Dutta [2] have also targeted an ABE scheme in VANETs for vehicular communications, and addressed the problem of large cipher-text size that leads to large communication overhead. Reducing communication overhead was approached by adopting Disjunctive Normal Form (DNF) for the access policy. In doing so, the length of cipher-text is directly proportional against the number of conjunctions instead of the number of attributes. In addition, during the encryption and decryption operations, the number of pairings remains constant.

Xia *et al.* [3] have implemented CPABE to secure vehicles in VANETs, which communicate in vehicular ad-hoc networks. However, to maintain efficient privacy preservation in resource-constrained units in VANETs, the work proposes a CPABE delegation scheme. In this scheme, the decryption operation is delegated to another unit of higher computational capabilities in order to enhance efficiency, and most of the computation is carried by the nearest Road Side Units (RSUs) without jeopardizing confidentiality of data.

Kwon *et al.* [19] have specifically addressed man-in-the-middle and replay attacks that occur due to vulnerabilities in existing mobile multi-hop networks. The work introduced a novel Device-to-Device (D2D) authentication protocol exploiting the CPABE scheme. In different mobile multi-hop network scenarios, the involved entities (or member nodes) in the network are enabled to authenticate each other and pre-share initial secret keys in a scalable environment. The proposed work has mainly targeted mobile devices, such as smartphones and tablet PC.

Seo *et al.* [20] have targeted home automation only operated in ZigBee networking, and applied CPABE on the ZigBee technology. Wang and Chu [21], on the other hand, have applied CPABE in Personal Health Record (PHR) systems, where Linear Secret-Sharing Schemes (LSSS) is adopted to support monotonic access structure. The work is mainly based on a mediated-CPABE system, in which a semi-trusted mediator is assigned to carry heavy computations that cannot be performed on the mobile devices.

Ponomarev [11] has introduced a service mesh networking, in which ABE methods are applied for highly dynamic environments. Several related factors are addressed, such as complex key management and fine-grained access control, however, the solution presents an abstract model that does not address computational capabilities. Another solution proposed by Huda *et al.* [22] has introduced CPABE with authentication. However, the work has been implemented on two laptop PCs (one for encryption, and the other for decryption). The two laptops were communicating with each other wirelessly, but without adopting any Ad-hoc-based communication topology.

ECC has been adopted in the work of Chatterjee and Das [23] along with the ABE scheme for real-time access in hierarchical wireless networks. The proposed solution claims invulnerability against several types of attacks. The security scheme was simulated using the AVISPA tool for validation.

The work of Yao *et al.* [24] was one of the first contributions to address a KPABE scheme with no-pairing ECC to adhere to resource-constrained IoT environments. This was approached by placing point scalar multiplications instead of the expensive bilinear pairings in ECC. A later enhancement of Yao *et al.*'s [24] work was proposed by Tan *et al.* [25] that addresses a security vulnerability in one type of attack.

Overall, previous work in [1]–[3], [11], and [19]–[24] have widely discussed different variations of ABE schemes; however, they have not addressed both mesh network communications and ABE schemes for lightweight implementation on resource-constrained IoT devices. Similarly, other works that deployed ABE schemes for lightweight security in IoT environments are Touati *et al.* [7], Oualha and Nguyen [26], Girgenti *et al.* [8], and Ali *et al.* [27]. However, none of these schemes or the aforementioned works have addressed the topology and architecture of ad-hoc mesh communication, in which ABE schemes are applied for IoT environments.

Combining the three factors altogether, i.e., a collaborative and self-forming mesh communication with an ABE scheme performed on resource-constrained devices, is the main focus of this paper. Unlike implementing the cybersecurity scheme on a single/standalone device as in related works, this work proposes an implementation on an integrated system as a multi-device mesh network for distributed areas. This combination enables the deployment of a wide range of practical IoT applications adopting cutting-edge technologies in communication and security. Table 1 presents a summary and commentary on the reviewed related work.

III. PROPOSED MESH NETWORK ARCHITECTURE

A. OVERVIEW

As described earlier, it is aimed to solve cyber-security challenges related to wireless communication between resource-constrained devices by creating a secure mesh network that uses Attribute-Based Encryption as an encryption scheme. Consequently, in a wireless IoT network, every physical location is equipped with sensing units that need to communicate with each other and with the router.

On that account, the sensors in an IoT network can be interconnected through a mesh network. Hence, every sensing unit, referred to as the device, can route its data and its neighbor's data to another device in intermediate paths, or wireless multi-hops, to eventually reach the sink,

TABLE 1. A summary of related work.

Work	Type of ABE	Networking Used	Nature of Hardware	Commentary
Kang *et al.* [1]	CPABE	VANETs	Vehicles	Devices (VANETs) not specified as resource-constrained devices.
Rao and Dutta [2]	Generic	VANETs	Vehicles	Devices (VANETs) not specified as resource-constrained devices.
Xia *et al.* [3]	CPABE	VANETs	Vehicles	Devices (VANETs) not specified as resource-constrained devices.
Touati *et al.* [7]	CPABE	N/A	Resource-Constrained Devices	No IoT-based communication (e.g., Ad-Hoc network) has been used.
Girgenti *et al.* [8]	GPSW-KPABE, BSW-CPABE, and YCT-KPABE	N/A	Resource-Constrained Devices	No IoT-based communication (e.g., Ad-Hoc network) has been used.
Ponomarev [11]	Generic	Mesh	N/A (abstract model)	Only abstract model is presented without implementation. Resource-constrained devices not specified.
Sudarsono and Nakanishi [18]	Generic	Delay Tolerant Networks (DTNs)	N/A	Resource-constrained devices not specified.
Kwon *at al.* [19]	CPABE	Device-to-Device (D2D)	Smartphones and tablets	Adopts peer-peer communication, but not mesh network functionality.
Seo *et al.* [20]	Generic	ZigBee mesh networks	ZigBee devices	Only compatible with resource-constrained ZigBee devices and protocol.
Wang and Chu [21]	Mediated-CPABE (mCPABE)	Generic	Personal Health Record (PHR) systems (computers)	Implemented on computers and not resource-constrained devices. Lacks mesh network functionality.
Huda *et al.* [22]	CPABE with HMAC	Wireless Network	Laptop Computers	No Ad-Hoc based communication has been used.
Chatterjee and Das [23]	Generic	Wireless Network	Resource-Constrained Devices	Invulnerability against several types of attacks, simulated with AVISPA.
Yao *et al.* [24]	KPABE with No-Pairing ECC	N/A	Resource-Constrained Devices	Foundational work for resource-constrained ABE implementation.
Oualha and Nguyen [26]	CPABE	N/A	Resource-Constrained Devices	No IoT-based communication (e.g., Ad-Hoc network) has been used.
Ali *et al.* [27]	Lightweight Revocable Hierarchical ABE (LW-RHABE)	N/A	Mixture of unlimited storage and computational resources for expensive computations, and recourse-constrained IoT devices	No IoT-based communication (e.g., Ad-Hoc network) has been used. Moreover, not all computational operations are performed by the resource-constrained IoT devices.
This work	KPABE with No-Pairing ECC	WiFi Mesh Network	Resource-Constrained Devices (ESP32)	A lightweight KPABE-enabled mesh networking on resource-constrained devices.

referred to as the root node or the destination. The mesh network creates self-forming downstream hierarchal connection layers joining all available authorized devices. The mesh network has been implemented successfully on ESP32 [29] devices. An Ad-Hoc mesh network is considered as one of the state-of-the-art communication technologies for scalable IoT architectures. An overview of the adopted mesh networking topology presented from its hierarchal topology structure and compatibility with the KPABE security scheme through serialization follows below.

B. TREE TOPOLOGY AND NODE TYPES

The root node acts as the sink that communicates with the wider wireless network. In cases where some of the devices are within the rage of the root node, they still can communicate with it directly and avoid a hop, unlike devices that are out of its range and still need to rout through the wireless hops.

In the proposed implementation, the mesh network creates self-forming downstream hierarchal connection layers joining all available authorized devices as presented in Fig. 2. Data are aggregated to the root node, of which in return, transmits collected data to the cloud.

The deployed mesh communication architecture is based on the ESP-MESH [29] in the ESP-IDF following the hierarchal structure presented in Fig. 2. ESP-MESH itself is a networking protocol built based on the Wi-Fi protocol. Under an application layer protocol, such as HTTP, MQTT, and JSON, data can be encoded [29]. In this work, the HTTP application layer protocol is used. Authorized devices within one zone share a common MESH network name (SSID) and password that identify the zone's MESH network from another. The root node of the MESH network can be automatically selected based on its signal strength, or the user,

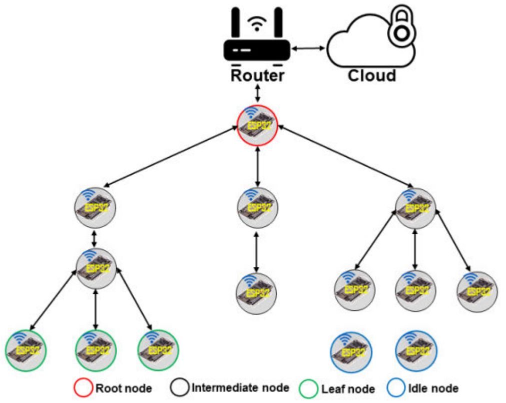

FIGURE 2. Adopted mesh networking topology.

despite of its signal strength, can manually set it as the fixed network's root node.

C. SERIALIZATION AND DESERIALIZATION

To make this scenario applicable for IoT communications, all communications must be prepared to go through the KPABE scheme. All data and metadata must be converted into a suitable format to prepare data for transmission over the network. This process is called serialization [30].

Serializing KPABE objects (to be described in Section IV) involves the following components: the ciphered message, the decryption key, the encryption parameters (Cw), and the private key. To serialize basic data types, such as characters, integers, or floats, the format is converted into its binary form. This can be done readily for the above data types, notwithstanding, converting a complex data type, such as components of the list above, can be quite challenging. Therefore, a serializer for KPABE tailored for constrained devices (e.g., ESP32) has been developed. The serializer comprises a multi-stage binarizer that breaks down each component into its low-level counterparts. Following, the low-level counterparts are converted into a simple container data type (e.g., a character vector), which can be easily transmitted. After binarizing all components, an aggregator combines all of them into a single, large character vector that can be transmitted in one shot.

After the serialization is successfully transmitted over the network, the corresponding entity receives the data object. To convert it back into the components mentioned in the list, a deserializer is required. In conjunction with the proposed serializer, a deserializer has been developed to convert the serialized components back into their respective data types. The deserializer is composed of a disaggregator and a multi-stage debinarizer.

To deserialize the received data object, the character vector is disaggregated into the character vectors corresponding to each component. After that, the vectors are further deserialized into their original complex objects with the use of special debinarization functions.

IV. IMPLEMENTED ECC-BASED AND NO-PAIRING KPABE SECURITY ARCHITECTURE

The implementation of the KPABE scheme is based on Yao *et al.* [24] proposal, in which the computationally expensive bilinear operations are replaced by one point-scalar multiplication for each attribute in the encryption process, and another point-scalar multiplication for each leaf in the access policy. Moreover, the enhancements introduced by Tan *et al.* [25] are reflected in this architecture in a future work. Therefore, the scheme provides a no-pairing cryptographic solution. A previous work [31] has been presented assessing the scheme's performance in terms of execution time with increasing number of attributes.

As depicted in Fig. 3, the security architecture of the enabled scenario is described.

First, the Private Key Generator (PKG) generates a Public Key (PK) that is public to all member entities, and the Master Key (MK) that is private only to itself. Based on the KPABE scheme, it then generates a Decryption Key (DK) for each member entity based on its unique attributes associated with the access policy, and sends the DK to the corresponding entity. The PKG uses the key generation function, i.e., *KeyGen()*, to generate the corresponding DKs, and uses a manually stored MK to avoid exploitation. Until this point, these processes are done in the pre-installation phase, where the entities are offline and not connected in a mesh network, nor connected with the cloud server. The architecture shown in Fig. 3 is illustrated in an end-to-end fashion focusing on the type of entity (i.e., sensor, actuator, TTP), rather than the type of network (i.e., mesh network).

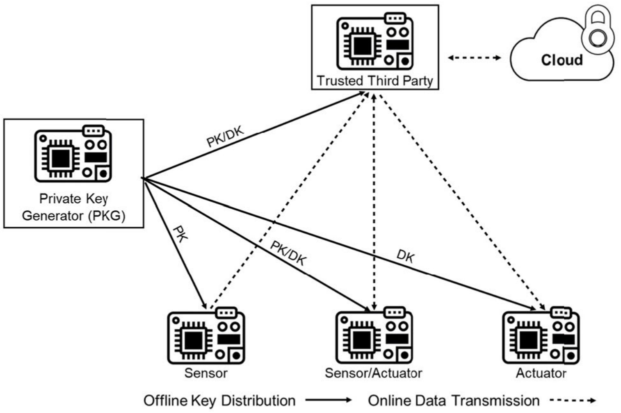

FIGURE 3. The proposed security architecture in the IoT enabled scenario.

In the operational phase, all entities are alive, and start self-forming a mesh network to collect data. The architecture includes (a) a Trusted Third Party (TTP), or sink, that aggregates data from the sensors and transfers it to the cloud server. It also passes control commands from the cloud server back to the sensors. Therefore, it both encrypts and decrypts sensor data; (b) sensors, which are encryptors of their sensing data; (c) actuators, which are decryptors of control commands they receive from the TTP; and sensors/actuators, which have the functionalities of both (b) and (c).

A common distinction can be made between sensors, actuators, and sensors/actuators. Sensors only transmit data to the TTP and do not receive any communication from this specific entity. On contrary, actuators only receive commands from the TTP. The sensor/actuator, however, can both send to and receive from the TTP. Sensors are expected to collect real-time simple numeric data (e.g., temperature, humidity, presence, energy consumption, etc.), while actuators receive commands in the form of simple strings or numbers.

The TTP communicates with the assigned cloud server (i.e., EmonCMS) the aggregated data for further analysis and monitoring. EmonCMS is a powerful open-source platform for processing and logging energy, and other environmental data [32]. It is also connected to a mobile application and web portal for analyzing and visualizing the stored data. The cloud employs a secure firewall in order to protect data against different attacks. It also encrypts all stored data for further protection. It is considered as a backup endpoint for the data. Besides, the TTP (i.e., the sink) can be a single-board computer (e.g., a Raspberry Pi) that has the ability to communicate with entities through a secure channel. It also can be a personal computer, or a server depending on the scale of deployment and complexity of data.

A. PRE-INSTALLATION PHASE

In this phase, the following algorithms are executed offline; when the mesh network is not established yet. By the end of this phase, each device is equipped with the needed encryption and/or decryption keys, and is ready for installation in the enabled scenario.

1) SETUP → {PK, MK}

The setup function, i.e., *Setup()*, is performed by the PKG initializing the algorithm. It randomly generates the Public Key (PK) and Master Key (MK) from a security parameter. PK is publicly known by all entities, and is used for encryption purposes throughout the architecture, whereas the MK is kept secret to the PKG only.

2) KEYGEN(τ, MK) → {DK}

The key generation function, i.e., *KeyGen()*, is performed by the PKG. It takes MK and the access policy τ as inputs, and produces the Decryption Key (DK). The access policy is associated with the unique attributes related to each entity.

B. OPERATIONAL PHASE

In this phase, sensors start collecting electric energy consumption and environmental data in each physical location to be aggregated in the TTP, the sink, and eventually transmitted to the cloud server. Based on the type of these entities (sensor, sensor/actuator, actuator, TTP), the below algorithms are executed.

1) ENCRYPT(M, W, PK) → {CT}

The encryption function, i.e., *Encrypt()*, is performed by sensors, sensors/actuators, and the TTP. PK is used for encrypting a message M that is associated with a set of attributes w intrinsic to the encrypting entity. A cipher-text CT is produced carrying the attributes to be validated across the access policy τ.

2) DECRYPT(DK, CT) → {M OR $\perp$}

The decryption function, i.e., *Decrypt()*, is performed by actuators, sensors/actuators, and the TTP. It uses the private DK to decrypt CT that contains attributes w for the corresponding user. If w satisfies the access policy contained in the DK, the message is successfully decrypted, otherwise, a null message $\perp$ is returned.

The security architecture's algorithms are illustrated in the sequence chart of Fig. 4 correspondingly.

V. CASE STUDY: QATAR GREENER SCHOOLS ENABLED SCENARIO

The mesh network integrated with the KAPBE scheme investigated above are applied in an enabled scenario of a school building as an initiative for targeting energy efficiency and eco-friendly electrical consumption as described below.

A. ZONE-DISTRIBUTED MESH NETWORKS

The wireless sensor network inside the school is divided with respect to different physical zones, in which each physical zone consists of several physical locations (e.g., classrooms, stores, laboratories, etc.). Each physical location in a local zone incubates two types of IoT devices: the environmental sensing unit, and the smart power plug unit.

The first produces sensing data related to temperature, humidity, presence status, and light intensity, whereas the second produces data related to the electric power consumption of appliances/switch boards connected to the plug. All IoT devices are based on the ESP32 MCU [28]. The design and implementation of the addressed IoT devices were introduced in an earlier work [33]. Each zone has a TTP device, called the sink, that aggregates all data collected from the IoT devices in different locations of the zone, and transmits them to the cloud server.

The aforementioned description is illustrated in Fig. 5, in which one of the school building's zone is structured to constitute the security and communication topologies. Applying the previously described mesh network in Section III, the IoT devices form a mesh network, in which data are sent via a multi-hop pathway, and received by the sink securely. The corresponding security architecture algorithms is previously illustrated in the sequence chart of Fig. 4.

Similarly, control commands delivered by the sink undertake the multi-hop mesh network to reach a destined IoT device for fulfillment. Control commands are originated from either a mobile application, or EmonCMS, and then are sent to the sink for delivery. Each zone has its own mesh network of IoT devices, and each mesh network is identified by a network name and password that distinguish each mesh network from another. The IoT device that joins a certain mesh network acquires these access credentials.

B. DEFINITIONS OF ENCRYPTION ATTRIBUTES AND ACCESS POLICY

In this section, the encryption and decryption processes are described in detail with respect to the addressed enabled scenario. As described in Section IV, DKs are installed offline into the IoT devices as well as the TTP to carry secure data transmission. TTP needs a DK to decrypt sensor data aggregated from sensors and sensors/actuators, whereas actuators and sensors/actuators need DKs to decrypt control commands delivered by the TTP. Intrinsic attributes of an encrypting entity, A, are associated within the encryption process, and they are defined as follows.

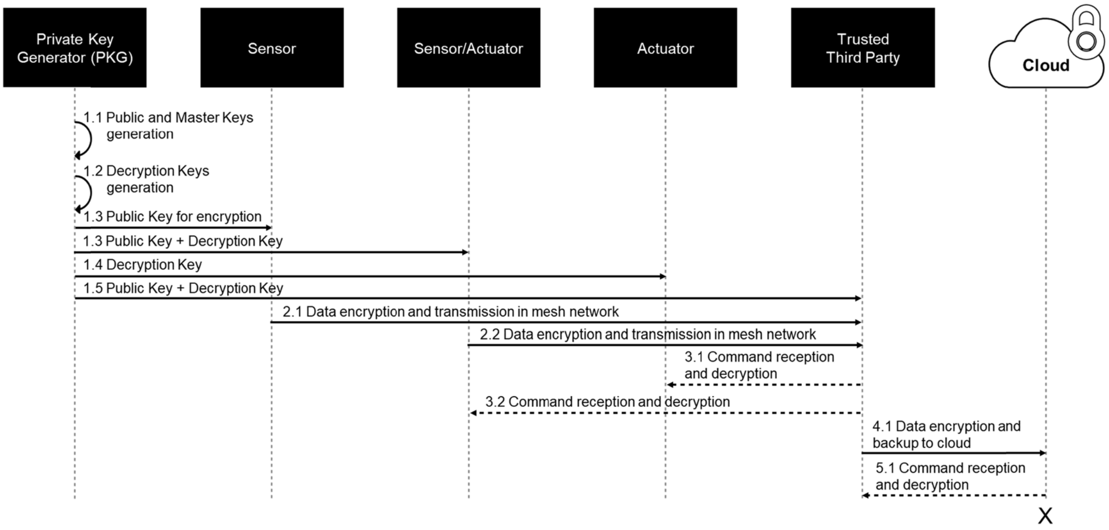
Private Key Generator (PKG)
Sensor
Sensor/Actuator
Actuator
Trusted Third Party
Cloud
1.1 Public and Master Keys generation
1.2 Decryption Keys generation
1.3 Public Key for encryption
1.3 Public Key + Decryption Key
1.4 Decryption Key
1.5 Public Key + Decryption Key
2.1 Data encryption and transmission in mesh network
2.2 Data encryption and transmission in mesh network
3.1 Command reception and decryption
3.2 Command reception and decryption
4.1 Data encryption and backup to cloud
5.1 Command reception and decryption
X

FIGURE 4. Sequence chart of the no-pairing KPABE-based security architecture.

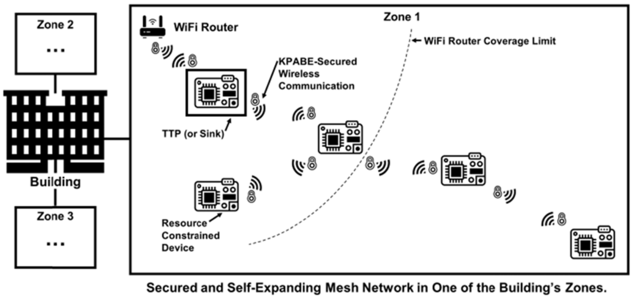
Zone 2
...
Building
Zone 3
...
WiFi Router
Zone 1
WiFi Router Coverage Limit
KPABE-Secured Wireless Communication
TTP (or Sink)
Resource Constrained Device
Secured and Self-Expanding Mesh Network in One of the Building's Zones.

FIGURE 5. Elements of the security and communication topologies constituting one of the school building's zones.

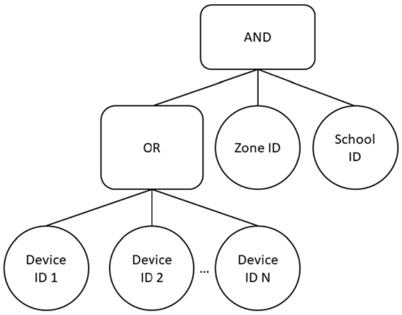

FIGURE 6. Access tree design embedded within the decryption key of the TTP for decrypting data coming from IoT devices.

1) UPSTREAM DIRECTION OF DATA TRANSMISSION

Set of intrinsic attributes A at an encrypting IoT device: A={Device ID, Zone ID, School ID}. By default, each ESP32 MCU has its own intrinsic Device ID number that distinguishes it from any other Device ID number in the same zone of Zone ID in school of School ID. As there are N number of member IoT devices in a local zone, the TTP, a decryptor, checks first if the device is an authorized member. The Device, Zone, and School IDs are assigned offline in the Pre-installation Phase.

Set of leaves in the access policy τ at TTP: leaves are a set of qualities possessed by the encrypting entity that should be satisfied by the access structure in the Operational Phase upon decryption. If one of the Device IDs is satisfied to be a member of the mesh network with the required local Zone ID and school ID, data can be decrypted successfully. The access tree is designed as in Fig. 6.

2) DOWNSTREAM DIRECTION OF DATA TRANSMISSION

Set of intrinsic attributes A at the TTP for encryption: A={TTP ID, Zone ID, School ID}. The TTP, Zone, and School IDs are assigned offline in the Pre-installation Phase.

Set of leaves in the access policy τ at a decrypting IoT device: actuators and sensors/actuators can only decrypt control commands received from the TTP, or the sink. The qualities possessed by the sink should comply with the access policy for successful decryption in the Operational Phase. The access tree is designed as in Fig. 7. Note that, in this case, the access tree is much simpler when compared to the access tree in Section V.B.1). This enables the IoT device to consume less time in the decryption process, whereas the access policy is considered convenient for the TTP, as it is not occupied with other tasks related to data collection or multi-hop networking.

VI. RESULTS AND DISCUSSION

A. EXPERIMENTAL SETUP

In this implementation, a sample setup was deployed at Qatar University. The setup included a PKG bundled with a TTP along with a set of sensors and actuators. Simulated data are used for both the sensors and actuators. The simulated data include numbers and string messages, which are merely used for the experiment's purpose following an access policy described later in this section.

The proposed architecture uses the ESP32, a dual-core 240 MHz MCU, 520 KB of SRAM, and 448 KB of programmable ROM equipped with Wi-Fi and Bluetooth

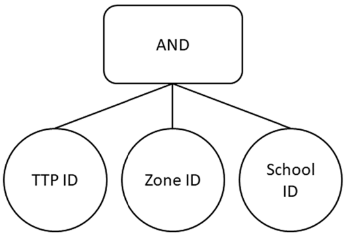

FIGURE 7. Access tree design embedded within the decryption key of an actuator for decrypting control commands coming from the TTP.

networking that supports a broad variety of IoT applications, and ensures ultra-low power consumption. Alternatively, other boards can be employed for this application, although, the ESP32 supports a well-documented architecture for mesh networking, namely ESP-MESH [29]. The KPABE implementation, conversely, can be compiled for various Arduino-compatible boards with WiFi connectivity features. Also, our custom serializer/deserializer can run on any MCU that supports C++ programming.

The goal of this section is to evaluate the current implementation the proposed solution in terms of mesh network performance, KPABE performance, along with the serialization/deserialization component. For the mesh network, we are evaluating the network build time, network healing time, and per-hop latency. For the proposed KPABE implementation, the setup time, encryption, and decryption latencies are benchmarked while varying the number of encryption attributes between 3, 6, and 9. For the custom serializer/deserializer, the serialization and deserialization speeds are calculated.

In this implementation, the following access policy has been used for the TTP using the case study described in Section V:

$R = \text{AND}\{\text{OR}\{\text{node ID}\}, \text{zone ID}, \text{school ID}\}$,

where node ID is $\{1,2,3,4,5,6,7,8,9\}$; a set of the member IoT devices of the mesh network, zone ID is 1, and school ID is 2. The values are chosen arbitrarily for demonstration purposes.

An average of five tests is calculated for the above benchmarking metrics. In addition, the tests are repeated for different encryption attribute configurations, i.e., three, six, and nine parameters. This is carried out to observe the system's performance with respect to data complexity.

A laptop computer running Ubuntu 18.1 is used for uploading the code onto the used ESP32 boards in addition to displaying the output of each board via a serial monitor software package. For the purpose of this study, three ESP32 boards are used, where one of them was assigned as the root note, i.e., the TTP. In this implementation, the root node is manually set as the fixed root node to establish the mesh network for security and deployment purposes, instead of being automatically chosen in the network.

B. IMPLEMENTATION RESULTS AND DISCUSSION

The performance of the implemented mesh network is illustrated in Fig. 8. It is evident that the increase of attributes' number does not affect the performance. This can be explained by the fact that the encryption attributes do not directly influence the operation of the mesh network.

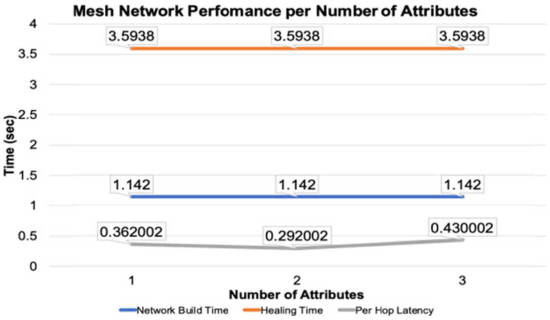

FIGURE 8. Mesh network performance with changing encryption attributes.

Moreover, KPABE performance is depicted in Fig. 9, where the number of attributes is increased with respect to the setup time, encryption time, and decryption time. Note that key generation was omitted from the plot as it revealed very low values (e.g., 0.1 ms).

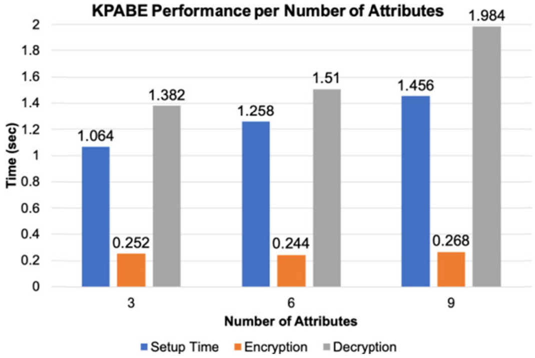

FIGURE 9. KPABE performance with changing encryption attributes.

As the visualization portrays, the parameters most affected by increasing attributes are the setup and decryption operations. On the other hand, encryption and key generation are less influenced by the attributes' number.

It is worthy to mention that the most computationally expensive task is the decryption, averaging at 1.382, 1.510, and 1.984 s for three, six, and nine parameters, respectively. Accompanied by the encryption and decryption process, a serialization and deserialization process is taken place to prepare data for transmission/reception at a given node accordingly. The serializer/deserializer components achieved extremely high performance, reaching as low as 2 ms for both serialization and deserialization for varying number of attributes.

The proposed work has been compared against previous work as presented in Table 1. In the proposed implementation, the three key differentiators: a lightweight KPABE scheme, mesh networking topology, and adaptation for resource-constrained devices have been holistically combined in one system.

On the other hand, limitations of the current implementation include the limited nature of data, i.e., a simple string used as the message, in addition to using only integers as attributes. It is also worthy to mention that the implementation takes a maximum of 10 integer-based attributes due to both hardware and software limitations.

C. SECURITY OVERVIEW

KPABE, on its own, is merely a theoretical architecture; however, to implement such a security scheme in real-life applications, proper integration with both a hardware platform and a communications system is necessary. In this subsection, we shed light on important challenges in implementing KPABE.

From a hardware perspective, ESP32 devices can be vulnerable to a number of cyber-security attacks including leaky noise, fault injection, Zero Pairwise Master Key (PMK) Installation, ESP Access Point (EAP) client crash, beacon frame crash, forever hack, etc., [34]–[39]. Some of those vulnerabilities can be mitigated with upgrading firmware, disabling the Analog-Digital Conversion (ADC) input, in addition to software specific solutions [34]–[39]. However, from a KPABE point of view, a security vulnerability related to the scheme is assessed with a proposed mitigation. Security proofs will be expanded in a future publication.

Moreover, from a communications standpoint, developing a KPABE implementation on a mesh networking architecture involves a number of challenges. First, the ESP-MESH architecture sends messages as a fixed-size string packet. Hence, all of the KPABE variables are required to be consolidated into one large string via a custom serializer. Second, when a message is received, the obtained string must be deconstructed into all the corresponding KPABE variables to ensure successful decryption. In terms of security, this additional step of serializing/deserializing can be a vulnerability if an eavesdropper captures the mesh packet, which can be exploited to find out the encrypted message. Thus, an integrated mesh-KPABE workflow is needed to mitigate the risk caused by transmitting a large string of data.

In the current configuration of the KPABE, the entity's secret key is specified over the access policy, and has no one-to-one correspondence with any individual user. As a result, a registered entity is able to ''share'' its secret key and abuse the privilege of access. This kind of misbehavior is called a key abuse attack. Such vulnerability requires developing an improved scheme, which is proposed by Yu *et al.* [40]. There, the modified KPABE scheme discloses the ID of any illegal key distributor when any key abuse is discovered. Specifically, each user ID bit is characterized as an attribute, and the entity's secret key is linked with their unique ID. The tracing algorithm deceives the pirate device into decrypting the cipher-text linked with the corresponding bits of their ID. In comparison, it does not allow the hidden keys of the pirate tool to be easily exposed. Such security modifications to the KPABE scheme are considered in this work as future work.

VII. CONCLUSION

This article addresses the integration of a communication and security topologies that comply with resource-constrained IoT devices. The work has introduced a case study in which a practical enabled scenario of greener schools is presented for the deployment of IoT sensing devices in a secure and cooperative architecture. Compared to the state-of-the-art, this work focuses especially on KPABE-enabled and mesh-networked resource-constrained IoT devices for distributed areas. Unlike other works that implement the cybersecurity scheme on a single/standalone device, this work proposes a novel contribution through an implementation on an integrated system as a multi-device mesh network. Results show exemplary performance in terms of mesh networking, KPABE performance, and the proposed serializer/deserializer.

Future work is extended to include the improvements executed on the no-pairing KPABE scheme following by deploying the system at a number of schools, where richer data are securely communicated along with attributes that are more expressive.

ACKNOWLEDGMENT

This publication was made possible by the National Priority Research Program (NPRP) grant [NPRP10-1203-160008] from the Qatar National Research Fund (a member of Qatar Foundation) and the co-funding by the IBERDROLA QSTP LLC. The publication of this article was funded by the Qatar National Library. The findings achieved herein are solely the responsibility of the authors.

REFERENCES

[1] Q. Kang, X. Liu, Y. Yao, Z. Wang, and Y. Li, "Efficient authentication and access control of message dissemination over vehicular ad hoc network," *Neurocomputing*, vol. 181, pp. 132–138, Mar. 2016, doi: 10.1016/j.neucom.2015.06.098.

[2] Y. S. Rao and R. Dutta, "Efficient attribute based access control mechanism for vehicular ad hoc network," in *Network and System Security*. Berlin, Germany: Springer, 2013, pp. 26–39, doi: 10.1007/978-3-642-38631-2_3.

[3] Y. Xia, W. Chen, X. Liu, L. Zhang, X. Li, and Y. Xiang, "Adaptive multimedia data forwarding for privacy preservation in vehicular ad-hoc networks," *IEEE Trans. Intell. Transp. Syst.*, vol. 18, no. 10, pp. 2629–2641, Oct. 2017, doi: 10.1109/TITS.2017.2653103.

[4] A. Lounis, A. Hadjidj, A. Bouabdallah, and Y. Challal, "Secure and scalable cloud-based architecture for e-Health wireless sensor networks," in *Proc. 21st Int. Conf. Comput. Commun. Netw. (ICCCN)*, Munich, Germany, Jul. 2012, pp. 1–7, doi: 10.1109/ICCCN.2012.6289252.

[5] J. Han, C.-S. Choi, W.-K. Park, I. Lee, and S.-H. Kim, "Smart home energy management system including renewable energy based on ZigBee and PLC," *IEEE Trans. Consum. Electron.*, vol. 60, no. 2, pp. 198–202, May 2014, doi: 10.1109/TCE.2014.6851994.

[6] Y. Tian, Y. Peng, X. Peng, and H. Li, "An attribute-based encryption scheme with revocation for fine-grained access control in wireless body area networks," *Int. J. Distrib. Sensor Netw.*, vol. 10, no. 11, Nov. 2014, Art. no. 259798, doi: 10.1155/2014/259798.

[7] L. Touati, Y. Challal, and A. Bouabdallah, "C-CP-ABE: Cooperative ciphertext policy attribute-based encryption for the Internet of Things," in *Proc. Int. Conf. Adv. Netw. Distrib. Syst. Appl.*, Bejaia, Algeria, Jun. 2014, pp. 64–69, doi: 10.1109/INDS.2014.19.

[8] B. Girgenti, P. Perazzo, C. Vallati, F. Righetti, G. Dini, and G. Anastasi, "On the feasibility of attribute-based encryption on constrained IoT devices for smart systems," in *Proc. IEEE Int. Conf. Smart Comput. (SMARTCOMP)*, Washington, DC, USA, Jun. 2019, pp. 225–232, doi: 10.1109/SMARTCOMP.2019.00057.

[9] V. Kirilline, H. D. Owens, V. Ivanov, and V. Kozlovsky, ‘‘Virtual machine extended capabilities using application contexts in a resource-constrained device,’’ U.S. Patent 7 895 594 B2, Feb. 22, 2011.

[10] B. Sudharsan, J. G. Breslin, and M. I. Ali, ‘‘RCE-NN: A five-stage pipeline to execute neural networks (CNNs) on resource-constrained IoT edge devices,’’ in *Proc. 10th Int. Conf. Internet Things*, Malmö, Sweden, vol. 5, Oct. 2020, pp. 1–8. [Online]. Available: https://dl.acm.org/doi/abs/10.1145/3410992.3411005

[11] K. Y. Ponomarev, ‘‘Attribute-based access control in service mesh,’’ in *Proc. Dyn. Syst., Mech. Mach. (Dynamics)*, Omsk, Russia, Nov. 2019, pp. 1–4, doi: 10.1109/Dynamics47113.2019.8944652.

[12] K. A. McKay, L. Bassham, M. S. Turan, and N. Mouha, ‘‘Report on lightweight cryptography,’’ Nat. Inst. Standards Technol., Gaithersburg, MD, USA, Tech. Rep. NISTIR 8114, Mar. 2017, vol. 8114. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8114.pdf

[13] S. Belguith, N. Kaaniche, and G. Russello, ‘‘PU-ABE: Lightweight attribute-based encryption supporting access policy update for cloud assisted IoT,’’ in *Proc. IEEE 11th Int. Conf. Cloud Comput. (CLOUD)*, Jul. 2018, pp. 924–927.

[14] J. Bethencourt, A. Sahai, and B. Waters, ‘‘Ciphertext-policy attribute based encryption,’’ in *Proc. IEEE Symp. Secur. Privacy (SP)*, May 2007, pp. 321–334.

[15] V. Goyal, O. Pandey, A. Sahai, and B. Waters, ‘‘Attribute-based encryption for fine-grained access control of encrypted data,’’ in *Proc. 13th ACM Conf. Comput. Commun. Secur. (CCS)*, New York, NY, USA, 2006, pp. 89–98.

[16] Y.-L. Tan, B.-M. Goi, R. Komiya, and S.-Y. Tan, ‘‘A study of attribute-based encryption for body sensor networks,’’ in *Informatics Engineering and Information Science*, vol. 251. Berlin, Germany: Springer, 2011, pp. 238–247, doi: 10.1007/978-3-642-25327-0_21.

[17] H. A. Al Hamid, S. M. M. Rahman, M. S. Hossain, A. Almogren, and A. Alamri, ‘‘A security model for preserving the privacy of medical big data in a healthcare cloud using a fog computing facility with pairing-based cryptography,’’ *IEEE Access*, vol. 5, pp. 22313–22328, 2017, doi: 10.1109/ACCESS.2017.2757844.

[18] A. Sudarsono and T. Nakanishi, ‘‘An implementation of secure data exchange in wireless delay tolerant network using attribute-based encryption,’’ in *Proc. 2nd Int. Symp. Comput. Netw.*, Shizuoka, Japan, Dec. 2014, pp. 536–542, doi: 10.1109/CANDAR.2014.34.

[19] H. Kwon, D. Kim, C. Hahn, and J. Hur, ‘‘Secure authentication using ciphertext policy attribute-based encryption in mobile multi-hop networks,’’ *Multimedia Tools Appl.*, vol. 76, no. 19, pp. 19507–19521, Oct. 2017, doi: 10.1007/s11042-015-3187-z.

[20] H. Seo, C. Kim, and H. Kim, ‘‘ZigBee security for home automation using attribute-based cryptography,’’ in *Proc. IEEE Int. Conf. Consum. Electron. (ICCE)*, Las Vegas, NV, USA, Jan. 2011, pp. 367–368, doi: 10.1109/ICCE.2011.5722631.

[21] Z.-W. Wang and Z.-Z. Chu, ‘‘Efficient mediated ciphertext-policy attribute-based encryption for personal health records systems,’’ *Internet Technol. J.*, vol. 16, no. 5, pp. 877–883, 2015.

[22] S. Huda, A. Sudarsono, and T. Harsono, ‘‘Secure data exchange using authenticated ciphertext-policy attributed-based encryption,’’ in *Proc. Int. Electron. Symp. (IES)*, Surabaya, Indonesia, Sep. 2015, pp. 134–139, doi: 10.1109/ELECSYM.2015.7380829.

[23] S. Chatterjee and A. K. Das, ‘‘An effective ECC-based user access control scheme with attribute-based encryption for wireless sensor networks,’’ *Secur. Commun. Netw.*, vol. 8, no. 9, pp. 1752–1771, Jun. 2015, doi: 10.1002/sec.1140.

[24] X. Yao, Z. Chen, and Y. Tian, ‘‘A lightweight attribute-based encryption scheme for the Internet of Things,’’ *Future Gener. Comput. Syst.*, vol. 49, pp. 104–112, Aug. 2015.

[25] S.-Y. Tan, K.-W. Yeow, and S. O. Hwang, ‘‘Enhancement of a lightweight attribute-based encryption scheme for the Internet of Things,’’ *IEEE Internet Things J.*, vol. 6, no. 4, pp. 6384–6395, Aug. 2019, doi: 10.1109/JIOT.2019.2900631.

[26] N. Oualha and K. T. Nguyen, ‘‘Lightweight attribute-based encryption for the Internet of Things,’’ in *Proc. 25th Int. Conf. Comput. Commun. Netw. (ICCCN)*, Waikoloa, HI, USA, Aug. 2016, pp. 1–6, doi: 10.1109/ICCCN.2016.7568538.

[27] M. Ali, M.-R. Sadeghi, and X. Liu, ‘‘Lightweight revocable hierarchical attribute-based encryption for Internet of Things,’’ *IEEE Access*, vol. 8, pp. 23951–23964, 2020, doi: 10.1109/ACCESS.2020.2969957.

[28] *Espressif Official Website*. Accessed: Mar. 1, 2019. [Online]. Available: https://www.espressif.com/en/products/hardware/esp32/overview

[29] *Espressif Official Website, ESP-MESH Programming Guide*. Accessed: Apr. 1, 2019. [Online]. Available: https://docs.espressif.com/projects/esp-idf/en/latest/esp32/api-reference/network/esp_mesh.html

[30] (Apr. 5, 2015). *Standard C++*. Accessed: Oct. 24, 2020. [Online]. Available: https://web.archive.org/web/20150405013606/http://isocpp.org/wiki/faq/serialization

[31] U. Hijawi, D. Unal, R. Hamila, A. Gastli, and O. Ellabban, ‘‘Performance evaluation of no-pairing ECC-based KPABE on IoT platforms,’’ in *Proc. IEEE Int. Conf. Informat., IoT, Enabling Technol. (ICIoT)*, Doha, Qatar, Feb. 2020, pp. 225–230, doi: 10.1109/ICIoT48696.2020.9089641.

[32] *EmonCMS Official Website*. Accessed: Jun. 1, 2020. [Online]. Available: https://emoncms.org

[33] U. Hijawi, A. Gastli, R. Hamila, O. Ellabban, and D. Unal, ‘‘Qatar green schools initiative: Energy management system with cost-efficient and lightweight networked IoT,’’ in *Proc. IEEE Int. Conf. Informat., IoT, Enabling Technol. (ICIoT)*, Doha, Qatar, Feb. 2020, pp. 415–421, doi: 10.1109/ICIoT48696.2020.9089443.

[34] D. R. E. Gnad, J. Krautter, and M. B. Tahoori, ‘‘Leaky noise: New side-channel attack vectors in mixed-signal IoT devices,’’ *IACR Trans. Cryptograph. Hardw. Embedded Syst.*, vol. 2019, no. 3, pp. 305–339, 2019, doi: 10.13154/tches.v2019.i3.305-339.

[35] *Security Advisory Concerning Fault Injection and eFuse Protections (CVE-2019-17391) | Espressif Systems*. Accessed: Jul. 16, 2020. [Online]. Available: https://www.espressif.com/en/news/Security_Advisory_Concerning_Fault_Injection_and_eFuse_Protections

[36] *ESP32 Fault Injection Vulnerability—Impact Analysis | Espressif Systems*. Accessed: Jul. 16, 2020. [Online]. Available: https://www.espressif.com/en/news/ESP32_FIA_Analysis

[37] (Sep. 5, 2019). *Espressif IoT Devices Susceptible to Wi-Fi Vulnerabilities Can Allow Hijackers to Crash Devices Connected to Enterprise Networks, Security Boulevard*. Accessed: Jul. 16, 2020. [Online]. Available: https://securityboulevard.com/2019/09/espressif-iot-devices-susceptible-to-wifi-vulnerabilities-can-allow-hijackers-to-crash-devices-connected-to-enterprise-networks/

[38] InfoQ. *ESP32 IoT Devices Vulnerable to Forever-Hack*. Accessed: Jul. 16, 2020. [Online]. Available: https://www.infoq.com/news/2019/12/esp32-fatal-fury/

[39] M. Eduardo. (Jul. 12, 2020). *Matheus-Garbelini/ESP32_ESP8266_Attacks*. Accessed: Jul. 16, 2020. [Online]. Available: https://github.com/Matheus-Garbelini/esp32_esp8266_attacks

[40] S. Yu, K. Ren, W. Lou, and J. Li, ‘‘Defending against key abuse attacks in KP-ABE enabled broadcast systems,’’ in *Security and Privacy in Communication Networks*. Berlin, Germany: Springer, 2009, pp. 311–329, doi: 10.1007/978-3-642-05284-2_18.

ULA HIJAWI received the B.S. degree in electrical engineering from Qatar University, Doha, Qatar, in 2017, where she is currently pursuing the M.S. degree in electrical engineering.

Since 2017, she has been working as a Research Assistant with the Electrical Engineering Department, Qatar University, in different fields including machine learning, the IoT communication networks, and the IoT-oriented cybersecurity. Her research interests include machine learning, Industrial IoT applications, wireless sensor networks, and building energy management in smart grids.

DEVRIM UNAL (Senior Member, IEEE) received the M.Sc. degree in telematics from Sheffield University, U.K., in 1998, and the Ph.D. degree in computer engineering from Bogazici University, Turkey, in 2011.

He is currently a Research Assistant Professor of Cyber Security with the KINDI Center for Computing Research, College of Engineering, Qatar University. His research interests include cyber-physical systems and the IoT security, wireless security, artificial intelligence, and next-generation networks.

RIDHA HAMILA (Senior Member, IEEE) received the M.Sc., the LicTech (Hons.), and Dr.Tech. degrees from the Tampere University of Technology (TUT), Tampere, Finland, in 1996, 1999, and 2002, respectively.

From 1994 to 2002, he held various research and teaching positions at the Department of Information Technology, TUT, Finland. From 2002 to 2003, he was a System Specialist with the Nokia research Center and Nokia Networks, Helsinki. From 2004 to 2009, he was with Emirates Telecommunications Corporation, UAE. Also, from 2004 to 2013, he was an Adjunct Professor with the Department of Communications Engineering, TUT. He is currently a Full Professor with the Department of Electrical Engineering, Qatar University, Qatar. His current research interests include mobile and broadband wireless communication systems, edge computing, Internet of Everything, and machine learning. In these areas, he has published more than 200 journal and conference papers most of them in the peered reviewed IEEE publications, and filed seven U.S. patents. He has been involved in several past and current industrial projects, Ooredoo, Qatar National Research Fund, Finnish Academy projects, EU research, and education programs.

ADEL GASTLI (Senior Member, IEEE) received the B.Sc. degree in electrical engineering from the National School of Engineers of Tunis, Tunisia, in 1985, and the M.Sc. and Ph.D. degrees in electrical and computer engineering from the Nagoya Institute of Technology, Japan, in March 1990 and March 1993, respectively.

From September 1985 to September 1987, he worked with the National Institute for Standards and Intellectual Property, Tunisia. He worked with Mitsubishi Electric Corporation, Japan, from April 1993 to July 1995. He joined the Electrical and Computer Engineering Department, Sultan Qaboos University, Oman, in August 1995. He served as the Head of the Department from September 2001 to August 2003 and from September 2007 to August 2009. He was appointed as the Director of the Sultan Qaboos University Quality Assurance Office from February 2010 to January 2013. In February 2013, he joined the Electrical Engineering Department, Qatar University, as a Professor and the Kahramaa-Siemens Chair in energy efficiency. From August 2013 to September 2015, he was appointed the College of Engineering Associate Dean of Academic Affairs. He has established the Clean Energy and Energy Efficiency Research Group, QU, in March 2013. His current research interests include energy efficiency, renewable energy, electric vehicles, and smart grids. He is an ABET Program Evaluator.

OMAR ELLABBAN (Senior Member, IEEE) received the B.S. degree (Hons.) in electrical machines and power engineering from Helwan University, Egypt, in 1998, the M.S. degree in electrical machines and power engineering from Cairo University, Egypt, in 2005, and the Ph.D. degree (Hons.) in electrical engineering from the Free University of Brussels, Belgium, in 2011.

He is currently a Senior Researcher and the Creative Manger with more than 20 years of combined experiences (teaching, research, industrial experience, consulting services, and project management) between academia, research institutes, industry, and power utility companies in various fields. He is conducting and leading many research projects in different areas, such as power electronics, electric vehicles, automatic control, motor drive, energy management, grid control, renewable energy, energy storage devices, distributed energy systems, and their integration into the smart grid. He joined the Research and Development Department, Punch Powertrain, Sint-Truiden, Belgium, in 2011, where he and his team developed a next-generation, high-performance hybrid powertrain. In 2012, he joined Texas A&M University, Qatar, as a Postdoctoral Research Associate and became an Assistant Research Scientist in 2013, where he is also involved in different renewable energy integration projects. In 2016, he joined Iberdrola Innovation Middle East as a Research and the Development Director to lead various research, development, and innovation projects under various topics focusing on transforming the current electric grid into a smart grid and integrating renewable energies and energy storage systems interfaced by power electronics converters as microgrids penetrating the distribution networks. In addition to, improving and optimizing building energy management systems. In 2020, he joined CSA Catapult as a Principal Power Electronics Engineer to lead different project focusing on Compound Semiconductors application in different sectors. He has authored more than 70 journal and conference papers, one book chapter, two books entitled, *Impedance Source Power Electronic Converters*, 2016 and *Smart Grid Enabling Technologies*, 2020 and many international conference tutorials. His current research interests include renewable energies, grid control, smart grid, automatic control, motor drives, power electronics, and electric vehicles. He is IET member and currently serves as an Associate Editor for the IEEE TRANSACTIONS ON INDUSTRIAL ELECTRONICS.