Information Systems Frontiers
https://doi.org/10.1007/s10796-021-10199-5

Future Industry Internet of Things with Zero-trust Security

Shan Li[1] · **Muddesar Iqbal**[2] · **Neetesh Saxena**[1]

Accepted: 7 August 2021

Abstract
The emerging techniques, such as the fifth-generation communications (5G), Internet of Things (IoT), blockchain, artificial intelligence, *etc*., are operating in unison will drive the transformation of global business forward. The 5G technology is expected to unleash a massive IoT ecosystems by providing massive connectivity for huge number of IoT devices with faster data rate, ultra-low latency, and low-cost access. The 5G networks will be designed to bring the level of performance needed for massive IoT and will enable a perceived fully ubiquitous connected world. Meanwhile, the blockchain being promoted as the fundamental for new business model in Future IoT (FIoT). This paper attempts to provide a set of new directions and ideas for research in 5G/6G enabled IoT and new technique trends in IoT. The current IoT are facing a number of challenges, such as massive IoT devices access, network performances, security, standardization, and critical applications. This paper investigates new technologies, such as 5G, zero-trust, and blockchain will catalyse the innovation in IoT. Specifically, a zero-trust security architecture for FIoT is proposed and a blockchain-based device authentication in IoT environment (BasIoT) is proposed that can provide massive secure device access in FIoT.

Keywords Privacy preserving · Internet of things (IoT) · Industrial 4.0 · Data anonymisation

1 Introduction

The cellular and WiFi are two primary wireless networking technologies required almost by every IoT devices. The fifth generation networks (5G) will hit the market by 2020 (Sarrigiannis et al., 2020; Al-Turjman et al., 2019; El-Tanab & Hamouda, 2020). Many current IoT services are making performance trade-offs to get the best from data speed, latency, massive access, and cost (Kiran & Rajalakshmi, 2019; Da Xu et al., 2014). The IoT is believed one of the most rapidly developing ecosystems to greatly benefit from 5G (Kaplan, 2014; Li et al., 2018). The main evolution is beyond the massive IoT access, data speed improvements, lowered latency, and expansion of cell sites compared with the current 4G and 4.5G networks. Together with the emerging new technologies, such as artificial intelligence (AI), blockchain, *etc.*, the 5G will significantly improve the efficiency and capability of the IoT (Scoop, 2018) and the 5G services over the world market will reach up to $123.27 billion by 2025 (Scoop, 2018).

There is a significant demand of services for high speed data traffic, reliable and ultra-low latency connectivity, and massive IoT devices access capabilities (Kaplan, 2014). In 5G-IoT, new business models and applications will require a higher level of performance, such as high data rate, ultra-low latency, massive access, security, coverage, trustworthy, ultra-reliability, *et al*. for massive IoT devices (Nipun Jaiswal, 2014). As an example, the "ultra-low latency" will extremely enhance the applications in industry by providing real-time interactivity for services, such as industrial IoT (IIoT), smart grid, self-driving cars, vehicle intelligence, *etc.* The main requirements in industry include (Notes, 2018; Li et al., 2018; Jaiswal et al., 2020):

- *High data speed*, 1-10 Gbps data rate for IoT connections
- *Ultra-low-latency*, 1 millisecond device-to-device delay
- *High band*, 1000x bandwidth
- *Massive connections*, 10 - 100x devices number,
- *High availability and coverage*, nearly 100%
- *Ultra-low energy consumption*, up to 10-year of battery life

✉ Shan Li
ieee.scli@gmail.com

[1] School of Computer Science and Informatics, Cardiff University, Cardiff, CF24 3AA, UK

[2] School of Computer Science and Informatics, London South Bank University, London SE1 0AA, UK

Published online: 10 March 2022

We are approaching the final stage of 5G and a number of key technologies are still in development, include the physical connection methods like radio access technology (such as LTE, 3G, and GSM), multiple antenna, re-architecting of networks (Da Xu et al., 2014; Kaplan, 2014; Akpakwu et al., 2018; Hošek, 2016). Unlike the existing 4G, 4.5G (LTE), the 5G is designed to provide performances needed for large scale IoT. According to the Cisco, up to 500 billion devices are expected to be connected to the IoT by 2030 (Egham, 2017; Lyu et al., 2018; CISCO, 2016). In the past decade, a large volume of researches have been made on key technologies related to 5G and IoT. Many key enabling technologies, such as software-define network (SDN) (Akyildiz et al., 2014; Matias et al., 2015; Akyildiz et al., 2015), network function virtualization (NFV) (Akyildiz et al., 2015; Matias et al., 2015), device-to-device (D2D) connectivity (Mach et al., 2015; Pyattaev et al., 2015), *etc*. have been developed that cover the IoT, wireless communications, networking techniques, security, and applications in IoT (Simsek et al., 2016).

In the upcoming 5G/6G enabled IoT all data sources and computing services are considered resources, in which all access to resources will be dynamic and strictly enforced before granting access (Zhang et al., 2020; Lin et al., 2020). The traditional perimeter-based security approaches are not secure enough anymore due to the fact that if a device is compromised, the attacker can access all resources without passing through the perimeter (Li, 2020; Dhar & Bose, 2020). Unlike perimeter-based security approaches, the zero-trust security model follows 'verify and never trust' principle and assumes any access within the system is untrustworthy and needs to be verified (Bhattacharjya, 2020). The zero-trust security model is a promising approach of modernising IoT security without limiting to the scope of IoT system. The main contribution of this work are summarised as:

1. This paper attempts to provide a set of new directions and ideas for research in 5G/6G-enabled IoT and new technique trends in IoT; Specifically, a zero-trust security model for FIoT is proposed;
2. A blockchain enabled zero-trust security framework (BasIoT) is proposed that achieves zero-trust devices/users/apps authentication in complicated 5G-IoT systems, which provides an efficient zero-trust authentication solution that following the 'never trust, always verify' principle in IoT;
3. Realizing zero-trust in IoT. This work also introduces the key research challenges and future research trends that can satisfy the requirements of new applications in 5G enabled industrial IoT architecture, including *5G-IoT architectures, trusted D2D communication, etc.*

2 Background and Related Works

The existing IoT systems are facing with very heterogeneous devices and applications, where a number of current wireless networks co-exist together, such as WiFi, BLE, 3G, 4G, 5G/6G *etc*. These co-existing technologies provide Internet interconnection to a large number of IoT devices (of All Thing, 2015). It is reported that the 2G networks cover 90% of the world's population and the 3G currently covers of 65% of the world's population that can provide both voice and data. Compare to 3G, the current 4G is a better technology and all smart mobile phones are now support 4G as well as 3G (Da Xu et al., 2014; Duan et al., 2018). In many current IoT applications, both 3G and 4G networks are widely deployed (of All Thing, 2015). Compare with 3G, 4G significantly have enhanced the capabilities of cellular networks by providing IoT devices applicable wireless network access.

The 4G and 4G LTE can coexist with 5G for a while, which means the 4G LTE will continue to evolve and get better in the following few years. The 5G will be deployed broadly along with legacy 4G that can make it smoother to transition to 5G (Notwel, 2017). The typical data speed provided by current 4G and 4.5G (LTE) networks is between 10 and 30$mbps$. Actually, there are a number of competing wireless networking technologies, such as 5G NR (New Radio), 3GPP (Rouse, 2014), WiMaxb (Alliance, 2011), SigFox (Sigfox, 2018), LoRa (Vangelista et al., 2015), *etc*. are also available for IoT connectivity.

In Jackson (2017), T-mobile reported that the initial 5G speed will be 20-25% faster than the current 4G LTE, which have demonstrated real download speed up to 429$Mbps$ and upload speed up to 66.4$Mbps$ (Mills, 2018). The 5G based massive connectivity can provide IoT devices with more reliable and faster speed than 4G up to *10 Gbps* (Egham, 2017; of All Thing, 2015; Rouse, 2014). Meanwhile, the 5G is intended to introduce new security procedures (Li et al., 2018).

5G features massive capacity and connectivity, which can fully satisfy the demand for digital content and services in the IoT. Figure 1 describes the massive machine-type communication (MTC) in many IoT scenarios, such as smart cities, industrial IoT (IIoT), healthcare, *etc.*, in which a large number of Internet-enabled smart devices will be interconnected. In the past decade, a number of communication technologies have been developed for IoT devices that provide low-throughput, low-power, wide-area coverage for IoT, including short-range MTC, Low-Power wide-area network (LPWAN) (Akpakwu et al., 2018) or low-power network (LPN), Ingenu random phase multiple access (RPMA) (McClelland, 2017), SigFox (Sigfox, 2018), LoRaWAN (Vangelista et al., 2015), *etc.*

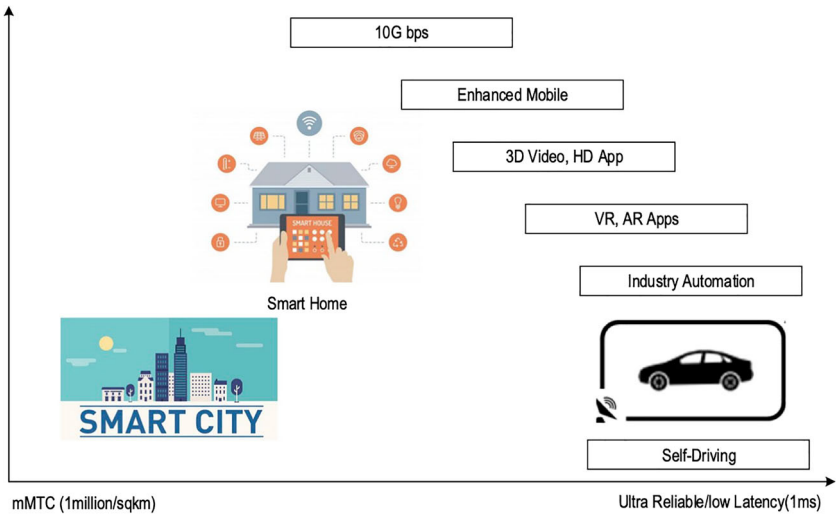

Fig. 1 MTC in 5G-IoT

Aimed at developing globally acceptable 3G systems for IoT connectivities, the 3GPP proposed narrow-band LTE IoT technologies (NB-IoT) and enhanced MTC (eMTC) to fill the 5G gap for IoT. The global 5G NR introduces eMBB (enhanced mobile broadband) and ultra-reliable, low-latency communication (URLLC) to provide high-performance IoT applications (of All Thing, 2015).

2.1 5G Wireless Networks

In the past few years, a number of IoT standards and protocols have been published, which involves the IoT network architecture and stack as listed in Table 1 and layered protocols in IoT in Table 2, in which most of protocols/stacks are facing security and privacy challenges. The 5G-based IoT networks can provide reliable and faster wireless connection based on SDN paradigm (Akyildiz et al., 2014). There are a number of WSDN solutions have been developed for 5G, including Scalable SoftAir (Akyildiz et al., 2015), Cloud-RAN (Wu et al., 2015), content distribution, D2D (Commission, 2018), *etc.*

In Asia (2017), a geographic based IoT solution was proposed that aimed at providing service-driving interconnectivity for IoT devices. Unlike conventional network, the energy consumption is a big issue in IoT (Vangelista et al., 2015) and a number of energy-efficient IoT solutions have been proposed (Dongbaare et al., 2016; Abu-Mahfouz et al., 2016; Jin et al., 2014), and in (Abu-Mahfouz et al., 2016; Jin et al., 2014) wireless spectrum sharing/reuse technologies have been developed, which are the main enabling techniques in 5G-IoT. Narrowband IoT (NB-IoT) is a wireless standard proposed by the 3GPP for low power wide area network, which can be used in independently licensed bands as well as unused 200KHz bands. In recent, a large volume of research efforts have been conducted in NB-IoT (Yongfu et al., 2012; Schinianakis, 2017; Khalfi et al., 2017; Xu et al., 2017), the NB-SCMA solution for uplink communication in 5G is developed in (Yongfu et al., 2012), a spectrum-efficient channel model is proposed by Chen for 5G-IoT in (Chen et al., 2016), and Zhang *et al.* developed an integrated architecture from the view point of energy efficient (Zhang et al., 2016).

Table 1 IoT connectivity protocols vs internet protocols

Layer	Internet protocol suite	IP smart objects protocol suite
Application	HTTP/FTP/SMT/ etc.	CoAP
Transport	TCP/UDP	UDP
Network	IPv4/IPv6	6LoWPAN, RPL
Link	IEEE 802.3/802.11	IEEE 802.15.4e

2.2 5G-enabled IoT (5G-IoT)

Many research efforts focus on bridging the 5G and IoT, or the IoT enabled by 5G, namely 5G-IoT (Da Xu et al., 2014; Kaplan, 2014; Hošek, 2016), including theory methods, enabling technologies, standardization, and implementation in IoT scenarios. The emerging blockchain technologies are

Table 2 IoT protocols and stack

Layers	Protocols
Infrastructure	6LowPAN, IPv4/IPv6, RPL
Identification	EPC, uCode, IPv6, URIs
Communications/Transport	Wifi, Bluetooth, LPWAN
Discovery	Physical Web, mDNS, DNS-SD
Data Protocols	MQTT, CoAP, AMQP, Websocket, Node
Device Management	TR-069, OMA-DM
Semantic	JSON-LD, Web Thing Model
Multi-layer Frameworks	Alljoyn, IoTivity, Weave, Homekit

believed to significantly boost the applications over 5G-IoT (Da Xu et al., 2014). A number of industrial gaints, like Intel, Verizon, Huawei, and CISCO, have jointly worked on the 5G-IoT, as an example, the joint project "Neuroscience-based algorithms" aims at developing human eye-adaptive video quality control techniques in FIoT (Kaplan, 2014).

The massive connectivity features in 5G-IoT can perfectly match the demands from billions of smart devices (Hošek, 2016). The current wireless networks are unable to satisfy the needs of massive IoT in many applications, such as smart cities, *etc.* In current IoT areas, many wireless technologies (such as BLE, ZigBee, *etc.*) together with mobile wireless networks (such as *WiFi, 6LoWPAN, and cellular networks* (e.g., MTC using 3GPP, 4G (LTE)), *etc.*) are widely used to satisfy the needs of IoT and the IoT network architecture very heterogeneous.

Many current smart IoT applications can only provide limited services due to the lack of high reliable and fast data rate. Particularly in IIoT, many applications require devices can provide reliable and secure services even in extreme environmental conditions. Actually, the IIoT is faced a number of technical challenges, such as reliable IoT system, secure data transmission, trust platform management, lack of standards, *etc.* Juliane Stephan (2016). In some IIoT applications, such as train-to-land communication, power supply units, *etc.*, extra robustness, reliabilities, timeless, and secure data transmission are still facing many technical challenges.

In many IoT applications, the 3GPP, 4G, and 4G LTE based networks are widely used to provide communications between devices (Astely et al., 2013), which offer IoT applications with high data transmission rate, wide coverage, and some levels of security protection (Palattella et al., 2016). However, these communication techniques are unable to provide the MTC communication when large number of IoT devices are involved. The emerging 5G networks are promising to provide MTC communication with ultra-high speed, low-latency, and wide coverage for massive number IoT devices.

2.3 Secure FIoT Architecture

The 5G-IoT is targeting at providing IoT applications with massive connectivity with high level of performances, including high data rate, low latency, spectrum efficient, energy efficient, re-configurability, and security, which requires the 5G-IoT should be designed in a scalable and flexible way. Typically the 5G-IoT architectures are featured:

- *Logical independent*, the architecture should support logically independent networks according the IoT applications requirements.
- *Cloud radio access networks (CloudRAN)*, which will enable the 5G-IoT to reconstruct the radio access network and offer massive connectivity for IoT devices
- *Simplicity*, the simplified architecture of core network, which aims at meeting new demands for configuration flexible network functions.

Figure 2 describes the future international mobile telecommunications (IMT) framework of standards, where 5G networks can provide following new features: (1) the architecture of the future IMT, in which the 5G networks can provide following new features: (1) Enhanced mobile broadband (eMBB); (2) ultra-reliable and ultra-low-latency communications, 4ms for eMBB and 1ms for URLLC; (3) connection density, massive MTC.

2.4 Key Security Requirements in FIoT

The IoT is significantly changing the way we communicate with physical system by offering a wide range of IoT applications, which leverage on ecosystems of smart and highly heterogeneous devices. However, there are still many new technical requirements and challenges to be fixed in FIoT, such as:

- *High speed data rate*, many new IoT applications, such as media streaming, gaming, big data, augmented reality (AR), virtual reality (VR), *etc.*, require ultra-high data transmission speed (Akyildiz & Nie, 2016).
- *Scalability*, 5G-IoT contains massive users, devices, services, applications, and operations, to well accommodate all these requirements are very challenging. The fine-grained NFV based technologies can improve the scalability of 5G-IoT.
- *Ultra-low-latency*, particularly in real-time applications, in industrial automation, intelligent transportation systems, healthcare, AR, serious gaming, *etc.*, require ultra-low-latency with round trip latency of *1ms* (Da Xu et al., 2014) .
- *High reliability*, many IIoT applications have strict requirements of reliability, such as in smart grid, train-land communications, robotics, etc., where 5G-IoT requires high reliability and robust recovery mechanism.
- *Security*, many IoT systems (such as industrial control systems (ICS), supervisory control and data acquisition (SCADA) systems) are facing severe security threats, like cyber attacks, device security, distributed denial of service (DDoS), or data security. The FIoT is required to be secure by design.
- *Low-energy consumption*, for smart devices in IoT supplied by battery, the energy consumption is an essential issue that affect the running of IoT system, as a result, energy saving IoT is a trend in 5G-IoT.

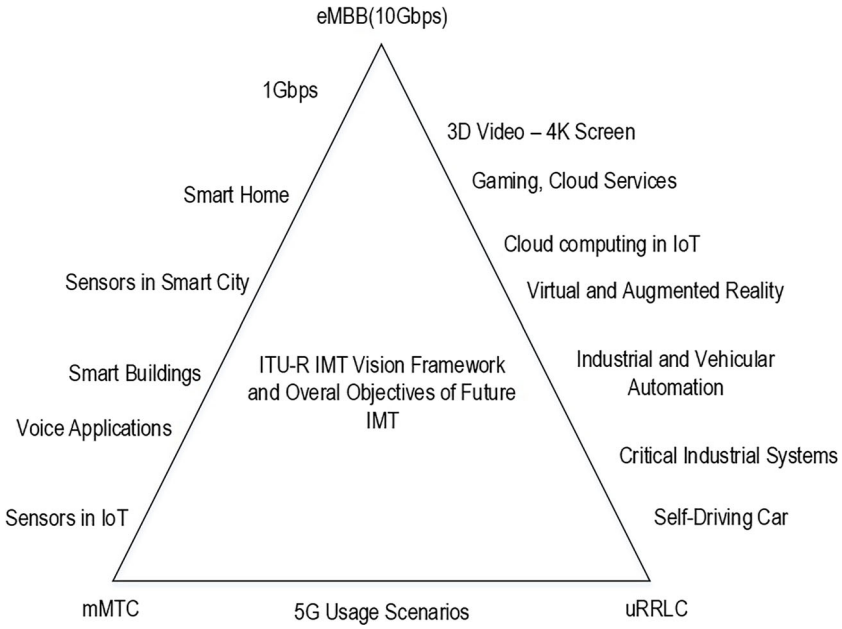

Fig. 2 Key technologies in the future IMT

– *Mobility*, the FIoT supports many mobile services over mobile phone, tablet, and other mobile devices, so it is key for 5G-IoT to provide entities with high mobility.

Most current IoT solutions assume applications upload and store all the IoT generated raw data to the back cloud servers, which are able to process and analyse these data using many techniques, such as machine learning, big data, *etc.*

3 Zero-trust Security Model in 5G-IoT

It is clear that the current security solutions are unable to secure and manage the increasing IoT applications. The zero-trust security model shows great potential in securing IoT in terms of identity to authenticate devices, least privileged access, device health, continual updates, security monitoring and incidents response.

3.1 Zero-trust Security Model in 5G-IoT

Zero-trust security has been widely adopted in private networks (Li, 2020; Bhattacharjya, 2020; Dhar & Bose, 2020), which is identified as one of the options that will address most of the security concerns in the 5G-IoT. Since a 5G-enable IoT system involves a huge number of IoT devices, zero-trust security model will help the system to authenticate and identify all IoT device and keep track of all the activities of IoT devices for any malfunctions within the system.

For industrial systems, including ICS and SCADA system, it is very difficult to use segmentation techniques due to the unprecedented agility. Zero-trust will enable ICS and SCADA systems easily segment a process control network without having to re-IP the devices. The zIoT provides the assurance to protect and prevent security breaches for IoT devices, data, and applications. The zero-trust security model can well monitor and identify malicious activities by either a user or a device inside or outside the IoT system.

The zero-trust model is also facing challenges: (1) Specifically, zero-trust model runs successfully in large scale works, e.g. Google infrastructure. However, for an IoT system connects of millions of device, it will be very complex to put down security policies that will be followed on the 5G network. Furthermore, a 5G-IoT will involve multi-access edge networks and network slice, having a hybrid policy definition will be a challenge for the network service providers; (2) The zero-trust model involves continuous monitoring and analysing of each device and tracking activities, which might hamper latency as it involves an intermediately monitoring application taking a bit of time to fetch and send details to the central cloud. Figure 3 shows a zero-trust security architecture in IoT, in which the entire IoT system is not considered an implicit trust zone. Specifically, the IoT devices, users, or applications may not be owned by the IoT system and devices/applications will not be inherently trusted. In 5G-enabled IoT, the evolving zero-trust approach will be able to handle identity and authentication mechanisms which can allow 5G-IoT to secure the network.

3.2 Blockchain-enabled IoT device authentication

In this work, we propose a blockchain-enabled security solution for authentication of IoT devices, critical infrastructure, and IoT systems in IoT environments (BasIoT), which provides a promising high-level security system to protect IoT systems against cyber-threats.

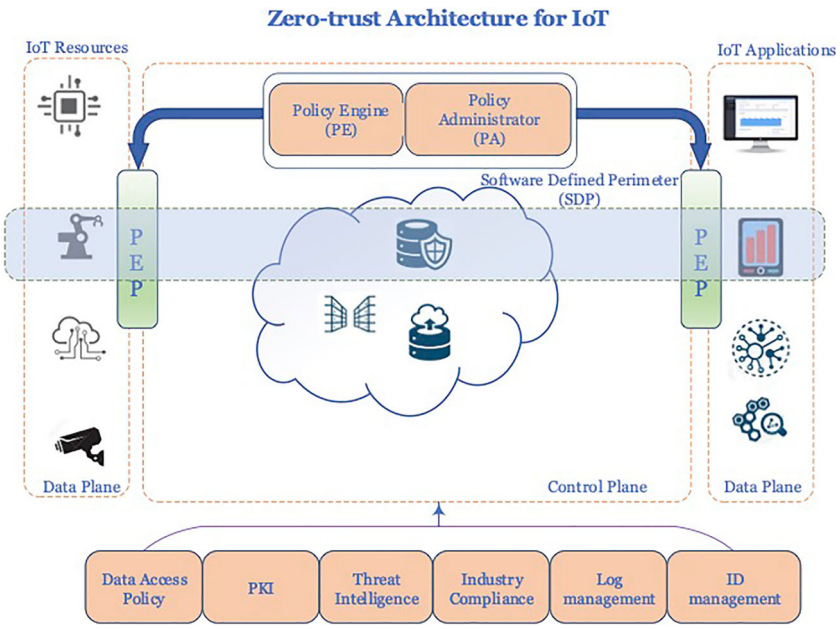

Fig. 3 Zero-trust security architecture IoT

The proposed Bloackchain-enabled authentication for IoT (BasIoT) leverages digital signature-based identity and authentication for users, devices, and applications, there by securing the IoT systems. BasIoT delivers a zero-trust software-define security perimeter by providing strong secure authentication using private permission blockchain. The RSA signature allows IoT devices/users to authenticate and authorise resource access within an dynamic security perimeter in IoT. The BasIoT offers zero-trust security for users, devices, and critical infrastructure in IoT systems.

In the initialisation state, a user/device can be registered as an IoT devices u_i, which includes {"$device\_identifier$: $identifier$", "$device\_descriptor$: $device/user/apps$"}, in which the 'identifier' could be *name, ID, serial number, etc.* and the 'device descriptor' is some detailed description for the device, could be "*usage, service type, etc.*". As

```
{
  "device_identifier":"deviceID",
  "device_descriptor":"IoT devices"
}
```

The generated keys as:

```
{
  "d_addr":"P5JqhB6dr...J4FFNor",
  "sk":"b3BlbnNzaC1rZ...8+/jDF+/Lr",
  "RSA_pk":"AAAAB3NzaC...cGN6b0qp+FtLfcE=",
  "RSA_sk":"b3BlbnNzaC1r...U1nsuBEaWAgShN",
}
```

Each device d_i needs to be registered on the private permission blockchain of IoT system, and the blockchain will create: device blockchain address addr_{d_i}, device private key sk_{d_i}. The BasIoT includes following five main steps:

1. If a user/device d_i wants to access a specific resource s_j in IoT, it needs to retrieve the public key cpk of s_j from the blockchain, and then encrypt its blockchain address addr_{d_i} using the pk_{s_j};
2. The device d_i encrypts the blockchain address and transmits to the resource holder s_j in IoT; On receiving the encrypted blockchain address, the resource holder s_j can decrypt using its private key sk_{s_j};
3. The s_j retrieves the public key of d_i from blockchain and creates an nonce for this session;
4. The s_j generates a hash of timestampled nounce using $sha256(nonce, t)$ and transmits the encrypted the hash to d_i;
5. The d_j decrypts the hash and Sign the hash using its private key sk_{d_i}, then encrypts the signature and then transmits to s_j;
6. The s_j check if the received signature authentic and makes decision to *accept* or *refuse*.

Figure 4 shows the detailed procedures of the BasIoT, which includes three key roles: devices, blockchain, and resource holder in IoT.

To further evaluate the effectiveness BasIot, we implemented the solution in a neo-local blockchain environment with 10 nodes. The devices (as resource requester) and a resource holder (s_j) in IoT verify the access request, if s_j authenticates d_j, then it will grant the access the the requested resource. Each node is running in a Docker container running on the same machine (3.2GHz Core i7, 16GB Ram; docker 19.03.5, Golang 1.13.4, ubuntu 18.04). In this work, we use TPS, cpu, and memory usage to evaluate the performance for IoT nodes.

To validate the proposed authentication scheme, we follow the process proposed above. A request for access to a specific resource (data, computation service, etc.) needs

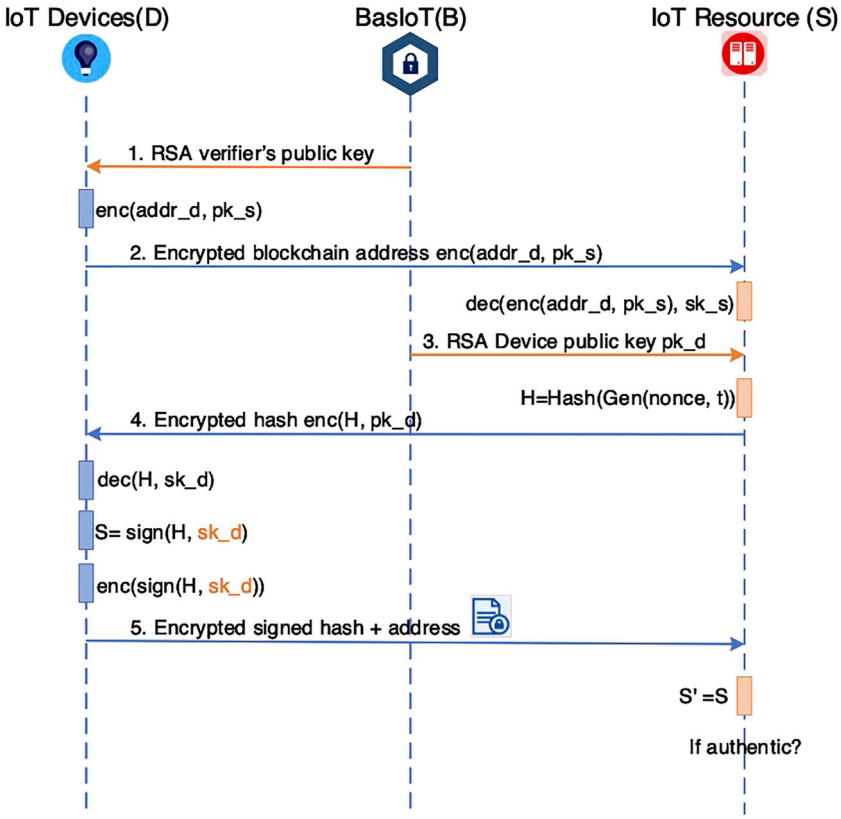

Fig. 4 Blockchain-enabled device authentication solution in zero-trust IoT environment

to be verified by the source holder (data owner, etc.). We presume that the blockchain addresses of requester d_i and resource holder r_i are $\{P5Jqh \ldots FFNor\}$, $\{P5JCm \ldots owfio\}$, respectively.

The requester retrieves the RSA rsa_pk of s_i from the blockchain, which will be encrypted using

$$c = \mathsf{enc}(s_i\_rsa\_\mathsf{pk}, add_{d_i}) \tag{1}$$

and then send to s_i;

On receiving c, the s_i decrypts the blockchain address of d_i using $\mathsf{dec}(s_i\_rsa\_\mathsf{sk}, c)$ as $\{P5Jqh \ldots FFNor\}$;

The s_i then retrieves the RSA public key $d_i\_rsa\_\mathsf{pk}$ from the blockchain and generate a nonce $nonce$, then encrypts timestamped $nonce$ as

$$c' = enc(d_i\_rsa\_\mathsf{pk}, sha512(nonce, t)) \tag{2}$$

and then sends c' to d_i, in which t is the timestamp.

On receiving c', d_i performs $\mathsf{dec}(d_i\_rsa\_\mathsf{sk}, c')$ to extract the hash value of timestamped $nounce$. Then d_i signs the hash using $\mathsf{Sign}(hash)$ and encrypts

$$c^* = \mathsf{enc}(\mathsf{pk}\_s_i, hash, \mathsf{addr}\_d_i, \mathsf{Sign}) \tag{3}$$

that needs to be sent to s_i.

On receiving c^*, the s_i can perform decryption and extract the data using its private key; s_i can verify the sig, $addr_{d_i}$, and $hash$, if the signature is valid then s_i will return $accept$ and grant d_i the access.

The zero-trust security model provide trust and security in the expanding boundaries of IoT systems, which includes a numbr of key enabling technologies as addressed in next Section.

4 Key Enabling Technologies in 5G-IoT

As discussed above, the 5G-IoT is facing many challenges and needs to be clearly addressed. It is essential to solve these challenges and help to develop and deploy innovate solutions in many areas, including mobile networks, IoT devices, network, security, and applications. Figure 2 shows the key enabling technologies associated with 5G-IoT (Blyler, 2017), which can be further grouped into following five major categories: (1) wireless communication technologies for massive connectivity; (2) scalable and secure 5G-IoT architecture; (3) communication protocols between IoT devices; (4) innovations in services and applications; and (5) data analytics and new business models that can boost the competitiveness of 5G-IoT and support growth.

4.1 Architecture of 5G-IoT

From the view point of applications, 5G-IoT architecture generally includes *data plane* and *control plane* (Akyildiz et al., 2015):

- **Data plane**, can create new data sensing network, data analyse technologies, such as SDN based architecture (Qin et al., 2014), QoS-based architecture (Matias et al., 2015), *etc*.;
- **Control plane**, scalable and reliable network management tools and re-configurable services (applications), such as SoA-based architecture (Da Xu et al., 2014), IoT-A architecture (Da Xu et al., 2014), and S-IoT architecture (Huang et al., 2017), *etc*.

New research and innovation on 5G-IoT architecture will cover following requirements:

- NFV is very helpful to develop and deploy scalable IoT solutions in 5G networks.
- Cloudification, to bridge the 5G networks with the cloud networks in IoT.
- Network virtualization capability is key function for the scalable network management, includes mobility control, access control, and security.
- Services deployment over smart devices can introduce new functionalities and improved properties over resource constrained IoT devices.

4.2 Wireless Network Function Virtualisation (WNFV)

The WNFV refers to virtualised network services and functions, which is a complementary to the 5G networks. In the large scale 5G-IoT, the WNFV can implement the virtualization of the entire network functions and services that can significantly simplify the management and deployment of 5G-IoT. In 5G-IoT scenarios, the WNFV can decouple flexible an scalable physical infrastructures and underlying network functions and services on cloud servers (Akyildiz et al., 2014). The NFV serves to provide scalable and flexible network services in 5G-IoT, including network slicing, customization, and management of programmable networks for 5G-IoT applications (Central, 2018). Figure 5 shows an example of network management in a NFV-enabled 5G-IoT, where devices are re-configurable and can be sliced into multiple sub-virtual networks. The NFV technology can enable IoT applications to work in a real-time way in logically sliced high speed and reliable sub-networks, as shown in Fig. 6.

In summary, the NVM technology is able to increase the scalability of 5G-IoT and provide low cost and flexible broadband connectivity. Particularly, in conjunction with the existing radio access networks, small cell, SDN, etc., 5G-IoT can provide users with dynamic and programmable 5G networks (Akyildiz et al., 2015).

4.3 Heterogeneous Networks (HetNet)

In the complicated 5G-IoT, a number of heterogeneous network (HetNet) with different operating systems and protocols will be involved to connect IoT devices. The HetNet is a new network connecting paradigm aims at linking different networks and/or networks using different access technologies. The HetNet can enhance the scalability of 5G-IoT by providing on-demand data transmisison rates and deployment model for different IoT devices. In wireless networks, HetNet will be helpful to deploy large-scale multiple-input and multiple-output (MIMO) networks (Hasan et al., 2013; Ge et al., 2014).

The machine-to-machine (M2M) communication refers to the direct communication technologies between two IoT devices, and in Pereira & Aguiar, (2014), Dawy et al., (2017), Biral & Centenaro, (2015a, b) comprehensive reviews have been made on this technologies. In many M2M solutions, mobile devices are used as gateway for resources constrained IoT devices as discussed in Pereira and Aguiar (2014) and Biral and Centenaro (2015a), and the solutions proposed in Biral & Centenaro, (2015a, b) highlighted on the deployment of M2M applications using 3GPP/LTE-A networks.

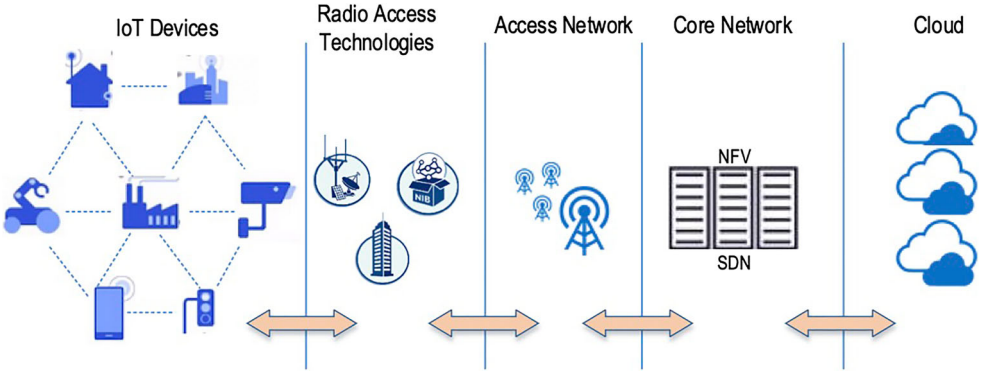

Fig. 5 5G NFV technology

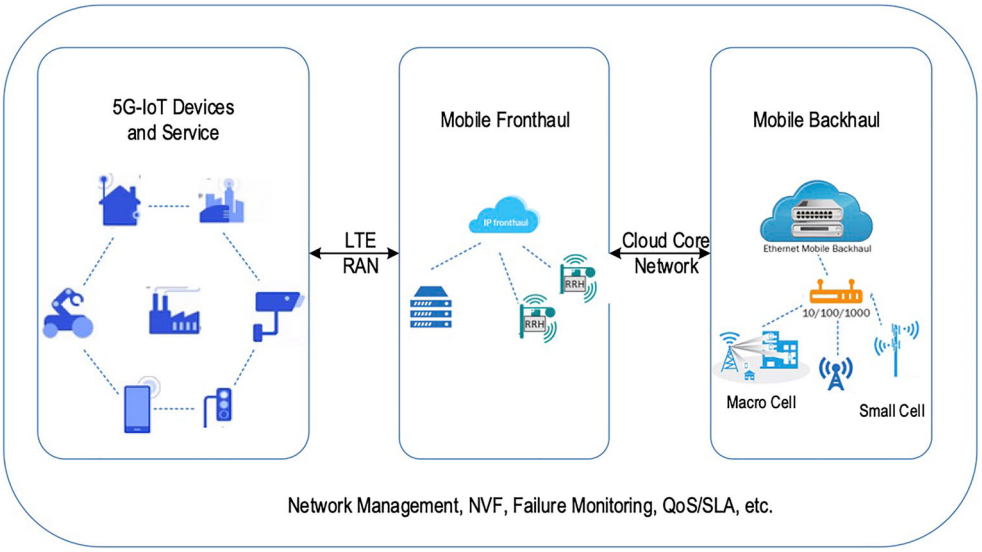

Fig. 6 Network management in 5G-IoT

In 3GPP, the M2M is also called as machine-type communication (MTC) which aims at providing massive connections for applications and MTC based IoT applications, such as healthcare, smart homes, *etc*. are increasingly becoming an important part of our daily lives. It can be exptected that it is a robust communication solution in HetNet (Ali et al., 2017; Hasan et al., 2013).

4.4 Direct Device-to-Device (D2D)

In mobile networks, the D2D denotes the communications directly between two mobile users without routing base station (BS) or other network infrastructure. Since D2D can provide communication between two devices on the cellular frequencies or unlicensed spectrum, the D2D is regarded a new way for short-range communications in 5G-IoT that can offer high speed data and power, spectrum efficient transmission. It is a potential communication technology for applications that require efficient short-range communications (Da Xu et al., 2014).

In many existing applications, short-range communication technologies, such as BLE, Zigbee, WiFi, and cellular networks are widely used. In recent, a number of new technologies, such as low-power wide-area network (LPWAN), SigFox, NB-IoT, LTE category M1 (LTE-M), *etc.*, are believed a promise technology that can fully integrate D2D to more wide IoT applications, such as smart cities, industrial IoT, smart agriculture, *etc*.

The D2D communication also features with reduced energy consumption and spectrum efficiency, which make it to be one of the leading technologies in 5G-IoT. In recent, new research efforts on D2D show that the spectrum reuse solution can improve the efficiency of up-link spectrum (Liu et al., 2015; Mach et al., 2015). Just like the D2D can offer IoT applications new unprecedented opportunities, it is also facing new challenges that must be addressed, such as architectures, *etc*. Pyattaev et al. (2015).

4.5 Advanced Spectrum Sharing and Interference Management

As discussed above, a huge number of IoT devices might be densely deployed in 5G-IoT for applications, such as wireless sensor networks (WSN), smart cities, intelligent transportation, *etc.* However, the spectrum is a scarce asset and demand is growing very fast, which makes spectrum sharing solution to be an urgent need. Meanwhile, to well manage the interference between IoT devices, the interference management in HetNet is becoming one of the key enabling technologies. The massive MIMO technology is promise for improving higher spectrum efficiency. The variants of massive MIMO, including multiuser MIMO (MU-MIMO), very large multiuser MIMO, *etc.*, have been proposed to further improve the spectrum efficiency (Talwar et al., 2014).

Actually, there are many key enabling techniques are in development for 5G-IoT, from communication technologies to business models, all these will be important enablers for boosting the success of 5G-IoT.

5 Research Challenges and Future Trends

The 5G is expected to provide IoT with high communication capacity that can satisfy the requirements of new applications. However, there still are many research challenges in communication technologies, 5G-IoT architectures, trusted D2D communication, security issues, *etc.* As a huge system, 5G-IoT integrates many key enabling technologies and is creating significant impact on the growth of technologies.

This section will present the potential research challenges facing by IoT 5G and address future trends.

5.1 Technical Challenges in 5G-IoT

Although many research efforts have been made on 5G-IoT, there are still many technical challenges to be addressed.

1. The architecture of 5G-IoT is one of the most significant challenges, as mentioned above, lots of architectures for 5G-IoT have been proposed but many of them are still not ideal for massive IoT networks due to following shortcomings:
   - **Scalability and network management**, in large scale 5G-IoT, the scalability is a key challenge due to the diversity of devices and their states management (Ndiaye et al., 2017; Modieginyane et al., 2018).
   - **Interoperability and Heterogeneity**, seamlessly interconnection between a large number of devices and heterogeneous networks will increase productivity, however the lack of interoperability between these devices and networks is a major challenge in 5G-IoT. Many key IoT platforms developers are working on providing open source frameworks, such as Microsoft azure IoT hub, *etc.*, the universal framework will enable interoperability across IoT devices, sub-IoT systems, networks (Elkhodr et al., 2016; Ishaq et al., 2013).
   - **Security and Privacy-preserving**, security and cyber-attacks, increased privacy concerns in 5G-IoT, build-in security framework in 5G-IoT architecture become key challenges.
2. **Wireless software defined network** is emerging recently which aims to provide vendor independence and operator sovereignty for networks. To integrate the 5G with SDN will significantly benefit the IoT with scalability and high level of performance.
3. **Network Function Virtualization**, as discussed above the **NFV** is highly complementary to the SDN and software-define infrastructure (SDI). Many existing NFV technologies, such as SoftAir (Akyildiz et al., 2014), OpenRoads (Akyildiz et al., 2015), CloudMAC (Commission, 2018), SoftRAN (Akyildiz et al., 2015) et al., have been developed for 5G-IoT, in which the agility is still a major challenge. The NFV architecture should be able to fulfil the requirements of agility, acceleration, and automation in integrating NFV into 5G-IoT. Specifically, following issues should be considered: (1) Network cloudification, closely bridges the IoT with cloud environment; (2) Security and privacy-preserving, NFV runs over untrusted public third-party cloud environment, in which security and privacy-preserving are two concerns must be considered; (3) NFV can make 5G-IoT easier to manage, but it will cause extra management challenges, such as NFV switching, NFV interfaces, etc.
4. **D2D communication** is expected to be an essential component of 5G-IoT, which is able to facilitates decentralised devices to communicate with lower energy consumption and spectrum efficient. The D2D relies on resource utilization, routing techniques, and interference management, and can provide efficient throughput and reliable communications between IoT devices.
5. **Deployment of massive applications** is very challenging in large scale 5G-IoT, in which the resource constrained IoT devices and complicated network environment cannot handle latency-sensitive applications. In 5G-IoT, the massive heterogenous devices make it very challenging to management and integrate IoT applications due to the differences of capabilities and efficiency. In recent, multi-level and multi-dimensional service provision platform is proposed for large scale IoT applications deployment that addresses both above challenges in Zhao et al. (2016).
6. Many other challenges, such as dense heterogeneous deployment of networks, multiple radio access, and full-duplex transmission at the same time over 5G, etc., are still to be addressed.

5.2 Standardization Issues

The standardisation of 5G is a complex and innovative process. In the past few years, a number of M2M and IoT standards have been defined, such as the enhanced coverage GSM-IoT for the use of licensed spectrum, power saving model (PSM) for reduction of power consumption, and 3GPP solutions for MTC and NB-IoT. The diverse nature of IoT systems make it very difficult to standardize both the networks and applications in 5G-IoT. The standardization presented very severe challenges to 5G-IoT, which can be classified into following four categories (Banafa, 2016):

- IoT platforms, include IoT devices, operating systems, features of IoT products, and analytic tools and methods used in IoT data analytics.
- Connectivity, such as the message protocols, communication technologies, and protocols in different level of IoT systems.
- Business model innovations, include 5G and IoT industry digitalization business models to meet the demands of new applications and services.
- Killer applications, such as control function, data collection and analysis functions.

Both the standardization process of 5G and IoT are complex and highly innovative, which needs the collaborations of academia and industries. Basically, it involves following standards: (1) technical standards, such as 5G radio access, security, sustainability, *etc.*; (2) regulatory standards, including information regulations, services standards, security and privacy-preserving. Typical regulatory standards like general data protection regulation (GDPR), cryptographic primitives, *etc.*; and (3) standards of adoption of 5G-IoT applications and application level protocols (Banafa, 2016).

The 3GPP R16 brings to broaden the use cases that NR can be applied, key features include (1) highly demanding critical industrial use cases by spporting time-sensitive communications (TSC), which are key for IIoT; (2) larger bandwidths at band 5 and 6GHz; (3) NR V2X solutions for enhancing LTE V2x for advanced automative industry service (Nasraoui & Ikki, 2020); and (4) integrated access and backhaul (IAB), referring to the solution that the backhaul link of a node uses NR link (Yilmaz & Susitaival, 2020).

According to the Bertenyi (2020), more 5G system enhancements are set to following the upcoming 3GPP R17, which is scheduled for delivery in 2021. The 5G systems will provide better standardisation of cellular communications, it will bring more use cases that can cover all devices, anywhere, and anytime with non-limiting access. In R17, 5G LPWA IoT communication is based on mMTC, including LTE-M and NB-IoT, both cover wide range of use cases and requirements for high voumes of deivce. The R17 also will focus on critical MTC (cMTC) use cases that are expected to enhance the IIoT. Other features, such as MIMO, IAB enhancements, sidelink, NR on high frequencies ($\geq$ 52.6 GHz), will be introduced.

5.3 Research Trends

The evolving 5G is still in its infancy and there are many unresolved research challenges as mentioned above and the main research trends include

1. The zero-trust security model will address most of the security concerns in 5G networks, that can dynamically detect/identify malicious activities of users/devices/apps. The zero-trust security solution will restrict both internal and external access to resources in the 5G IoT.
2. The 5G-IoT is experiencing a major wave of revolution, in which applications are more demanding in terms of ultra-low latency, ultrahigh reliability, and flexible network architecture compared with conventional applications. The new named data network (NDN) has been proposed to support the high density applications in 5G-IoT environment (Lei et al., 2018), in which network virtualisation technologies, *e.g.*, NFV will be utilized to manage the increasingly fragmented networks (Aijaz & Sooriyabandara, 2018; Li et al., 2018).
3. The edge computing is another key use case in 5G-IoT, including edge devices, edge cloud, edge intelligence, and the processing of data where move to the edge of the network, instead of in a centralised data-processing warehouse. The edge computing in 5G-IoT environment will focus on two categories: (i) 5G-IoT drived edge intelligence, which is the union of edge-computing and AI aimed at providing capabilities of analytic; (ii) it will boost the proximity of sources of data at the edge network of the 5G-IoT. The edge computing in 5G-IoT can offer industrial IoT with time-critical applications, including micro data centres, VR/AR, smart cities, *etc.*
4. The convergence of 5G, artificial intelligence, blockchain and IoT (Morgado et al., 2018). The 5G-IoT will bring new technologies together to offer powerful and intelligent capabilities required by new business models in IoT, which will enable completely new applications while also benefitting many IoT applications in 5G-IoT, such as connected automotive, consumable IoT, entertainments, agriculture, manufacturing, and variable-reality.
5. Spectrum sharing cellular 5G networks will be one of key research trends in 5G-IoT (Ejaz & Ibnkahla, 2018; Tang et al., 2018). 5G has been designed to support a wide range of spectrum bands from sub-1 GHz to mmWave bands. The spectrum sharing in shared/unlicensed spectrum will continue to be one of the main research trends aimed at delivering multi-gigabit, ultra-reliable, and ultr-low latency connectivity.
6. The 5G-IoT involves many different sections and to understand the security challenges, threats, and the security requirements that 5G-IoT scenarios will become a main concern. Lots of research efforts are on-going on 5G security and a number of security standards are in development.
7. Context-aware IoT middle-ware solutions, which aim at hiding the details of different technologies between technological and application layers. The context-aware middle-ware solutions can increase the scale, mobility, and heterogeneity of entities to dynamic changes in context in 5G-IoT.
8. The new blockchain technology (or called ”distributed ledger”) attracts many research attentions, which aims at solving manipulation problems and offering transparency, authenticity, durability and attack resistances

for applications. However, there are still some challenges to be solved, include, security issues, operational challenges, legal and compliance issues, *etc.*

5.4 Security and Privacy

A number of new features in 5G-IoT need new security capabilities and many new security concerns need to be addressed, including new trust model, new service delivery model, increased privacy concerns, evolved threat landscape, *etc.* Due to the high level of performance in IoT, the real-time visibility of cyber attacks or threats from both outside and inside increase significantly (Girson, 2017). Meanwhile, the security assurance must consider avoiding weak security links. Typical security concerns include:

- Authorized and authenticated IoT devices
- Data encryption and assurances
- IoT devices updates
- Vulnerabilities and incidents detection
- Misuse of cryptography algorithms
- Predict and preempt security issues
- Secure mobility, backward compatibility and availability

The existing IoT suffers from large number of cyber attacks, such as data leakage, distributed denial of service (DDoS), *etc.* The 5G enabled IoT will be the target of new cyberthreats. Given massive devices and applications in 5G-IoT, the security and privacy issue becomes more challenging.

- Trusted massive connectivity between devices, middlewares, and applications in 5G-IoT is a key research trend. The 5G will have security integrated as part of the framework, which will significantly change the ways of information exchanging by satisfying new requirements in faster speed, low latency and higher reliability. It means the existing communication security protocols will be changed in 5G-IoT.
- Privacy and data protection. The privacy of massive number of entities in 5G-IoT, such as users, devices, services, etc., will be an important issue. The privacy in data collection, sharing, and management, as well as data security remain open research topics to be solved. To develop privacy and data protection solutions, advances in following areas are required: sophisticated cryptograpic techniques, fine-grain and configurable access control, location privacy of entites, *etc.*
- Lightweight security solutions in 5G-IoT will be a new trend. Given the massive connectivity of resource constrained devices in 5G-IoT, the current security suites can not be employed due to the expensive computational costs, as a result, the lightweight solutions will be a promising research trend.
- Devices and applications protection. 5G-IoT will cover a huge number of devices and applications, which will increase the vulnerability to cyber threats and attacks, such as DDoS, *etc.* Therefore, to develop more strong authentication and protection solution using strong cryptographic modules will be another main trend.

The 5G-IoT will bring new security and privacy requirements, in which a systematic security and privacy protection strategy is necessary. And while the cyber threats are increasing in IoT, new security solutions, including valid security architecture, lightweight cryptographic, privacy and data protection solutions are still to be revisited.

6 Conclusion

The 5G-IoT aims at integrating emerging 5G communications and networks into the future IoT, which is promising to accelerate future revenue through innovative services. The 5G-IoT continues to evolve and expand not only in terms of the number of user, service, devices, and applications, but can also create fundamental new types of product, services, analytic insights, business model and drive future innovations of IoT. In this paper, we have introduced the background and current researches for 5G-IoT and it's key enabling techniques. We also addresses the main challenges and potential research trends. Zero trust and security solutions are introduced by design for IoT. Specifically, in this work we proposed a zero-trust security solution by design for IoT and a blockchain-based IoT device authentication (BasIoT) is developed. The BasIoT is able to provide secure and zero-trust authentication for massive device authentication.

References

Akpakwu, G. A., Silva, B. J., Hancke, G. P., & Abu-Mahfouz, A.M. (2018). *IEEE Access*, *6*, 3619.

Al-Turjman, F., Ever, E., & Zahmatkesh, H. (2019). *IEEE Communications Surveys Tutorials*, *21*(1), 28. https://doi.org/10.1109/COMST.2018.2864779.

Akyildiz, I. F., Lee, A., Wang, P., Luo, M., & Chou, W. (2014). *Computer Networks*, *71*, 1.

Akyildiz, I. F., Lin, S. C., & Wang, P. (2015). *Computer Networks*, *93*, 66.

Alliance, Z. (2011). Interconnecting zigbee & m2m networks.

Akpakwu, G. A., Silva, B. J., Hancke, G. P., & Abu-Mahfouz, A. M. (2018). *IEEE Access*, *6*, 3619. https://doi.org/10.1109/ACCESS.2017.2779844.

Akyildiz, I. F., Wang, P., & Lin, S. C. (2015). *Computer Networks*, *85*, 1.

Asia, T. W. (2017). The next generation of iot. https://techwireasia.com/2017/08/next-generation-iot/.

Abu-Mahfouz, A. M., Hamam, Y., Page, P. R., Djouani, K., & Kurien, A. (2016). *Procedia Engineering*, *154*, 99.

Astely, D., Dahlman, E., Fodor, G., Parkvall, S., & Sachs, J. (2013). *IEEE Communications Magazine*, *51*(7), 154.

Akyildiz, I. F., & Nie, S. (2016). *Computer Networks*, *106*, 17.

Ali, K. T., Rejeb, S. B., & Choukair, Z. (2017). In *2017 13th International Wireless Communications and Mobile Computing Conference (IWCMC)* (pp. 1126–1131). IEEE.

Aijaz, A., & Sooriyabandara, M. (2018). *Proceedings of the IEEE*, 1–22. https://doi.org/10.1109/JPROC.2018.2878265.

Bhattacharjya, S. (2020). *A novel zerotrust framework to secure iot communications*. Ph.D. thesis, University of Kansas.

Blyler, J. (2017). Top 5 rf technologies for 5g in the iot. http://www.mwrf.com/systems/top-5-rf-technologies-5g-iot.

Biral, A., & Centenaro, M. (2015a). *Digital Communications and Networks*, *1*(1), 1.

Biral, A., Centenaro, M., Zanella, A., Vangelista, L., & Zorzi, M. (2015b). *Digital Communications and Networks*, *1*(1), 1.

Banafa, A. (2016). Iot standardization and implementation challenges. https://iot.ieee.org/newsletter/july-2016/iot-standardization-and-implementation-challenges.html.

Bertenyi, B. (2020). 5G in Release 17 – strong radio evolution. https://www.3gpp.org/news-events/2098-5g-in-release-17.

CISCO (2016). Cisco: Internet of things. https://www.cisco.com/c/dam/en/us/products/collateral/se/internet-of-things/at-a-glance-c45-731471.pdf.

Commission, E. (2018). Project content fp, 2012–2015. https://cordis.europa.eu/guidance/archive_en.html.

Chen, X., Liu, S., Lu, J., Fan, P., & Letaief, K. B. (2016). *IEEE Access*, *4*, 8888.

Central, S. (2018). How 5g nfv will enable the 5g future. https://www.sdxcentral.com/5g/definitions/5g-nfv/.

Da Xu, L., He, W., & Li, S. (2014). *IEEE Transactions on industrial informatics*, *10*(4), 2233.

Dhar, S., & Bose, I. (2020). *Journal of Organizational Computing and Electronic Commerce*, 1–17.

Duan, P., Jia, Y., Liang, L., Rodriguez, J., Huq, K. M. S., & Li, G. (2018). *IEEE Transactions on Industrial Informatics*, *14*(6), 2715. https://doi.org/10.1109/TII.2018.2794615.

Dongbaare, P., Chowdhury, S. D., Olwal, T., & Abu-Mahfouz, A. (2016). In *Proceedings of the 51st International Universities' Power Engineering Conference* (pp. 06–09).

Dawy, Z., Saad, W., Ghosh, A., Andrews, J. G., & Yaacoub, E. (2017). *IEEE Wireless Communications*, *24*(1), 120.

El-Tanab, M., & Hamouda, W. (2020). *IEEE Network*, 1–6. https://doi.org/10.1109/MNET.011.2000513.

Egham (2017). Gartner says 8.4 billion connected "things" will be in use in 2017. https://www.gartner.com/newsroom/id/3598917.

Elkhodr, M., Shahrestani, S., & Cheung, H. (2016). arXiv:1604.04824.

Ejaz, W., & Ibnkahla, M. (2018). *IEEE Internet of Things Journal*, *5*(1), 150.

Girson, A. (2017). Iot has a security problem – will 5g solve it?. https://www.wirelessweek.com/article/2017/03/iot-has-security-problem-will-5g-solve-it.

Ge, X., Cheng, H., Guizani, M., & Han, T. (2014). *IEEE Network*, *28*(6), 6.

Hasan, M., Hossain, E., & Niyato, D. (2013). *IEEE Communications Magazine*, *51*(6), 86.

Huang, C., Shao, C., Xu, S., & Zhou, H. (2017). *IEEE Transactions on Emerging Topics in Computing*, *5*(3), 425.

Hošek, J. (2016). Enabling Technologies and User Perception Within Integrated 5G-IoT Ecosystem (vysoké učení technické v brně nakladatelství VUTIUM.

Ishaq, I., Carels, D., Teklemariam, G. K., Hoebeke, J., Abeele, F. v. d., Poorter, E.D.., Moerman, I.., & Demeester, P. (2013). *Journal of Sensor and Actuator Networks*, *2*(2), 235.

Jackson, M. (2017). Ee start roll-out of 400mbps 4g+ mobile broadband to big uk cities. https://www.ispreview.co.uk/index.php/2017/06/ee-start-roll-400mbps-4g-mobile-broadband-big-uk-cities.html.

Jaiswal, A., Kumar, S., Kaiwartya, O., Kumar, N., Song, H., & Lloret, J. (2020). *IEEE Systems Journal*, 1–12. https://doi.org/10.1109/JSYST.2020.3036417.

Juliane Stephan, K. K. (2016). Understanding the industrial internet of things. http://usblogs.pwc.com/emerging-technology/understanding-the-industrial-internet-of-things/.

Jin, J., Gubbi, J., Marusic, S., & Palaniswami, M. (2014). *IEEE Internet of Things Journal*, *1*(2), 112. https://doi.org/10.1109/JIOT.2013.2296516.

Kaplan, K. (2014). Will 5g wireless networks make every internet thing faster and smarter?. https://qz.com/179794/will-5g-wireless-networks-make-every-internet-thing-faster-and-smarter/.

Kiran, M. P. R. S., & Rajalakshmi, P. (2019). *IEEE Transactions on Vehicular Technology*, *68*(5), 4774. https://doi.org/10.1109/TVT.2019.2903890.

Khalfi, B., Hamdaoui, B., & Guizani, M. (2017). arXiv:1707.06983.

Li, S., Xu, L. D., & Zhao, S. (2018). *Journal of Industrial Information Integration*, *10*, 1.

Li, S., Ni, Q., Sun, Y., Min, G., & Al-Rubaye, S. (2018). *IEEE Transactions on Industrial Informatics*, *14*(6), 2618. https://doi.org/10.1109/TII.2018.2799177.

Lyu, L., Chen, C., Zhu, S., & Guan, X. (2018). *IEEE Transactions on Industrial Informatics*, *14*(6), 2690. https://doi.org/10.1109/TII.2018.2799685.

Lin, H., Hu, J., Xiaoding, W., Alhamid, M. F., & Jalil Piran, M. (2020). IEEE Transactions on Industrial Informatics, 1–1. https://doi.org/10.1109/TII.2020.3038780.

Li, S. (2020). *EAI Endorsed Transactions on Internet of Things, 5*(20).

Li, C., Hosseini, K., Lee, S. B., Jiang, J., Chen, W., Horn, G., Ji, T., Smee, J. E., & Li, J. (2018). *Proceedings of the IEEE* (pp. 1–18). https://doi.org/10.1109/JPROC.2018.2864984.

Liu, J., Kato, N., Ma, J., & Kadowaki, N. (2015). *IEEE Communications Surveys & Tutorials*, *17*(4), 1923.

Lei, K., Zhong, S., Zhu, F., Xu, K., & Zhang, H. (2018). *IEEE Transactions on Industrial Informatics*, *14*(6), 2725.

Matias, J., Garay, J., Toledo, N., Unzilla, J., & Jacob, E. (2015). *IEEE Communications Magazine*, *53*(4), 187.

Mach, P., Becvar, Z., & Vanek, T. (2015). *IEEE Communications Surveys & Tutorials*, *17*(4), 1885.

Mills, C. (2018). 5g isn't going to be much faster than lte when it launches next year. https://bgr.com/2018/04/26/5g-speeds-vs-lte-verizon-t-mobile/.

McClelland, C. (2017). Rpma - overview of ingenu's lpwan technology. https://medium.com/iotforall/rpma-overview-of-ingenus-lpwan-technology-3d72c47f0461.

Modieginyane, K. M., Letswamotse, B. B., Malekian, R., & Abu-Mahfouz, A. M. (2018). *Computers & Electrical Engineering*, *66*, 274.

Morgado, A., Huq, K. M. S., Mumtaz, S., & Rodriguez, J. (2018). *Digital Communications and Networks*, *4*(2), 87.
Nipun Jaiswal, A. M. (2014). 5g: continuous evolution leads to quantum shift. https://www.telecomasia.net/content/5g-continuous-evolution-leads-quantum-shift.
Notes, E. (2018). 5g requirements for the next generation mobile wireless system.
Notwel, L. (2017). 3 things to know about 5g. https://www.ecnmag.com/article/2017/11/3-things-know-about-5g.
Ndiaye, M., Hancke, G. P., & Abu-Mahfouz, A. M. (2017). *Sensors*, *17*(5), 1031.
Nasraoui, L., & Ikki, S. (2020). *IEEE Internet of Things Journal*, 1–1. https://doi.org/10.1109/JIOT.2020.3039458.
of All Thing, T. I. (2015). Nokia networks to power internet of things with 5g connectivity. https://theinternetofallthings.com/nokia-networks-to-power-internet-of-things-with-5g-connectivity/.
Pyattaev, A., Hosek, J., Johnsson, K., Krkos, R., Gerasimenko, M., Masek, P., Ometov, A., Andreev, S., Sedy, J., Novotny, V., & et al. (2015). *Etri Journal*, *37*(5), 877.
Palattella, M. R., Dohler, M., Grieco, A., Rizzo, G., Torsner, J., Engel, T., & Ladid, L. (2016). *IEEE Journal on Selected Areas in Communications*, *34*(3), 510.
Pereira, C., & Aguiar, A. (2014). *Sensors*, *14*(10), 19582.
Qin, Z., Denker, G., Giannelli, C., Bellavista, P., & Venkatasubramanian. N. (2014). In *2014 IEEE Network Operations and Management Symposium (NOMS)* (pp. 1–9). https://doi.org/10.1109/NOMS.2014.6838365.
Rouse, M. (2014). Bluetooth low energy (bluetooth le). https://internetofthingsagenda.techtarget.com/definition/Bluetooth-Low-Energy-Bluetooth-LE.
Sarrigiannis, I., Ramantas, K., Kartsakli, E., Mekikis, P., Antonopoulos, A., & Verikoukis, C. (2020). *IEEE Internet of Things Journal*, *7*(5), 4183. https://doi.org/10.1109/JIOT.2019.2944695.
Scoop, I. (2018). 5g and iot in 2018 and beyond: the mobile broadband future of iot. https://www.i-scoop.eu/internet-of-things-guide/5g-iot/.
Simsek, M., Aijaz, A., Dohler, M., Sachs, J., & Fettweis, G. (2016). *IEEE Journal on Selected Areas in Communications*, *34*(3), 460.
Sigfox (2018). Sigfox technology overview. https://www.sigfox.com/en/sigfox-iot-technology-overview.
Schinianakis, D. (2017). *IEEE Circuits and Systems Magazine*, *17*(4), 6.
Talwar, S., Choudhury, D., Dimou, K., Aryafar, E., Bangerter, B., & Stewart, K. (2014). In *2014 IEEE MTT-S International Microwave Symposium (IMS)* (pp. 1–4). IEEE.
Tang, J., So, D. K., Zhao, N., Shojaeifard, A., & Wong, K. K. (2018). *IEEE Internet of Things Journal*, *5*(4), 2605.
Vangelista, L., Zanella, A., & Zorzi, M. (2015). In *Future Access Enablers of Ubiquitous and Intelligent Infrastructures* (pp. 51–58). Springer.
Wu, J., Zhang, Z., Hong, Y., & Wen, Y. (2015). *IEEE Network*, *29*(1), 35.
Xu, L., Collier, R., & O'Hare, G. M. (2017). *IEEE Internet of Things Journal*, *4*(5), 1229.
Yongfu, L., Dihua, S., Weining, L., & Xuebo, Z. (2012). *Control Conference (CCC), 2012 31st Chinese* (pp. 7674–7678). IEEE.
Yilmaz, O., & Susitaival, R. (2020). A look at key innovation areas of 3GPP Rel-17, 10. https://www.ericsson.com/en/blog/2019/12/3gpp-rel-17.
Zhang, J., Wang, Y., Li, S., & Shi, S. (2020). IEEE Internet of Things Journal, 1–1. https://doi.org/10.1109/JIOT.2020.3041386.
Zhang, D., Zhou, Z., Mumtaz, S., Rodriguez, J., & Sato, T. (2016). *IEEE Internet of Things Journal*, *3*(6), 1346.
Zhao, S., Yu, L., & Cheng, B. (2016). *IEEE Access*, *4*, 5038. https://doi.org/10.1109/ACCESS.2016.2606407.

Dr Shan Li is currently a researcher in cyber security. Over the last few years, he has been working on a few research projects funded by EU, EPSRC, A4B (Academic expertise for Business), Technology Strategy Board, and industry. He has authored and co-authored several papers based on these research projects. His current research interests include network forensics, device security, wireless sensor networks, Internet of Things, and lightweight cryptography over IoT.

Dr Muddesar Iqbal completed his PhD Funded by EPSRC Doctoral Training Award for 4G-based Reconfigurable Mobile Healthcare System from Kingston University, the UK in 2010. He has worked with several universities in UK, EU and South East Asia and currently working as a Senior Lecturer with London South Bank University. He has been a principal investigator, co-investigator, project manager, coordinator and focal person of more than 15 internationally teamed research and development, capacity building and training projects, resulting in several patented inventions and commercial products. His areas of research are Internet of Sense for Industry 5.0, Intelligent Autonomous Machines/Robotics, Conversational AI and Chabot's, Personalization/Recommendation, 6G Context.

Dr Neetesh Saxena is an academic member of staff with the School of Computer Science and Informatics at Cardiff University, UK. Before joining CU, he was an Assistant Professor with Bournemouth University, UK. Prior to this, he was a Post-Doctoral Reserach Fellow in the School of Electrical and Computer Engineering at the Georgia Institute of Technology, USA. He was also with the Department of Computer Science as a Post-Doctoral Researcher at Stony Brook University, USA and SUNY Korea. He earned his PhD in Computer Science and Engineering from Indian Institute of Technology (IIT), Indore, India. He was a DAAD Scholar at Bonn-Aachen International Center for Information Technology (B-IT), Rheinische-Friedrich-Wilhelms Universität, Bonn, Germany and was also a TCS Research Scholar. His current research interests include cyber security and critical infrastructure security, including cyber-physical system security: smart grid, V2G and cellular communication networks.