Journal of Ambient Intelligence and Humanized Computing
https://doi.org/10.1007/s12652-022-03707-1

ORIGINAL RESEARCH

Security and privacy issues in smart cities/industries: technologies, applications, and challenges

P. Muralidhara Rao[1] · **B. D. Deebak**[1]

Received: 6 November 2020 / Accepted: 10 January 2022

Abstract
The development of the Internet of things (IoT) is rapidly growing everywhere in our daily lives. Advanced information and communication technologies play a vital role in the development of smart cities/industries, including buildings, hospitals, transportation, and other related public and private environments. The emerging technologies are converging as a computing paradigm to optimize resource allocation dynamically to improve the quality of services. The deployment of interconnected devices uses heterogeneous networks and powerful data centers to perform ubiquitous sensing, which can collect and transfer real-time data to offer computational intelligence. Moreover, sustainable resources such as devices, networks, and databases are intellectually equipped to standardize governance and service deliveries. The sustainable environment has a network infrastructure to collect, store, and analyze real-time data to provide an efficient decision-making process. IoT-enabled smart sustainable environments integrate advanced technologies to build people-centric smart cities and industries. Most service intelligence and technical schemas are easily accessible and applicable to authorize the scope of civic intelligence. However, the potential issues such as security and privacy are open to deal with the challenges of security requirements. A thematic classification of security and privacy issues is primarily focused on authentication and key management protocols to secure Industrial IoT environments. To highlight the potential visions of the smart cities/industries, in this survey, numerous security threats, techniques, countermeasures, and tools are reviewed to address the key challenges of smart service intelligence within sustainable environments.

Keywords Security · Privacy · Internet of things · Authentication · Key management · Smart cities

1 Introduction

At present, connected IoT devices are massively growing to meet the standard requirements of various application domains such as smart homes, smart cities, transportation, agriculture, and healthcare. The standard governance and practical limitations address numerical technical challenges for the evolution of large-scale networks. The technological advancements include connective components of smart devices such as sensors, actuators, and gateway to offer innovative application services. Most application scenarios demand a new computing paradigm to highlight the significant challenges such as data management, security, and interoperability. The emerging IoT frameworks consider an intelligent platform to deal with a different source of aggregated information. New innovative services integrate numerous transmission flows to assess the necessities of social and business infrastructure. Most of the urban populations realize the utilization of enabling technologies, namely connectivity, continuity, compliance, co-existence, and cybersecurity. The technical challenges of IoT deal with a system of physical objects to develop an intelligent machine that determines the existence of logistic operations.

The advanced intelligent systems, including smart cities and IoT, standardize the requirements of convergence technologies such as edge, fog, and cloud computing. A large-scale system integrates four essential layers, such as sensors (endpoints), edges (gateway), platform (artificial intelligence, management connectivity), and application software. The unprecedented growth in sensor technologies shows a remarkable vision of smart cities. It enables individuals to endure reliable, secure, and sustainable developments (Cui

✉ B. D. Deebak
deebak.bd@vit.ac.in

[1] School of Computer Science and Engineering, Vellore Institute of Technology, Vellore 632014, India

Published online: 03 February 2022

et al. 2018a, b). In general, smart cities can be defined in various forms (Batty et al. 2012) to refer to the computing infrastructure, including information and communication technologies (ICT). It realizes the course of technological existence to improve the qualities of the individual. It does not have any physical limitation to restrict the visionaries; thus, it can handle different processes to achieve technological innovation and entrepreneurial opportunities. The major contributors to smart cities are investigators/researchers, public/private sectors, academic institutions, platforms, services, and application developers (Appio et al. 2019). Table 1 shows the important abbreviations used in the given sections.

It is widely known that physical objects are interconnected over Internet-based services. It connects computers and computing devices to expand network connectivity across the globe. The motivation behind technological convergence is to connect the Internet-based components such as smart television, automation, transportation, manufacturing, energies, healthcare, etc. In Wu et al. (2018a, b), the authors show the existence of intelligent sensing to describe the development as a smart city nerve system that uses IoT to build an interactive platform in the real world. It is more indispensable to integrate the sensors, actuators, and networks, whereby the real-time objects can be effectively deployed to collect, process, analyze, and store sensitive data. The network connectivity may be a wired or wireless point designing a secure gateway to offer data confidentiality, authenticity, and integrity.

It is also called a collection point to use message queuing, transport, and application protocol to preserve privacy and energy consumption. Moreover, the applications of the smart cities operate on the cloud platform to provide a real-time interaction over a standard interface. It converges the architectures, technologies, systems services, network applications, and protocols to create a scientific environment. It is intended to use human ecosystems to offer smart cities with intelligence techniques that consolidate the development technologies to obtain prominent solutions (Zhou et al. 2018). The main objective is to use embedded electronics, communication technologies, interfaces, protocols, and applications to build a high-level internetworking environment. In recent times, it has been emerging as global demand to meet the goals of the public or private sectors. It can improve the service qualities to widen the scope of application services in different industrial perspectives, including the power grid, retail, surveillance, and autonomous systems. It is called critical and non-critical applications. The former deals with latency sensitivity, whereas the latter is non-latency sensitivity.

Nowadays, the IoT is evolving in modern industrial application systems to meet the industrial requirements of convergence technologies. It could achieve through real-time analytics and embedded co-design tools (Yang et al. 2017; El-hajj et al. 2019). IoT applications are primarily equipped with sensors and limited computing power to deploy in any real-time environment, namely telecom, finance, manufacturing, logistics, retail, e parking, transportation, and hospitality. Currently, various industrial applications play a vital role, including smart grid, waste management, agriculture, and energy management (Atzori et al. 2010). IoT collects the data of physical objects integrated with electronic devices to

Table 1 List of abbreviations used

Acronym	Definition	Acronym	Definition
IoT	Internet of things	VANET	Vehicular ad-hoc networks
IIoT	Industrial internet of things	CHAP	Challenge handshake authentication protocol
IDC	International data corporation	RFID	Radio frequency identification
ICT	Information and communications technologies	PBA	Prediction-based authentication
		IDS	Intrusion detection system
AKA	Authentication and key agreement	MAC	Message authentication code
M2M	Machine to machine	ECDSA	Elliptic curve digital signature algorithm
WSN	Wireless sensor networks	IDS	Intrusion detection system
ECC	Elliptic curve cryptography	EAP	Extensible authentication protocols
D2D	Device to device	TESLA	Timed efficient stream loss tolerant authentication
S-IoT	Social internet of things	TFA	Three-factor authentication
IoT	Internet of vehicles	SFA	Single-factor authentication
ECD	Edge computing devices	MFA	Multi-factor authentication
HAN	Home area networks	OTP	One time password
NAN	Neighborhood area networks	CPS	Cyber-physical systems
CCPPA	Certificateless conditional-privacy-preserving authentication	BAN	Burrows–Abadi–Needham
		HLPSL	High-level protocol Specification language

actuate the connection setup to transfer the data over a wireless channel. Importantly, it provides a feature of interactive communication between the network and the devices. They can be remotely connected to monitor, sense, and collect the environment data to control smart devices (Kashyap 2019). The smart city is another important application of IoT, in which they create interest among the world's population. Smart cities comprise various essential applications, including smart surveillance, automated transportation, intelligent energy management systems, water distribution, urban security, and environmental monitoring.

According to the IDC report (Analytics 2014), the IoT devices' growth is predicted to be 41 billion in 2020, with an $8.9 trillion market value. In the past few years, the conception of Smart Cities has been emerging to resolve urban issues concentrating on environmental changes. However, the idea of "Smart" has started dissemination that would imply a synergetic response to address the various problems, including traffic congestion, skyrocketing, overcrowding, loss of open space, and air pollution. As per United Nations Dataset, over 55% of the global population lives in urban areas; it is expected to increase by "68%" of the global population by "2050" (Department of Economic and Social Affairs 2014). Besides, it combines the overall growth of the world's population, which may add 2.5 billion by 2050, resulting in massive effects on climate changes, energy usage, and living conditions. To meet the above challenges and improve its well-beingness, "sustainable and intelligent systems" develop the modern cities more providence that makes the rapid advancement in information and communications technologies (ICTs) (Diane Vautier 2019). It plays an increasing role in the progress of both people and public and private entities that are part of a smart city.

In 2017, Cisco announced near about one-billion-dollar investment for the growth of smart cities. Smart city applications have a wide range of acceptance because of digital intelligence utilizing data collection in various domains such as energy use, mobility, education, human wellbeing, knowledge transfer, and urban development (Townsend 2013). Sustainability attracts attention to the construction and utilization of resources necessary for private, modernistic industrial, residential, transportation, and commercial procedures (Deakin and Al Waer 2011). The notion of a smart city is moderately new and can be viewed as a successor digital city and sustainable city. In general, smart cities make use of ICTs widely to assist cities in building their competitive advantages, or that can be a visionary model where urban development could accomplish over technology enhancement (Anttiroiko 2008). An expanding significance to adopt smart solutions could determine urban growth as far as looking for approaches to address the related difficulties. Besides, it guarantees the impact of ICT development to improve urban growth because of mutuality (Chourabi et al. 2012). While considering security and better advancement of smart city innovations to customers, data privacy and preservation play a significant part in the development of smart cities using IoT (Scroxton 2020). Therefore, security and privacy are majorly concerned with preventing malicious activities in open-IoT environments.

As millions of devices are going online to share the data between the devices, the aggregate information may transfer over wireless channels without any direct involvement between humans to a computer or human-to-human interaction (Gubbi et al. 2013). IoT requirements and limitations address several challenges, including a number of device connectivity, device authentication, and confidentiality of data transfer, service protection, identity management, network access control, and hardware security to summarize the current state of literature (Rouse 2018). Gartner's report says that 20 percent of communication systems have had at least one IoT attack over the last few years, including Mirai Botnet and Persirai (Maresch and Gartner 2018; Ahmed and Kim 2017; McAfee 2017; Masters 2020). To withstand these issues, a standard security mechanism is highly demanded. As a result, authentication and key agreement (AKA) protocols play a significant role in providing high-security levels to various application domains, namely smart homes, wearable devices, smart cities, smart farming, and supply chain. Resultantly, several authentication mechanisms have been proposed to enhance the security of smart cities using IoT systems. However, many security mechanisms have some limitations to satisfy the standard requirements of the application domains.

Of late, various survey articles have been issued in the reputed publishers such as IEEE Digital Library, Wiley Online Library, IET Library, Sciencedirect, and Springer, considering challenges in IoT-based industrial environments. With the development of smart cities, massive IoT devices are connected online and open doors to several vulnerabilities. To protect the IoT devices in smart cities/industries, a variety of security mechanisms such as single-factor, two-factor, multi-factor, password-based, and identity-based have been implemented. As an instance, Lin et al. (2017) analyzed security and privacy issues and presented edge-based IoT applications. Their analytical study revealed the relationship between the cyber-physical system and IoT. Gharaibeh et al. (2017) showed research challenges on smart cities achieving resilience in data management against security and privacy threats. Their study identified several strategies such as authentication, confidentiality, privacy, trust, access control, and mobile security. Moreover, their analytical study highlighted several open challenges and technical approaches, and future directions. Furthermore, Reddy et al. (2018) analyzed secure pseudo-identity-based device authentication for smart cities.

Their proposed scheme has a security model based on authentication and key agreement between the IoT gateway and a mobile client. The real-time scenario considers mobile devices as a client and IoT gateway as a server to identify the potential threats (Al-Turjman et al. 2017; Deebak et al. 2020; Fadi and David 2020).In the prodigious vision of smart cities, the IoT networks connect a massive amount of sensors and devices to identify the fundamental challenges, including architecture, system governance, security, and privacy issues. These are the most important factors to signify the issues of IoT networks, such as availability, integrity, and confidentiality (Deebak 2020). It may apply a suitable strategy to meet system requirements, which may differ from centralized to decentralized networks. Therefore, security aspects are primarily concerned with authentication mechanisms to categorize the present and future developments within smart cities and industries. The emerging technologies analyze the network pattern or intruder behaviors to design a suitable detection system that represents the vector space in the form of multilayer perceptron (MLP) (Sudqi Khater et al. 2019) or machine learning (ML) (Hodo et al. 2017) or deep learning (DL) (Vinayakumar et al. 2019) or deep transfer learning (DTL) (Perera and Patel 2019).

Moreover, the smart IoT networks apply the authentication framework to authorize the activities of real-time entities such as sensors, smart devices, gateway/application servers, and remote servers. Real-time entities make an effort to establish secure communication over public or private networks. Most real-time systems cover the scope of potential attacks to prevent the vulnerabilities such as guessing, denial of service, masquerade, and man-in-the-middle. In general, the authentication mechanisms include three system phases, such as user identification, authentication, and authorization to guarantee privacy protection, people safety, and information credibility. The real-time device or server should register their confidential data to gain authentication access during the system login phase. In the execution of registration, login, and authentication, security and user privacy should be mutually considered to the efficiency rate of the communication or network system. The knowledge-based system or model has the potential threats to weaken the process of authentication that applies brute-force or dictionary-based to capture the screening process of virtual keyboards. The IoT research community has engaged its growth in the platform, people, and connectivity. The emerging technologies generate a massive amount of real-time data to offer competent features such as business opportunities, productivity, and cost reduction.

However, the development of IoT applications addresses potential threats such as trust, access control, security, and privacy. Thus, this paper extensively discusses security and privacy issues to highlight the core contributions of smart cities. At present, IoT is playing a crucial role in addressing the broad aspects of convergence technologies such as smart cities, industries, healthcare, grid, farming, transportation, etc. The converging technologies have several technical, political, and socioeconomics benefits to address challenges such as security, privacy, and risk assessments in smart cities/industries. The application systems highlight the threat models to administer the activities of real-time entities, including information security, infrastructure, platform development, storage processing, and management. In this study, security and privacy issues have been learned to focus extensively on authentication and key agreement mechanisms to evaluate the multi-criteria techniques, such as two-factor, three-factor, multi-factor, etc. To leverage a combination of key findings, comprehensive searching has been practiced using computer-assisted databases such as Springer, Sciencedirect, IET Library, Wiley Online, and IEEE Xplore, etc. In the last few years, major research studies have been conducted for IoT application systems (Mabkhot et al. 2018).

Most review papers strictly focus on the challenges and issues of smart application systems (Sabri et al. 2017; Jiang et al. 2018). This survey article covers major viewpoints to conduct a rigorous study on the issues of security and privacy. The major contributions are as follows:

1. Demonstrate a rigorous analysis of the state-of-the-art approaches to address the security issues of smart IoT applications.
2. Highlight a comprehensive survey of designing a secure IoT system to relate the security requirements with smart cities/industries.
3. Review several authentications and key agreement schemes to identify the current challenges in smart IoT.
4. Evaluate the security assessments to discuss open issues and effective countermeasures

The rest of the paper can be structured as follows: Sect. 2 discusses the evolution of ICT-enabled smart cities/industries application service, security issues, and potential threats to highlight the competent features in IoT sustainabilities. Section 3 explains the designing of a secure system, security requirements, malicious attacks, and perceptive of smart cities to outline the emerging area in smart IoT. Section 4 discusses the challenges in smart IoT, including device security, a key management protocol, and privacy-preserving. Section 5 focuses on countermeasures and validation tools to assess various authentication protocols. Section 6 summarizes the contributions of the survey article to realize the critical derivatives of key management protocols. Section 7 concludes the review work.

2 Background research in smart cities/industries

This section discusses the evolution of ICT-enabled smart cities/industries, system architecture, role of IIoT, management platform and architecture, application service, security issue, and potential threats to review the functional pillars of the smart cities/industries.

2.1 Evolution of ICT-enabled smart cities/industries

The future generation of urban evolution is moving beyond connected devices. Smart cities in the future employ governments, visitors, businesses, and citizens in an intelligent, connected system. Indeed, the smart city speaks to essential effectiveness that relies on smart management of urban systems utilizing ICTs (Chaturvedi and Kolbe 2019; Habeeb et al. 2019). The prime goal of a smart city is to support better services and quality of life for residents and visitors. An environment is consciously focusing on sustainability and economic competitiveness to attract industrial competencies. The evolution of smart cities increases people's experience and city decision-making using digital data (Jeschke et al. 2016). Smart cities' sustainable development makes compact regions on a reproducible model that should act as a beacon to other aspiring cities (Jin et al. 2014). Of late, various developing countries, including India, Indonesia, Egypt, Zambia, Yemen, and Romania have emerged with the demands for different core infrastructure elements, namely social community, people use, governance, mobility, economy, and environment as shown in Fig. 1. Moreover, these elements are also a part of smart city requirements to create a sustainable environment (Devarakonda et al. 2019). The concept of smart cities is rapidly gaining importance by using all the applications and services enabled by ICT to the citizens.

A competent society can be transformed into a smart city based upon six characteristics: people, environment, living, economy, mobility, and governance. Most strategies focus on physical infrastructures such as water, energy, waste, energy, transport, and communication technology through ICT. However, the soft infrastructure focuses on services to maintain people's economic and social capital in terms of knowledge, equity, safety, and participation (Nam and Pardo 2011). Smart cities acquire the importance of ICT-enabled applications and services where people, industries, and authorities are the parts of the development of smart cities. The general objective is to improve the quality of people's life, user efficiency, and quality of experiences provided by governing bodies and business regulations. The core concept of a smart city is to utilize the computing resources such as transportation, energy, payment system, public safety, and security. It is revealed that at least 10% of energy demands fulfills by solar energy. In contrast, at least 80% of constructions in Greenfield projects utilized the resource base efficiently to develop a sustainable environment. Moreover, smart public services such as streetlights,

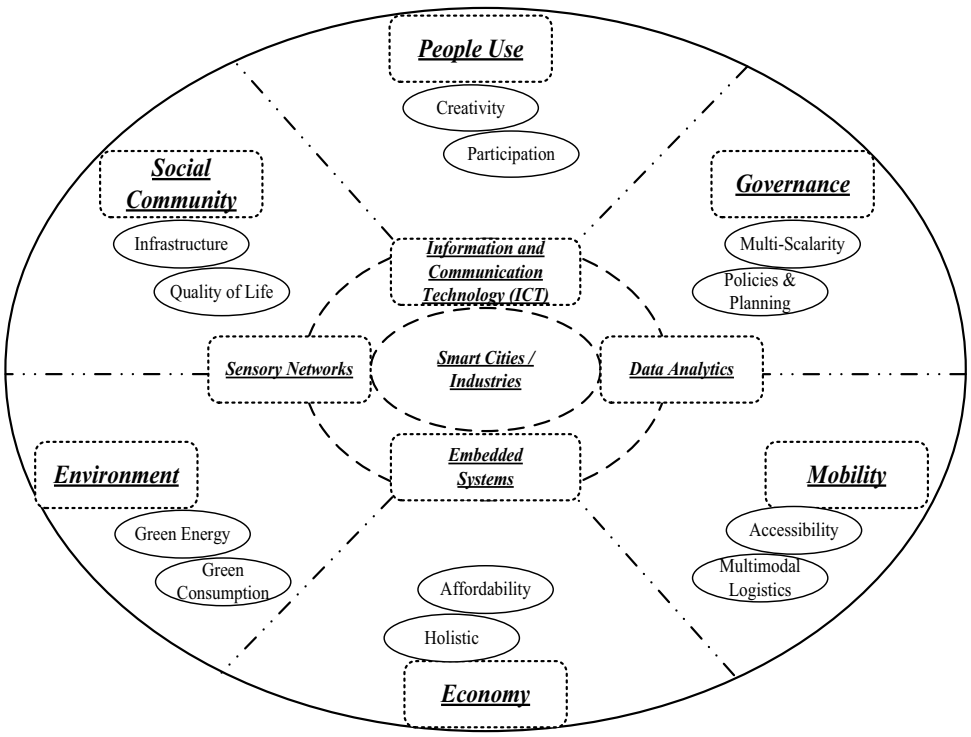

Fig. 1 Multi-dimension of ICT-enabled smart cities/industries

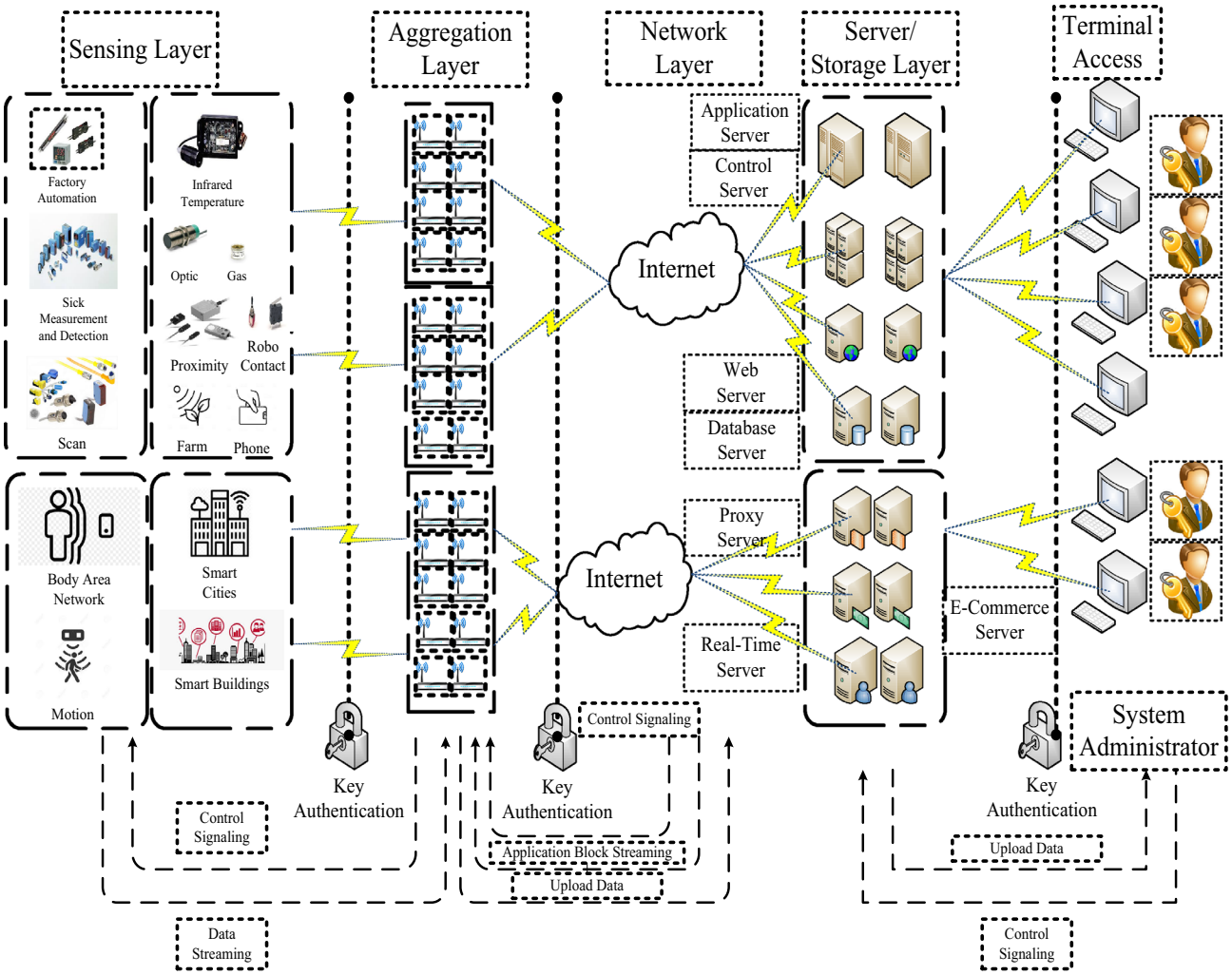

Fig. 2 System architecture for ICT-enabled smart IOT networks

traffic management, rainwater harvesting, and wastewater-recycling plans can be automated to improve safety and mobility (Pellicer et al. 2013).

2.2 System architecture: ICT-enabled smart IoT networks

Most of the real-time entities use a large number of sensing devices to form a group of interconnected objects that can be either static or dynamic to build an intelligent system. In industry, the applications of IoT connect with interconnected networks and cyber-physical systems to refer to the environment as industrial IoT (IIoT). It aims to design intelligent systems such as smart factories. It cooperates with customers and business partners to digitize the process of physical objects (Butt and Afzaal 2019). It is commonly referred to as Industry 4.0 that trains sensors, actuators, and networks to visualize the production flow that makes the system to produce a firm decision process. Figure 2 shows the system architecture for IoT-enabled smart networks. It has possession of sensor devices, machinery, network components, servers, cloud, and application software to cater to the specific needs of end-users. Besides, it encompasses sensing, aggregation, network, server/storage, access, and management to meet the legal constraints of the smart manufacturers.

Sensing and aggregation It integrates intelligent hardware, including radio frequency identification, sensor, and actuators, to the sensor or controls the machinery system. It can periodically feed real-time data to simplify the process of automation that associates the server or storage to send or store sensitive information. Since the sensors have a limitation of physical device constraints, it can rely on some dedicated operating systems, such as Contiki, TinyOS, RIOT, etc. It uses IoT-OS as a distributed platform to handle the software and hardware that offers centralized management (Bibri and Krogstie 2017).

Service and storage It associates a centralized network to provide a reliable service to the application, images of operating systems, and private data. It highly demands data streaming, whereby the multiple applications and operating systems are involved in loading and executing their requested services at the aggregation layer. It makes a logical connection to exercise the basic services, such as user authentication, management, device monitoring, and data storage, to protect the activities of software resources.

Interface and management It characterizes the important specification of smart applications and network services. It simplifies the issues of interconnectivity to manage a set of services interacting with the dedicated systems. It associates with the service and storage to analyze the real-time data shortly upon the protection of privileged certification. Consequently, it may track the activities of the industrial environments to analyze or monitor based on indexing, whereby the real-time data can be analyzed effectively to categorize the working status or scheduling process of the systems.

2.3 Role of industrial IoT in cyber-physical systems

It refers to the industrial revolution as Industry 4.0 that looms on the horizon of industrial automation and productivity. It emerges two key standards, such as industrial IoT (IIoT) and industrial cyber-physical systems (ICPS), to interconnect the system devices and hardware equipment, as shown in Fig. 3. It applies the cyber-physical system to manage critical real-time systems such as infrastructure, transportation, and power generation (Eggers and Skowron 2020). Moreover, it executes the system commands to ensure data security, service resiliency, and scalable automation. The convergence of IoT and the cyber-physical system provides better productivity to manage the automation and manufacturing process. In the ICPS, the industrial devices interconnect machines, assembly lines, system terminals, and control devices to form any smart factories, such as textiles, petroleum, chemicals, computer, and electronics. Smart devices or applications are the parts of vertical industrial systems to categorize into cyber and physical space. It integrates the IIoT to interconnect the machinery objects, whereby an effective development can be achieved.

Additionally, it incorporates three important layers, such as application, communication, and physical, to meet the industrial standards. Each industry has its application software to actuate some real-time features such as a monitor, control, data exchange, efficient management, and fault handling (Smart Cities Mission 2020). It has a communication layer to integrate network connectivity, including wired and wireless. Moreover, it includes a massive amount of devices or sensors to connect in the industrial environments physically. Finally, it has a physical layer that includes sensors, actuators, machinery equipment, and utilities to design or discover a suitable automation process. In the design of any industrial application, process automation and the functional

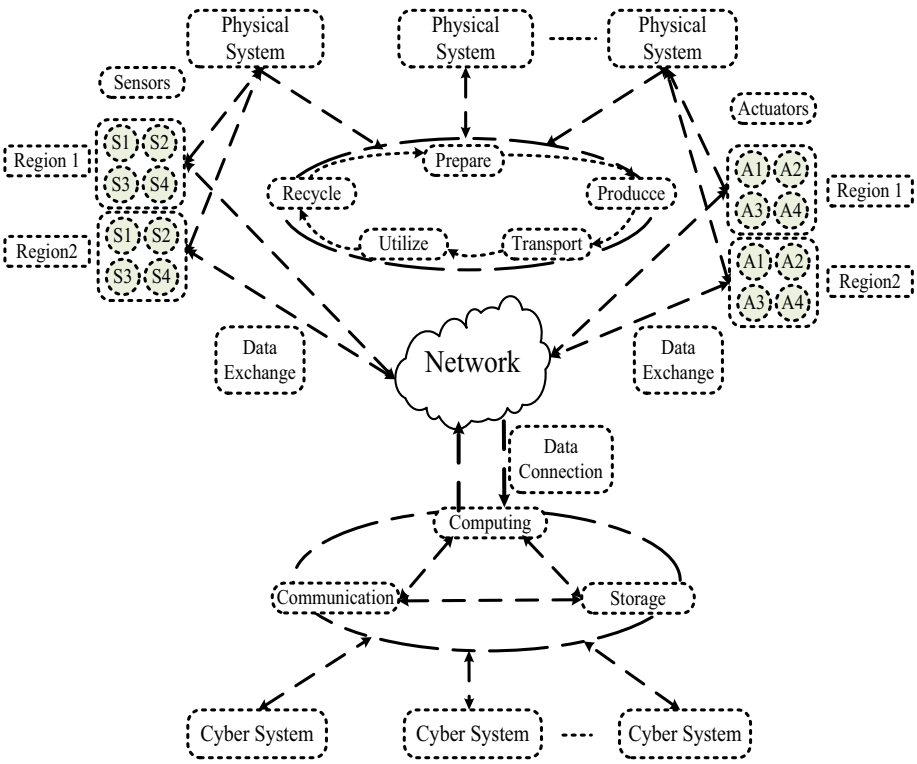

Fig. 3 Perceptive of industrial cyber-physical systems

groups play a crucial role in generating real-time data, which is from different machinery devices or equipment.

Each device or equipment holds its controller, networking, and computing machines to integrate the physical components and systems. However, it could logically manage the process of automation to perform the process of device control and data monitoring. It can substantially improve whereby the performance efficiency of the physical systems. The industrial applications involve IoT to cover the objectives of the real-world scenario that deeply understands the typical characteristic of critical production and transportation (Vembu 2020). It uses process automation to analyze and diagnose the industrial process without human intervention. Moreover, it integrates sensors, actuators, and controllers to analyze the system effectively. Similarly, it applies factory automation to leverage the assembly lines of the machinery that enables effective manufacturing to improve production efficiency.

2.4 Smart cities/industries: management platform and infrastructure

Notably, the IoT plays a vital role in connecting physical devices with the Internet through various protocols to communicate and transfer data between distant locations. To achieve intelligent recognition, tracking, location, monitoring, and management, the researchers have focused on the broad aspects of IoT such as automatic control, network infrastructure and communication system, cloud storage platforms, and big data analytics (Paul and Jeyaraj 2019). Subsequently, to build a sustainable society and environment, the advancements in information technology promote a multi-disciplinary approach to create novel applications and integrated solutions. The promising applications can interconnect the physical and virtual world with electronic devices distributed in public environments such as vehicles, homes, buildings, and streets (Chin et al. 2019). The emerging IoT-based Smart cities have been working for the benefit of both administrators and citizens (Cardullo and Kitchin 2019). The smart city services include smart vehicles, smart parking systems (Li et al. 2015), smart homes, weather systems, waste management, smart energy management, smart grid, environmental pollution, surveillance system, and vehicular traffic (Samarati and Sweeney 1998).

Hence, it is a mandate to further research the advancements in terms of technologies and applications in the area of IoT-based Smart cities. Figure 4 depicts the smart cities management platform. IoT infrastructure shows significance in the development of smart cities, primarily categorized into two types as follows:

Core infrastructure This category includes physical, social, economic, and institutional infrastructures; and

Smart solutions In this category, good governance, smart electricity, environment, transportation, IT Services and communications, Education, health, smart buildings, etc., are included to foster the utilization of urban services.

In smart cities, the prime objectives of the core infrastructure are to raise the quality of a citizen's life and to accomplish a clean and sustainable environment. With the promising solution of smart applications (Li et al. 2015),

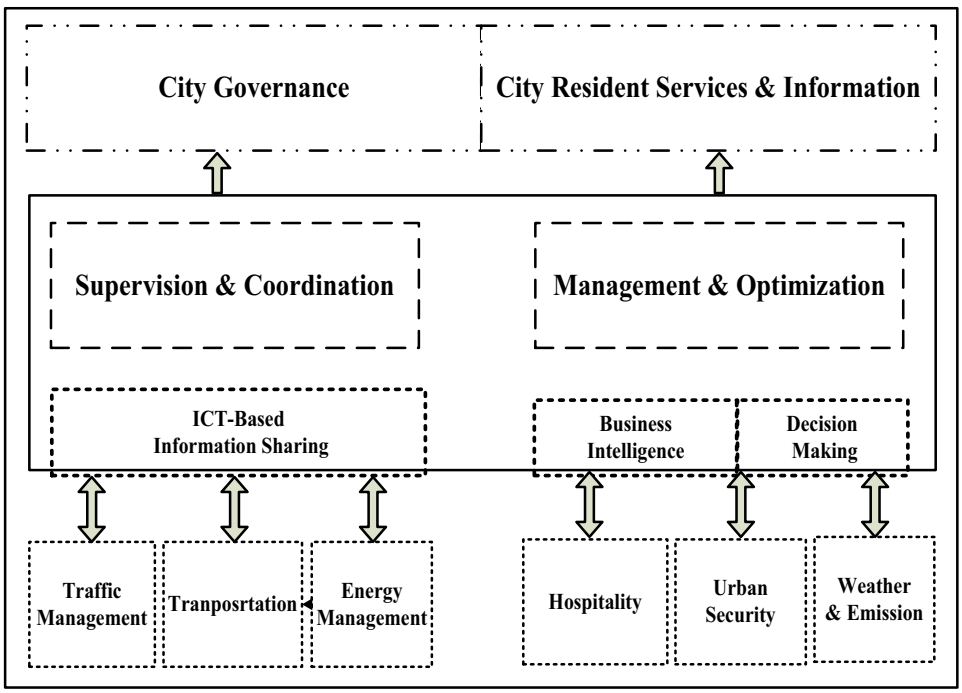

Fig. 4 Smart cities: IoT-based management platform

smart cities gain more attention to providing better living conditions to humans. The promising solutions of smart cities incorporate various technologies such as IoT and information and communication technology (ICT) to evolve standard infrastructure based on the features of IoT. Due to the massive variety of devices and services involved in the development of application interfaces (Gil et al. 2019), the functionalities such as governance, supervision, management, and optimization are recommended to enhance the accessibility of smart cities, as shown in Fig. 4.

2.5 Smart application services using IIoT

IoT considers various heterogeneous applications to offer seamless connectivity over the Internet. The dynamic environment provides ease of access and efficient usage to minimize the latency in delay-sensitive applications. Most intelligent systems use sensory technology to collect, process, monitor, analyze, and store sensitive data remotely. The sensory networks consider power consumptions to extend the durability of the system to improve system performance. Moreover, an application such as smart parking consumes less computation power to avoid parking issues, whereas smart buildings decentralize the process of automation control to estimate the health of buildings, waste management, and predictive maintenance (Li et al. 2015).

Structural health of buildings A continuous monitoring system initializes appropriate maintenance of the historical buildings in the smart cities. The actual conditions of the buildings are identified to evaluate the structural factors such as vibration, data fusion, and electromechanical impedance.

Waste management In modern cities, waste management is one of the major issues due to the service cost and the storage of garbage in landfills. With the deeper insights of ICT solutions, the use of intelligent systems is to enable garbage containers to determine the level of load and permit for optimization of truck roots. The waste management mechanisms and IoT can be integrated as a standalone device to minimize the cost of garbage collection and to enhance the quality of the recycling process.

Traffic congestion The traffic control systems connect the urban IoT systems to monitor traffic clogging and vehicle safety in the urban area. However, an existing mechanism such as camera-based traffic monitoring systems is widely deployed to provide an optimal decision-making process. Moreover, low-power channels can deliver a better monitoring service to accomplish the sensing capacities. The vehicle can install a GPS unit to track the live location of the users.

Noise monitoring In the workplace, the IoT can sense pollution index to measure the assessment factors such as sound level meter and integrating sound level meter. A standard noise monitoring system can be installed to compute the amount of noise-induced at any given time in the urban area. Also, the system can utilize a noise detection mechanism to provide public security and to conduct a noise assessment regulated by the pollution control board.

Smart homes and buildings The heterogeneous tools use IoT assistance to enable automation of systematic activities that help to monitor and control the devices remotely.

Air quality management The growth of the urban population increases in-vehicle usage and energy consumption which leads to permanent urban pollution. The advancements of IoT, such as sensory networks and communication technology, discover air quality monitoring systems. The systems are small in size, less expensive, and more localized to sense the pollutant factors such as temperature, traffic, and radiation.

Smart parking The parking system develops an IoT-based device to track the arrival and departure times of vehicles across urban areas. The parking slots are initialized to provide massive benefits to the consumers in their routine lives. The parking services are completely based on a sensory tracker deployed at the roadside, which can detect optimized paths to park vehicles. It could provide various benefits, including traffic congestion, signaling, the vehicle emission rate of Carbon Monoxide. The low range communication technologies such as NFC, RFID, and BLE make the e-verification process to offer better services to the public citizen.

Smart energy management An IoT service allows to monitor energy usage and produce optimized management services. The authorities can view the details of the energy management, including lighting, transport, control cameras, traffic lights, to identify the sources of actual energy consumption to optimize their operational cost.

2.6 Layered IoT architecture: security issues and potential threats

IoT offers smart and self-configured devices measurably connected to global grid infrastructures. The devices can assure enhanced performance, security, and reliability of the smart cities and their infrastructure. The basic architecture of smart cities comprises four layers, namely the perceptron, network, service, and interface to collect the confidential data. Moreover, it allows the network layer to enable transmission of bidirectional communication, whereas the service layer analyzes the confidential data and the application layer provides a graphical user interface to the users (Qin et al. 2020). The landscape of IoT with four layers is depicted in Fig. 5.

Perceptron layer This layer collects confidential data through sensory devices and transmits them to the network layer. In this layer, a group of Internet-enabled devices could connect through a wireless communication channel to identify, detect, gather, and enhance data services.

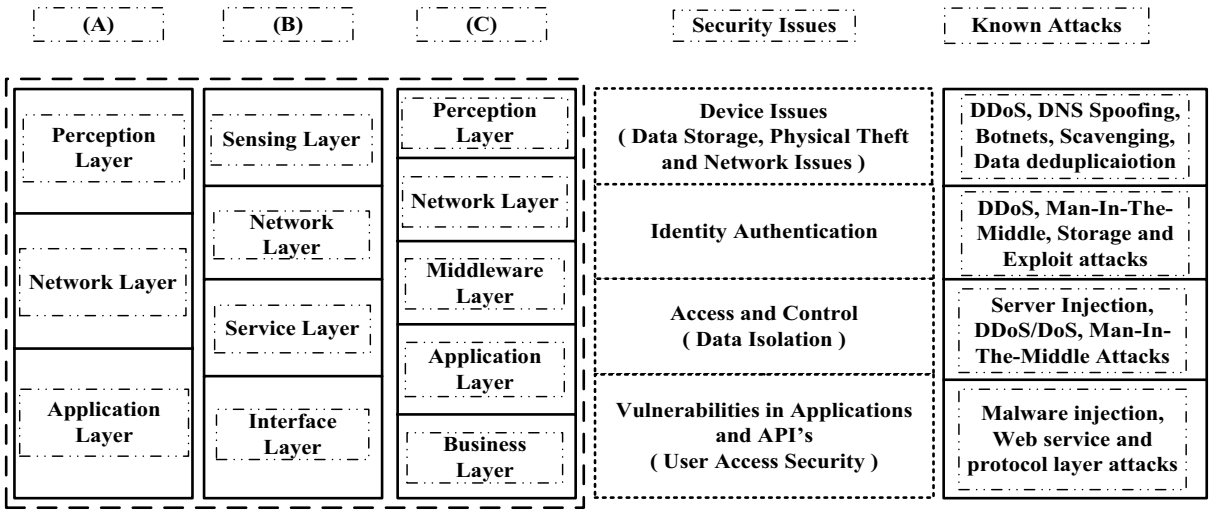

Fig. 5 Security issues and attacks of typical A three layered (Da Xu et al. 2014), (B) four layered (Khan et al. 2012), and (C) five layered (Wu et al. 2010) IoT architectures

Every sensing device connects with a network, and thus, it can collect private information through a trusted wireless communication channel. IoT device generates a unique ID in the distributed network to monitor and infer anonymous activities. Presently, the security challenges of the perceptron layer secure the IoT objects from unauthorized access and protect them from DoS attacks and routing attacks. As a result, an unauthorized device cannot perform any malicious activities. Moreover, the sensing source is capable of low computation power and storage capacity. Data protection is highly obliged to handle memory wastage or any data hazards. To test realistically, heterogeneous networks equipping with sensing devices generate the data over insecure public networks. Hence, the generated data can be encrypted using public and private keys to ensure data protection before transmitting to any distributed systems.

Network layer The network layer is one of the essential parts of the infrastructure in IoT architecture. This layer has a responsibility to make addressing and route the data packets delivered from one place to another using an IP address. IPV4 and IPV6 are the standard protocols of the network layer. Since IPV4 is exhausted and incapable of processing the transmission with the scalability of the IoT applications, the IPV6 standard has been adopted to accommodate address space to enable a massive number of IoT devices. The coordination of short-range communication technologies and Internet communication technologies have been utilized for the connectivity of IoT systems. Bluetooth and Zigbee are the real-time instances of short-range communication technologies to transmit the data between physical devices to the nearest gateway based upon the capacities of communications channels. Wi-Fi, 4G, 5G, Power Line Communication (PLC) are the instances of Internet technologies to carry the information over the long-distance (Roggema 2020).

Service layer This specific layer depends upon the basic needs for IoT infrastructure that allows or disallows data services of the user's application or device connectivity. The service layer comprises business logic, service division, service integration, service implementation, and service repository to explore as an essential part of the service layer because IoT devices have limited space to store the data. Therefore, this layer includes cloud storage as a logical pool to examine the security aspects such as availability, immutability, scalability, and verified access. Moreover, this layer supports secure end-to-end information exchange amongst IoT devices and applications providing proper authentication, authorization, identification, encryption, remote provisioning and activation, buffering, synchronization, and device management (Chahal et al. 2020).

Application layer It is one of the essential layers to retrieve, process, and visualize the application requests. Initially, the system examines the requester node to identify whether the data can be stored securely in the cloud or not. The distributed nature of IoT is not necessary to set up any additional server components to generate massive data processing (Mahmood 2020). Moreover, IoT has a rapid growth in the connection of physical objects that increases the usage of smart devices in all the application domains such as automation, monitoring, and controlling. However, the key findings, namely security, privacy, and performance efficiency, are majorly concerned with managing IoT infrastructure and services. To fulfill the above key challenges, it has several limitations: (1) IoT applications and their services are not utilizing the standard technologies; (2) there are no standard network protocols such as Wi-Fi, BLE, SigFox, LoRaWAN,

and Zig Bee to develop IoT-based application systems; and (3) there is an increasing number of resource usage in terms of processing power, data storage, bandwidth, and computation (Deebak and Al-Turjman 2020). At present, several distinct networking protocols are in use, including 3G, LTE, and other higher frequency bands. However, there is no such device to establish secure communication with current networking protocols. The gateway or an IoT device creates a heterogeneous network to include big data and cloud computing to expand the use of resources such as processing speed and storage computation (Astill et al. 2020). Since it is emerging as a computing paradigm, physical devices can easily establish a broader range of communication. Table 2 summarizes the security requirements, services, adaption, and challenges for IoT-smart cities/industrial environments.

2.6.1 Standard protocols in IoT devices

IoT communication platform comprises sensory devices, network gateways, communication protocols, network management, and storage systems. Various protocol entities are involved in developing smart cities (Al-Turjman et al. 2020). Firstly, IoT communication protocols operate at physical and data link layers to examine the critical components of the IoT communication system. These protocols are classified as follows:

IoT data protocols It can *enable* physical devices to exchange information from one to another. Numerous legacy protocols such as MQTT, CoAP, AMQP, Rest, XMPP, STOMP are preferred to support data transfer.

IoT communication protocols The protocols work at a lower level of connectivity with the IoT cloud platform. Various networking protocols such as Bluetooth, Zigbee, SigFox, LoRaWAN, Z-Wave, 6LowPAN, Thread, Wi-Fi, Cellular, NFC, Neul, RFID, LTE cat 0, 1 & 3, ANT&ANT+, DigiMesh, MiWi, EnOcean, Dash7 can work in short and long-range media to meet the demands of service-based IoT systems (Garcia-Carrillo and Marin-Lopez 2018). In general, Internet protocol versions such as IPV4 and IPV6 support IoT implementations at the network layer of the OSI model (Kraijak and Tuwanut 2015). Wireless sensor networks based IoT connects the smart devices over IPV6 such as bluetooth low energy (BLE), 6loWPAN, Zigbee, and Z-Wave to offer end-to-end connection. SigFox and cellular are the wide-range standard protocols for operating a low power wide area network (LPWAN) (Raza et al. 2017).

2.6.2 Security issues in IoT-enabled smart networks

The adaptability features of sensors and embedded electronics integrate cloud computing and IoT to improve security and trustworthiness. The majority of business applications use an Internet-based computing system to rely on a massive amount of real-time data. It connects the physical objects to collect sensitive information discovered by IoT systems (Tewari and Gupta 2020). Communication fields utilize wired and wireless technologies to provide the system functionalities including, accessibility, availability, reliability, extensibility, scalability, etc. However, security and trustworthiness highly demand hardware solutions and trusted software to minimize the transportation risk of the communication protocols. Technological advancements enable the IoT environment to develop innovative products and services (Farahat et al. 2019). It can rely on a smart, intelligent platform to design smart cities and cyber-physical systems that enhance the use of field-programmable gate arrays (FPGA) in cloud, edge, and fog computing. To a predictable degree, the infrastructure of smart cities and industries embeds billions of hardware devices to connect various real-time applications, namely transportation, surveillance, homes, environment, and governments (Zhang et al. 2017a, b). However, these application systems address security and privacy issues to protect data transmission. Due to network vulnerabilities, each layer can easily be prone to various security threats such as Sybil, denial-of-service (DoS) to degrade the qualities of intelligent systems.

Moreover, the service providers collect real-time data over the cloud or third parties, where the privacy threats are highly examined. Of late, various systematic studies have been published to address the issues such as security, privacy, and data protection (Braun et al. 2018). Most application systems have limited energy resources; thus, it prefers to use simple cryptographic algorithms (Alomair and Poovendran 2014). Moreover, ineffective strategies may lead to several security threats to real-time application systems. The traditional computing systems challenge addressing key issues, such as the heterogeneity, scalability, and dynamic characteristics of the smart application systems. The development technologies apply data mining, machine learning, deep learning, reinforcement learning, etc. These techniques play a crucial role in developing a suitable mechanism that protects smart cities or industries (Moustaka et al. 2019; Al-Turjman et al. 2019). It may provide a potential opportunity to strengthen the promising solutions of the application systems.

3 Thematic analysis: security requirements, malicious attacks, and perceptive

This section discusses designing a secure system, security requirements, malicious attacks, and perceptive of smart cities and industries to formulate a better roadmap in the emerging areas of smart IoT environments.

Table 2 A summary of security requirements, services, adaption, and challenges for IoT-smart cities/industrial environments

Layers	Security					Challenges	Secure adoption
	Requirements	Services					
Perceptual	Device security	Authentication and key agreement	Authorization and integrity	Confidentiality and non-repudiation	Availability and privacy	Secure communication	Mutual authentication between connected devices
						Frequency jamming	
	Secure device manufacturing					Access control	
						Vulnerable to DoS and interference	
	Lightweight encryption solutions					Social engineering assaults	
	Key agreement					CIA of sensor node	
	Data security					Identification and authorization	
	Wireless sensor network security					Insecure initialization and configuration	
	Node level security					Insecure interface	
Network	Intrusion detection					Attack tolerance	Integrity and confidentiality of data collected by devices
	Communication					Malicious node isolation	
	Secure routing					Secure route establishment	
	Attack detection					Attack tolerance	
	Privacy and confidentiality					Malicious node isolation	
						Quick recovery from vulnerabilities	
	Constrained resources					Insider resource blitz	
						Resource-efficient counter steps	
	Robust and resilient management					Profiling and localization of the tracking system	
Application	Privacy protection					Cryptographic techniques	Legitimacy and Integrity of software and devices Privacy preservation to the sensitive data
	Information security					Denial of service	
	Freshness					Authentication and access control	
	Forward secrecy					Application software liabilities	
	Backward secrecy					Insecure interfaces	
	Data access and control					Insecure middleware/ operating system	
	Physical application auditing mechanism					Enormous data handling	

3.1 IoT design: an approach to secure systems

Today, the term security coins the necessary provision of security services, including confidentiality, integrity, availability, authentication, authorization, and non-repudiation. The security systems utilize various cryptographic algorithms such as hashing, symmetric, and asymmetric. The cryptographic algorithm can standardize key management mechanisms to handle the generation of cryptographic keys. Moreover, the security mechanisms comprise several techniques to restore, preserve, and protect the information in computer systems over malicious attacks. Of late, IoT has accomplished massive research achievements; however various key issues are yet to resolve in the presence of security at each level, including device, communication, computation, and storage. The security systems focus on security functionalities to execute service requirements of IoT environments (Grammatikis et al. 2019). The physical device connectivity leads to addressing severe life threats. The network advancements are indirectly converted into adverse circumstances exploited by attackers. Various attack scenarios demonstrate the level of destruction (Chen et al. 2018) to develop IoT environments to handle sensitive information. The design strategies of the IoT systems are generally categorized into five types: network security, identity management, privacy, trust, and resilience (Iqbal et al. 2017).

Network security requirements It describes the requirements, including confidentiality, integrity, authentication, availability, and freshness.

Identity management It is an organizational procedure to authenticate and authorize user requests. Moreover, it can discuss various challenges to initialize the complex relations between the entities and systems in IoT environments. It deals with multiple objects such as physical devices, servers, service providers, owners, and users to meet the essential requirements of identity management such as authentication, authorization, revocation, and accountability.

Privacy It refers to the requirements of data privacy, pseudonymity, anonymity, and unlinkability to manage two-way data transmission between the networks and the protocols. Moreover, it can assure "non-accessibility" to private information over pubic or harmful objects (Choi et al. 2019).

Trust It refers to the integration of four distinct components such as IoT devices, network connectivity, data processing, and application interface to deal with data trust and entity trust. It can indicate an unexpected action of entities such as physical devices, service providers, servers, owners, and users to offer an entry point over a dedicated network.

Resilience It prefers large-scale IoT systems such as industrial applications, smart cities, and other related complex IoT systems to achieve acceptable security levels. These systems are highly susceptible to several known attacks, vulnerabilities, and failures because of the complexity and modernization of software and hardware functionalities. As a result, it is essential to guarantee resilience and robustness in case of system failures. Therefore, an intrusion detection system (IDS) offers protection against malicious attacks (Nadeem and Howarth 2013).

3.2 Security requirements

The standard key requirements of authentication and key agreement protocols are as follows:

Authentication and authorization It can guarantee the integrity of IoT devices to establish secure communication. However, the authentication procedure requires a few standard requirements to include a lightweight mechanism. Many IoT devices have limited computing, processing, storage, and battery to utilize a multi-factor authentication mechanism. The schema works with multi-factor authentication to apply encryption techniques such as RSA, SHA, AES, and ECC to enhance the levels of security (Ragab et al. 2019).

Confidentiality It cannot disclose confidential information to any users, and thus data can only be accessible to authenticated users. Public-key cryptography is a well-known standard method to assure the integrity of sensitive data. However, this approach demands more key resources such as computation and communication costs. As the sensory networks are resource-constrained, this approach cannot resist known key attacks. As a result, various security protocols have been proposed using symmetric-key cryptography for the application domain of wireless sensor networks (WSN) (Ghani et al. 2019). It can prevent unauthorized user access to achieve better security efficiency.

Integrity It ensures that the transferred data cannot be modified during transmission and storage. Also, the data contents can be more intact to guarantee searching accuracy and device protection.

Availability The appropriate networks and their services authorizes applications and data to assure that the IoT devices can improve the physical infrastructure to streamline the accessibility of resource constraints like power loss or DoS attacks.

Accountability It can operate the authorized entities such as devices, service providers, servers, owners, and users to guarantee uninterrupted access to the networking devices. However, a key challenge of an IoT-based environment is to deliver accountability due to the number of devices, access entrustment, and multiple organizational domains.

Freshness It can verify the newly added information of the communication parties to make sure that an attacker cannot replace the previous sessions.

Perfect forward security It can guarantee that the session keys cannot be compromised to disclose confidential information such as the private key of the server. Also, it may protect previous sessions against unknown session keys

and password cracking. Using SSL/TLS, the transport layer network can preserve data confidentiality to provide information security over a dedicated network (Malhi et al. 2020).

Data privacy It may ensure that the confidential data is accessible only to the trusted communication parties. It may include personally identifiable information to prevent malicious threats in IoT environments.

Backward and forward secrecy To maintain data secrecy, including forward and backward, the key generation center (KGC) broadcasts a newly generated message when a new node joins a network. Also, it may guarantee that the attackers cannot discover any session key from the previous sessions.

User anonymity It can ascertain that unauthorized uses cannot determine the original identities of the legitimate users to gain user access without disclosing any personal information of an individual.

Unlinkability It can ensure that the data or operations connected to the same individual cannot be linked together.

Pseudonymity It may refer to a tradeoff between anonymity and accountability to create a link between the data and operations to perform an action of a "persona" instead of the original name.

3.3 Malicious attacks

The potential attacks associated with cryptographic keys are as follows:

User impersonation attack It describes the attacker to record the message transmission between the real-time entities.

Privileged-insider attack It defines the legitimate user of the server that could explore privileged-insider to receive secret credentials of the recorded users. It may exploit the registration phase of an authentication mechanism to misuse its credentials. Therefore, a standard user authentication mechanism is recommended to protect IoT services (Gope et al. 2018a, b).

Node capture attack It is one of the frequent attacks in the IoT environments where the devices are physically not protected. Thus, there can be a possibility of physical capturing of the devices by adversaries. Therefore, an adversary can use the refined information stored in the captured devices to compromise communication (Jiang et al. 2017).

Reply attack It is a kind of retransmission attack which can process the system information, including storage and re-transmission, without any proper authentication (Cahyadi et al. 2021).

Password guessing It is an attack against web applications and servers to exploit key functions such as letters, numbers, and symbols to discover a correct combination. Guessing attacks are generally categorized into two types: Brute force attacks and Dictionary attacks to gain system authentication (Gope and Sikdar 2018).

Brute-force attack It may try to exploit each possible code, combination, or password until it finds a correct one (Newaz et al. 2020).

Dictionary attack It may generate or utilize a dictionary of common phrases to identify the protected password (Lee et al. 2019).

Smartcard lost/fraud attack In this attack, an adversary can initiate off-line password guessing to acquire a legitimate user's smartcard (Yu et al. 2019).

False data injection In this attack, an attacker can inject falsified data instead of actual data using the captured node to transmit fake data to IoT applications. Upon receiving erroneous data, an affected IoT "application" could yield malicious commands to execute erroneous services resulting in the degradation of IoT systems (Das et al. 2016).

Spoofing attack It can make an adversary impersonate the other device or user to launch attacks against the network hosts to steal information or inject malware and bypass controls. Moreover, it may mislead the communication from unauthorized sources to legitimate ones (David et al. 2017).

Sensor-node impersonation attack In this attack, a malicious node can exist between legitimate nodes in the same network but not in direct range, known as an invisible node. This node can impersonate other existing nodes to perform malicious activities (Deebak et al. 2021).

Session key verification/disclosure attack It may initiate an attacker to capture the user session to execute legal access on the server-side using the same session key identity (Jurcut et al. 2020).

Man-in-the-middle attack In this attack, the vulnerabilities such as Denial of Service and Man-In-The-Browser to listen to data traffic, which allows attackers to intercept the confidential data (Phan 2008; Hernandez-Castro et al. 2008).

Stolen verifier attack In real-time applications, an attacker may infer the present and previous session information to verify the legal information from the server. Moreover, the authenticated servers store the verified passwords to derive useful information (Sharma et al. 2019).

Jamming attack In this attack, an adversary continuously monitors a wireless communication channel to manage the signaling frequency receiving from the sender side through the knowledge of the destination node.

DoS This attack may cause the entire network or system to stop authorized users from accessing the computational resources. Also, the network layer may jam the transmitting radio signals with the help of fake nodes to affect the transmission of data between connected nodes (Sharma et al. 2017).

Distributed DoS This attack has the ability to make the resources unavailable to the intended users in a large-scale

IoT system which may temporarily disrupt the network connectivity to the authorized server (Wang et al. 2021).

Privileged insider attack In this attack, an attacker performs malicious activities on the network or the entire system. In addition, it may drive the security elements, including stealing sensitive information, passing malware, and injecting viruses to crash the entire network or system (Banoth et al. 2021).

Mass node authentication This attack could affect entire system performance involving the process of device authentication in the IoT environment (Ghazal 2021).

Desynchronization attack In this attack, an adversary tries to prevent the target node from server access. In addition, the primary goal is to diverge the integrity and synchronization of saved information in the IoT device such as chip, card, and tag to block the data communication between the legal entities (Habibzadeh et al. 2019).

Side-channel attack It can rely on encryption devices that use an electronic chip to store confidential information. Also, it can store cryptographic information along with "execution time," "battery usage" and "electromagnetic intervention" created by IoT physical devices using encryption procedures. These storage data can obtain secret keys utilized throughout the encryption process (Hernandez-Castro et al. 2010).

Hello Flood attack The primary objective of this attack is to overload the capacity of physical nodes in the connected network system. It sends "Hello" request packets by a Sybil node to impact every legitimate node in the whole system. It could affect all the nodes at the same level that lead to heavy traffic in the specific network (Dora and Nemoga 2021).

Routing attacks This is the most elementary attack in the network layer; however, it could also happen in the perceptron layer to cause a routing loop, which may eventually produce a deficiency or expansion of routing paths to increase the "end-to-end" delay and error messages (Fan et al. 2016, 2017; Chan and Zhou 2014).

Wormhole attack In this attack, an adversary acquires packets from one side of the network, and tunnels form the other side of the network. As a result, it may utilize some strategic approach to listen to network activities or to record the wireless media (Chatterjee et al. 2022).

Blackhole attack In this attack, an adversary overhears the requesting data packets over dynamic routing protocols to falsify the replied data packet (Chatterjee et al. 2022).

Sinkhole attack In this attack, an adversary may advertise a fake routing table to forge the legal identity. It could attract network traffic to launch a selective forwarding attack to compromise or to alter the routing information of the network (Chatterjee et al. 2022).

Fake/sybil node attack It is an attack that deploys fake identities to utilize counterfeit nodes. By enabling the malicious nodes, the entire system might corrupt the neighboring nodes to receive unauthorized data from authentic nodes. Moreover, it may lead to consuming more network resources in terms of computing, battery, and security services to the entire system (Safkhani and Bagheri 2016). Table 3 shows various authentication and key agreement mechanisms with potential key agreement properties.

Table 3 Comparison of various authentication schemes with key agreement properties

Published papers	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	P12	P13	P14	P15	P16	P17	P18	P19	P20
Reddy et al. (2018)	✓	✓	✖	✓	✓	✓	✓	✓	✓	✖	✓	✖	✖	✖	✖	✖	✖	✓	✖	✖
Gope et al. (2018a, b)	✖	✓	✖	✖	✖	✓	✖	✖	✖	✖	✖	✖	✖	✖	✓	✖	✓	✖	✖	✖
Jiang et a. (2017)	✓	✓	✓	✖	✖	✓	✖	✓	✓	✖	✓	✖	✖	✖	✖	✖	✖	✖	✖	✓
Gope and Sikdar (2018)	✖	✓	✖	✖	✖	✓	✓	✓	✖	✖	✖	✖	✓	✖	✖	✖	✖	✓	✖	✖
Newaz et al. (2020)	✓	✓	✓	✓	✖	✓	✖	✓	✖	✓	✖	✖	✖	✖	✓	✓	✖	✖	✓	✖
Lee et al. (2017)	✓	✓	✓	✓	✖	✓	✖	✓	✖	✓	✖	✖	✖	✓	✖	✖	✖	✓	✖	✖
Yu et al. (2019)	✓	✓	✓	✖	✖	✓	✓	✓	✖	✖	✖	✓	✖	✖	✖	✖	✖	✖	✖	✖
Das et al. (2016)	✓	✓	✖	✓	✓	✓	✓	✓	✓	✓	✓	✖	✖	✓	✓	✖	✖	✖	✓	✖
David (2017)	✖	✓	✖	✓	✖	✓	✖	✓	✖	✓	✓	✖	✖	✖	✓	✖	✖	✓	✖	✓
Deebak et al. (2021)	✖	✓	✓	✓	✖	✓	✖	✖	✓	✖	✓	✖	✖	✖	✓	✓	✖	✖	✖	✓
Jurcut et al. (2020)	✓	✓	✓	✓	✓	✓	✖	✓	✓	✖	✖	✖	✖	✖	✖	✖	✖	✖	✓	✓
Sharma and Kalra (2019)	✓	✓	✓	✓	✖	✓	✖	✓	✓	✖	✖	✓	✖	✓	✓	✓	✖	✖	✖	✓
Sharma and Kalra (2017)	✓	✓	✓	✓	✖	✓	✖	✖	✓	✖	✖	✖	✖	✓	✓	✖	✖	✖	✖	✖

P1: reply attack; P2: user anonymity and untraceability; P3: smart card lost/revocation attack; P4: offline/online password guessing/detection attack; P5: identity verification attack; P6: mutual authentication; P7: sensor-node impersonation attack; P8: user key impersonation attack; P9: privileged-insider attack; P10: MITM attack; P11: stolen verifier attack; P12: session key disclosure; P13: smart device security; P14: server spoofing attack; P15: forward secrecy; P16: user/gateway forgery attack; P17: secure localization; P18: de-synchronization; P19: DoS/DDoS; P20: secure key agreement; ✓: yes; ✖: no

3.4 Security perspectives in smart cities/industries

Of late, smart cities and industries have emerged various key promising technologies, including sensing, localization, and intelligent connectivity, smart computing, and wireless communication technologies. Smart cities comprise several traditional IT infrastructures, namely fiber-optic cables, wireless network hotspots, remote information systems, and other related physical systems. Moreover, the infrastructure allows IoT-enabled components such as sensors, end-point physical devices, user devices to connect with additional layers of the IoT infrastructure.

The emerging technologies have essential components such as embedded systems, wireless sensor networks, big data analytics, and device connectivity to build smart cities' development; however, it addresses several security potential risks. The security risks may lead to an impact on various resources, including power outage, and water pollution, traffic congestion, financial/economic damage, and loss of sensitive data such as government data and medical data. Li et al. (2017) identified security and trustworthiness as weak-link for smart cities. The addressed issues are crucial to the successful operations of smart city applications. A detailed comparison of recent survey articles and their new findings is shown in Table 4.

However, possible attacks could generate distorted data. As a result, the misrepresented reports malfunctioning on traffic or smart grid could cause incompatible controls of the system. It could also lead to life-threatening consequences, including car accidents, disparate water treatment, and inappropriate traffic control. Moreover, apart from these issues, IoT environments could deal with various security challenges, including potential vulnerabilities, error-prone communication, and transmission rate. It majorly relies on RFID and network topologies. More than 212 billion devices were installed based on the IoT technology that opens doors to translate into 212 billion potential attacks. Subsequently, IoT devices are highly prone to security attacks and thus can be compromised in many ways.

For instance, being connected to a botnet makes it malignant by a worm to penetrate private networks and control systems. In addition, physical devices often deploy necessary security requirements and default passwords to address the security weaknesses of various authentication schemes. Subsequently, the national crime agency (NCA) identifies numerous security problems concerning various manufacturers and IoT applications (Lloyd et al. 2021). IoT environments highly address complex security solutions such as botnets, including Mirai, Persirai, and Brickerbot (Watson 2017; Masters 2020; Biggs 2020). Therefore, this article considers the major issues such as authentication, auditing, and context-aware to exhibit promising solutions.

4 Challenges in smart IoT: device security, authentication and key management protocols, privacy-preserving

This section discusses the challenges in smart IoT, including device security, a key management protocol, and privacy-preserving to analyze the security and privacy disparities.

4.1 Device security

A secured physical device is difficult to apply privacy-preserving using the existing Internet model. The issues of IoT device constraints and their traditional cryptographic primitive challenge with conventional Internet to protect the environmental conditions (Trappe et al. 2015). The majority of computing devices arise three basic limitations such as battery life, computing power, and access control to prevent potential threats.

Battery life Most IoT devices have limited computation power for the design of system security, and heavyweight functionalities may lead to draining the battery resources. The researchers have recommended three possible strategies to overcome the security weaknesses. The first one uses the slightest security properties on the device to adopt a risk-driven approach. However, it cannot be recommended to deal with sensitive information like healthcare, military, and government. The second recommendation considers charging/battery capacity to assess the characteristics of device security as it is to be the tiny size. As a result, extra space can be provided to offer backup power or to extend additional battery backup to deal with a highly challenging task. Lastly, the third recommendation produces energies from natural resources, including heat, light, wind, and vibration, to upgrade the hardware and monetary costs (Alaba et al. 2017).

Computing power Since IoT devices are resource-constrained, traditional cryptographic solutions are not suitable because they have inadequate memory capacity. Moreover, the devices cannot offer better computation and storage requirements to perform advanced encryption. As a result, several research works have been proposed to implement the security methods, which use resource-constrained devices to explore key functionalities of the computing devices. For instance, physical layer authentication applies signal processing to enable secure authentication at the receiver's side that authenticates the communication parties to achieve system security and reliable connectivity. Moreover, an antenna has a specified analog characteristic to enable an efficient encode analog information to resolve the issue of reproducibility. The nuance serves as a unique key as it cannot be predicted or controlled during the phase of manufacturing. The device authentication considers radio signals to minimize

Table 4 Comparing recent survey articles and new findings

Existing papers	Title	Objective	New findings
Sengupta et al. (2020)	A Survey on attacks, security issues, and solutions for IoT environments	Classify attacks based on objectives of vulnerabilities Countermeasures to relevant security threats	A case study on two essential IIoT applications is highlighted Blockchain-based solutions over cloud-centered applications
Lohachab et al. (2020)	Survey on salient cryptographic mechanisms for secure communication	In-depth analysis of post-quantum on the role of cryptographic techniques for IoT environments	Open research challenges and future directions IoT layered architecture, its associated challenges, and counteractants
Malhi et al. (2020)	Survey on the security of vehicular ad-hoc networks	Eminent safety solutions to address the security issues of VANETs Discuss future research reflections on the evolutionary growth of security attacks	Attacks, security solutions Comparative analysis of cryptographic mechanisms Trust management schemes based on IDS
El-hajj et al. (2019)	Survey of IoT authentication schemes	Up to date review of authentication schemes in IoT Identifying the number of requirements and open issues	Multi-criteria classification to evaluate the strengths and weaknesses of each authentication protocol
Habibzadeh et al. (2019)	Study on applications and data planes for smart city development	Provide a multi-faced survey of machine intelligence	Provides a detailed summary of the application plane Sensing plane Communication plane Security and data plane
Ometov et al. (2019)	MFA for securing advanced IoT applications	Review of current research issues and counteractants for user authentication with the Advanced IoT (A-IoT) ecosystem	Introduced MFA for A-IoT as an alternative to existing SFA
Cui et al. (2018a, b)	Security and privacy in smart cities: challenges and opportunities	Providing the review of security and privacy issues in current smart city applications	Security properties for establishing stable and secure smart-city applications encapsulate existing protection technologies Identify future research issues
Sookhak et al. (2018)	Survey of security and privacy issues in smart cities	Provides an exhaustive survey of security and privacy challenges in smart cities	Presents the categorization of future improvements in smart cities
Habibzadeh et al. (2018)	A new challenge for smart city system design using sensing communication and security planes	Provides survey on pervasiveness and ubiquity of smart city services	Provide a concise view of smart city system architecture Challenges and state of the art approaches in each plane
Yang et al. (2017)	Survey on IoT security and privacy	Security mechanisms and architectures for authentication and access control	Provides appropriate limitations of IoT devices and specified counteractants Classification of attacks
Eckhoff and Wagner (2017)	Privacy in the smart city—applications, technologies, challenges, and solutions	Review the privacy-enhancing technologies, state-of-the-art approaches in smart cities around the world	Discusses promising future research directions in smart cities Provides a comprehensive study of privacy issues
Garcia-Font et al. (2017)	Attack classification schema for WSNs	Intrusion detection framework and an attack classification	Demonstrated with a proof of concept for utilizing classification schema

energy overhead and to meet the security requirements of mobile IoT (Jan et al. 2014).

Access control It may assure that the IoT devices cannot access the backbone technology to guarantee the information security to withstand various security vulnerabilities. The primary goal of access control is to monitor the access of resources efficiently and protect against the unauthorized flow of information. In the IoT environments, the data can be transmitted continuously and shares data between people and things. As the IoT domain is vulnerable to various attacks, including offline password guessing attacks and node capture attacks, it may easily lead to hardware failures (Jurcut et al. 2020). However, the deployed nodes may not always be legitimate as the malicious one forcibly operates the system entries to perform cybercrimes (Lohachab et al. 2020). As a result, it is a very complicated task to discriminate against the malicious node from the valid nodes in the specified network. Therefore, to deploy a new computing device, a standard access control mechanism is preferred. It may block malicious nodes to prevent unauthorized change in the IoT environment. Moreover, access control plays a vital role in consisting of authentication and key establishment mechanisms to maximize device protection against malware attacks. The authentication mechanism using "certificateless" or "certificate-based" issues trusted organizations to generate valid private keys.

4.2 Authentication and key management protocols

It is one of the essential security services for Today's IoT environments. A set of provisions including confidentiality and integrity is maintained to offer extensible communication. It uses an interoperable message format to simplify the process of data encryption to the key management server. The smart city applications initialize a trusted authority to manage massive connectivity, which configures confidential data into the memory-chip naming as key rings. For instance, two sensors/devices try to establish secure communication that uses a pairwise key configuration to preload their keyrings (Newaz et al. 2020). Their mechanism is based on the deployment of applications with common security concerns such as probabilistic and deterministic Jiang et al. (2017) proposed a lightweight 3FA and key agreement protocol based on the Rabin cryptosystem that enables computational asymmetry. Their scheme proves that it can withstand various known attacks to protect the application services.

Similarly, Challa et al. (2017) presented a secure signature-based authentication and key agreement mechanism for future IoT applications. This mechanism uses formal analysis such as BAN-Logic and AVISPA to verify security features and to prevent a potential attack such as denial of service (DoS). Moreover, this proposed mechanism achieves better security features and minimizes the computation and communication cost compared with other related schemes. Deebak et al. (2021) devised a seamless key establishment framework for mobile-sink in IoT-based cloud environments. This proposed mechanism utilizes bilinear pairing and ECC cryptosystem to meet the standard security properties such as data confidentiality, session key management, mutual authentication, user anonymity, and key impersonation. Moreover, it utilizes seamless connectivity between the sensor components to minimize the computation and communication costs of the communication system. Sanchez-Gomez et al. (2020) presented a novel authentication and key management mechanism in "narrowband" IoT and 5G. In this mechanism, two extensible authentication protocol (EAP) protocols, such as PANATIKI and LO-CoAP-EAP, were adopted to enable secondary authentication and key management mechanisms.

Amin and Biswas (2016) and Wu et al. (2017) addressed various security vulnerabilities, including sensor node capture attacks, user, sensor and gateway forgery attacks, and offline guessing attacks. They proposed a novel authentication scheme using "multi-gateway" in IoT deployments to resolve the key issues. Secure authentication plays an essential measure to prevent unauthorized access to the device or system. With the rapid advancement of Internet access and smart civilization in smart cities/industries, the validation and verification of the user are based on source identity. However, it cannot withstand potential attacks such as passive and active (Mohsin et al. 2017; Danny 2017). Most real-time applications use single-factor-authentication (SFA) mechanisms to offer continuous and passwordless authentication. Most real-time applications use the credentials such as username and password or personal identification number (PIN) to confirm user identification. However, this strategy has the weakest levels of security to transfer the secret password over a public network as the adversary can easily compromise the users' private information.

Moreover, unauthorized users may acquire service access to penetrate dictionaries and social engineering attacks (Heartfield and Loukas 2015). Most researchers deliberately proposed two-factor authentication (2FA) using the combination of different key entities such as key-card, smartphone, one-time password, and an access card with a photo to prevent the security issues of SFA. Few researchers proposed multi-factor authentication (MFA), known as three-factor authentication (3FA), to provide an enhanced level of safety and security.

Moreover, the MFA is based on a combination of SFA and 2FA with biometrics which recognizes the users based on their behavioral and biological features. As a result, the strategies such as SFA, 2FA, 3FA, and MFA can protect smart devices and other related complex systems from unauthorized access. Figure 6 depicts the detailed overview of authentication mechanisms from SFA to MFA. MFA plays

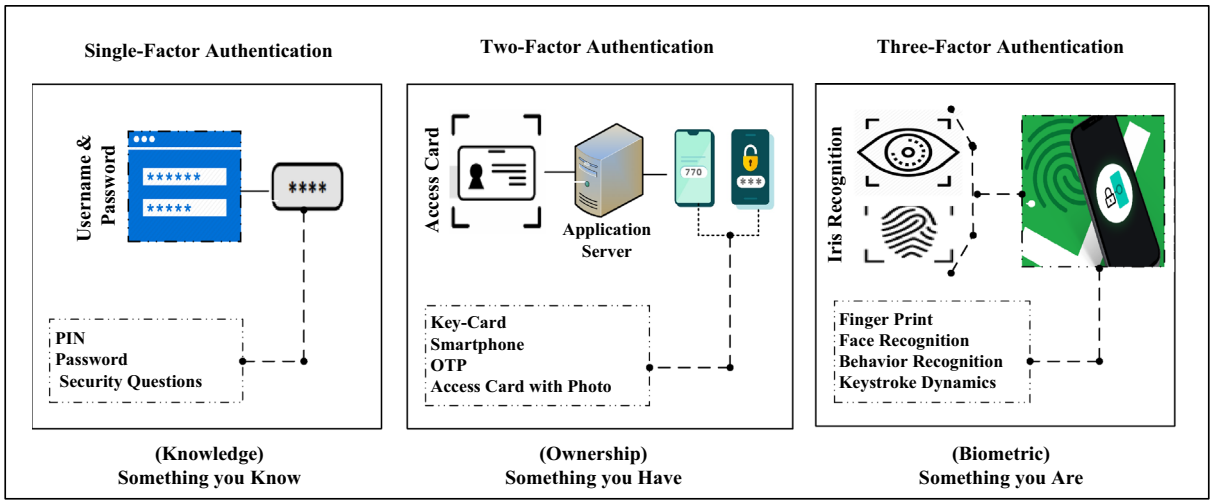

Fig. 6 Authentication methods from single-factor to multi-factor

a crucial role in verifying device identities and user information. It has dedicated infrastructure and network connectivity to validate interconnected IoT devices, such as smartphones, wearable devices, and other related digital devices (Ometov et al. 2018). The applications of MFA are categorized as follows:

Commercial applications It can include account login, ATM, e-commerce, and physical access control to limit the service access to mission-critical systems.

Government applications It can prefer government identities such as passports, driving licenses, border security control, and social security to avail different centralized services.

Forensic applications It may be useful to investigate criminal cases such as missing children, kidnap, assault, rape, and robbery to collect and preserve the potential pieces of evidence.

In IoT environments, during the identification process, node authentication schemes can avoid vicious users from entering the connected network via the sensing/perceptron layer. Liu et al. (2019) categorized the authentication protocols which are as follows:

Heavyweight authentication functions It can incorporate the traditional cryptographic suite, cryptographic hash functions, and public and private key cryptosystems to guarantee key freshness.

Middleweight authentication functions It may utilize the cryptography primitives such as ciphers, arbitrary length hash, digital signature, and pseudo-random number generator to build high-level security protocols.

Lightweight authentication functions It can prefer lightweight functions, including cyclic redundancy checks (CRC) and a pseudo-random number generator to prioritize the consumption of computing resources.

"Ultralightweight" authentication functions It can incorporate bitwise logical functions to improve the protocol's confidentiality rate, such as extremely good privacy (EGP).

The process of authentication includes user credentials to authorize application services (Clarke 1994). Generally, an identifier has three factors such as something you know, you have, and you are to fulfill the five features: (1) universality, (2) uniqueness, (3) permanence, (4) storage, and simplicity (Hu et al. 2013). Today, most authentication protocols serve as key identifiers and verifiers to offer the security properties such as mutual authentication and session key agreement. For instance, adversaries frequently counterfeit authorized readers to read the tag information and attempt for illegal concerns in the RFID system. As a result, a property of mutual authentication is highly recommended to achieve the security of the RFID system. Similarly, most IoT devices demand mutual authentication mechanisms to protect the physical devices from known attackers.

However, the authentication scheme is based on the requirements of IoT devices. Therefore, most authentication schemes utilize symmetric, asymmetric, and ECC encryption to minimize the computation and communication costs. Xu et al. (2019) designed an RFID authentication protocol using ECC encryption that efficiently handles mutual authentication to improve security. Authentication and key agreement (AKA) is identified to be a suitable security mechanism for smart IoT applications (Wu et al. 2009). It can provide data security to the millions of intelligent devices to offer reliable data access and sharing. The AKA mechanism is mainly considered in device-to-device, a device to the gateway, and a gateway to the server to protect network traffic (Zhao et al. 2017). Consequently, IoT devices have a provision of user privacy and protection to offer an excellent benefit for several smart applications.

However, IoT devices are still demanding to implement a robust security mechanism whereby the devices can prevent several potential risks for massive connectivity of insecure applications connected over the Internet. Therefore, conventional authentication systems cannot be applied to improve the confidence level of smart IoT environments.

Mutual authentication plays a vital role in Today's IoT applications. For example, smart homes, smart parking systems, smart vehicular systems, and other related wearable devices are significant contributions to smart cities. Various lightweight authentication schemes address the importance of mutual authentication between the devices and systems. Miettinen et al. (2018) devised a novel context-based mutual authentication scheme for physical IoT devices. This scheme uses context analytics and risk assessment to ensure that it has actual availability of transactions compared with other feasible solutions because it does not require password input.

Moreover, a one-time password (OTP) is another secure authentication mechanism to provide a standard solution for IoT and smart cities. Hammi et al. (2020) extended the principles of OTP to devise a novel mechanism of OTP using ECC and Isogeny. It can assure that this mechanism can offer better security efficiency than other techniques such as code-based OTP and time-based OTP. It can be defined as a two-way authentication process over secure communication to authenticate service connectivity. It may gain device access to authorize remote services between the real-time entities. Moreover, it can establish a secure session key between the entities to secure the device's connectivity.

4.2.1 Lightweight authentication

IoT devices use advanced RISC machine (ARM) architectures with low power consumption devices for the applications of a smart city. It comprises of simple CPU structure, less storage capacity, and smaller computing power. As a result, the traditional encryption mechanisms cannot assure better security efficiencies for emerging IoT applications. IoT systems demand lightweight authentication mechanisms to establish secure communication among M2M and H2M devices. The lightweight encryption techniques are highly utilized in resource-constrained devices such as RFID devices, medical devices, and sensors. At present, RFID is emerging in several smart IoT applications to offer machinery automation and object identification. It consists of two parts, namely RFID tags and RFID readers, to locate the intelligent sensors and to identify the real-time objects, including shipment verification and asset tracking. Tags are commonly attached to the device and correspondingly store information inventory information. The reader collects the information via a wireless communication channel to locate and identify the tagged items through a dedicated server, as depicted in Fig. 7.

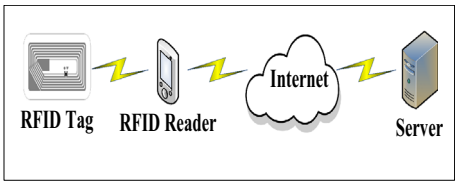

Fig.7 Communication between RFID Systems

Several cryptographic schemes have been designed to fulfill some quality services such as processing power and memory resources. However, the existing schemes could not offer better computing resources to meet the standard demands of smart IoT environments. As a result, a lightweight authentication scheme is preferred to minimize the computation and storage overhead. Few authentication schemes are specific to real-time scenarios such as IoT-based Sensor Networks, Cloud, and Fog-Edge computing environments (Deebak et al. 2021). It is worthy to note that emerging cloud computing cannot meet the selection criteria, such as latency, context awareness, and mobility, to design mission-critical IoT applications. To fulfill the design requirements, various emerging technologies have been recommended, such as mobile cloud computing, mobile edge computing, and fog computing (Roman et al. 2018). Gope et al. (2018a, b) developed a lightweight RFID mutual authentication protocol for the distributed infrastructure of smart cities, which highlights technical risks and execution strategies between the tag and reader to offer a reliable analysis. Radu and Garcia (2016) devised a lightweight authentication protocol for vehicle controller LANs. Their scheme adopts a subscribed pattern to enable the property of mutual authentication between the controller units of the vehicular systems. Liu et al. (2016) implemented a cloud-based lightweight mutual authentication for wearable devices.

This mechanism applies PUFs and lightweight passwords to accomplish mutual authentication between IoT applications and wearable devices. Xu et al. (2018) devised a lightweight authentication mechanism for RFID systems using a physical unclonable function (PUF). Their mechanism primarily comprises three essential functionalities, including tag recognition, verification, and updation. Initially, the tag reader recognizes the inventory items, whereas the second utilizes the verification phase to identify the items upon the execution of key authentication between the tag and reader. The third functionality uses the secret-key update phase to complete the system verification. Gope et al. (2018a, b) devised a robust, lightweight authentication scheme based on PUF to verify traditional RFID systems. This system uses lightweight authentication to support device anonymity and proper mutual authentication. Also, it improved the existing mechanism to address the issue of noisy PUF environments. Porambage et al. (2014) proposed a pervasive

lightweight authentication and key agreement mechanism for resource-constrained distributed IoT applications. Their proposed mechanism comprises (1) the registration phase intends to acquire personal login details to the devices and end-users; and (2) the authentication and key establishment obtains mutual authentication and session key agreement. Table 5 summarizes the key metrics of existing authentication schemes.

Also, this mechanism shows that the end-users can directly authenticate the service connectivity to the sensor nodes. It may gain network access to perform data collection, processing, and analysis. Moreover, it can utilize distributed IoT applications to offer lightweight authentication and high resource-constrained devices. In smart cities, the operation of the smart grid plays a vital role in providing intelligent solutions over traditional power grids. However, security vulnerabilities such as natural disasters, cyber-attacks, and distributed denial of service are yet to address in smart grids. In smart cities, the domestic residence is enabled with a smart meter to mobilize electricity spending over a specified time. Moreover, smart metering in IoT sends the data over a secure communication channel to generate the billings, which can be sent to the consumer to regulate digital monitoring and bidirectional communication. Li et al. (2013) devised a lightweight mutual authentication scheme using the Merkle-hash tree to provide efficient communication and to minimize the computational overheads. Nicanfar et al. (2011) designed a robust, secure authentication and key management scheme to authenticate HAN with a smart grid utility network. Li et al. (2012) developed a robust and effective authentication mechanism to analyze power consumption data in NAN with fault tolerance. Gupta et al. (2019) introduced a new authentication protocol to communicate with IoT using "XOR" and a one-way hash function. This mechanism demonstrated that it can resist several potential security attacks and provide privacy-preserving between the real-time entities. Social-Internet of things (S-IoT) can strengthen the behavioral relationship between the computing devices to offer efficient resource utilization. Sharma et al. (2017) proposed a novel mechanism considering trust and privacy-preserving solutions for S-IoT using edge-crowd integration-based fission computing. Xu et al. (2019) introduced an edge computing-based computation offloading method to address the challenges of privacy hassles of computation offloading to the ECD in IoV. Their mechanism is based on the edge computing offload (ECO) method to provide privacy preservation to Internet-connected vehicles. Luo et al. (2018) devised a secure framework for IoT-based healthcare systems with the feature of privacy-preserving. It can perform secret sharing and repairing data loss/compromising using

Table 5 Assessing the key metrics of existing authentication schemes

References	PE1	PE2	PE3	PE4	PE5	PE6	PE7	PE8	PE9	PE10
Gope et al. (2018a, b)	✖	✖	✖	✓	✓	✓	✓	✓	✓	✓
Montori et al. (2017)	✖	✓	✖	✓	✓	✓	✓	✓	✓	✖
Distefano et al. (2015)	✓	✓	✓	✖	✓	✓	✓	✓	✓	✓
Zeng et al. (2017)	✖	✖	✖	✓	✓	✖	✖	✓	✖	✖
Urbieta et al. (2017)	✖	✖	✖	✖	✓	✖	✖	✖	✖	✖
Seo et al. (2016)	✖	✓	✖	✓	✓	✓	✓	✓	✖	✖
Li et al. (2014)	✖	✖	✖	✓	✓	✓	✖	✖	✖	✖
Lee et al. (2017)	✖	✖	✖	✓	✓	✓	✓	✓	✖	✖
Akbar et al. (2018)	✓	✖	✓	✖	✖	✖	✖	✓	✖	✖
Sun and Ansari (2017)	✖	✖	✖	✖	✓	✓	✓	✖	✖	✖
Chai et al. (2015)	✓	✓	✓	✖	✖	✖	✓	✖	✓	✓
Jiang et al. (2021)	✖	✖	✖	✓	✓	✓	✓	✓	✖	✖
Naranjo et al. (2019)	✖	✖	✓	✖	✓	✓	✓	✓	✖	✖
Ghahramani et al. (2020)	✖	✖	✖	✖	✓	✓	✓	✓	✓	✖
Sharma et al. (2019)	✓	✖	✖	✖	✓	✓	✓	✖	✓	✖
Sharma et al. (2017)	✖	✖	✖	✖	✓	✖	✖	✓	✓	✓
Merabet et al. (2020)	✖	✖	✖	✖	✓	✓	✓	✓	✓	✖
Haseeb et al. (2020)	✓	✓	✓	✖	✖	✓	✓	✓	✓	✖
Robert et al. (2017)	✓	✓	✓	✖	✖	✖	✖	✖	✖	✖
Robert et al. (2017)	✓	✓	✓	✖	✖	✖	✖	✓	✖	✖
Sanchez-Gomez et al. (2020)	✖	✓	✓	✖	✖	✖	✖	✖	✓	✖

PE1: reliability; PE2: availability; PE3: scalability; PE4: cost; PE5: execution time; PE6: latency: PE7: power consumption; PE8: efficiency; PE9: security; PE10: privacy ✓: yes; ✖: no

Slepian-Wolf-Coding-based Secret Sharing (SWSSS). Ming and Cheng (2019) presented a novel certificateless conditional privacy-preserving authentication scheme which is based on a certificateless cryptosystem using ECC to secure vehicular communications in VANET. As a result, this mechanism applies bilinear pairing operation (Nikravan and Reza 2020) and map-to-point hash operations to improve performance efficiency.

4.2.2 Ultralightweight authentication

This authentication strategy uses only a bitwise logical operator and ultralightweight non-triangular primitives. Generally, it involves simple bitwise logical operators, including XOR, AND, OR, Rot, to design the security protocols. However, few authentication mechanisms are vulnerable to various known malicious attacks. Mujahid et al. (2020) reviewed ultralightweight mutual authentication protocols to secure restricted environments such as healthcare, data analytics, and agriculture. Also, they showed that the advanced ultralightweight authentication mechanisms are susceptible to desynchronization and full disclosure attacks. However, several researchers utilized non-triangular primitives such as permutation and recursive hash to build a lightweight computer system. Unfortunately, the existing mechanisms address several security vulnerabilities (Phan 2008; Hernandez-Castro et al. 2008; Safkhani and Bagheri 2016; Sun et al. 2009; Mujahid et al. 2020; Khalid et al. 2019; Mujahid et al. 2018) to realize the potential threats such as buffer overflow, missing data encryption, authorization, and authentication. As a result, the researchers recommend a suitable strategy to improve the design of ultralightweight authentication protocols to avoid active and passive attacks. The recommendations strategies include ultralightweight random number generators, comprehensive security analysis model, non-triangular primitives, and messages design to offer sensitive features such as reproduction, periodicity, and randomness.

Of late, various pseudo-random generator-based ultralightweight authentication mechanisms have been proposed for mission-critical IoT applications Hernandez-Castro et al. (2010) implemented secure lightweight and ultralightweight mutual authentication schemes for RFID systems use cache for IoT environments in 5G networks. Their mechanism enables content caching to the reader to store the secret keys that use system tags to minimize lower the computation cost and to improve the security efficiency. Fan et al. (2017) devised an ultralightweight mutual authentication mechanism with pseudonyms for IoT-NFC-based applications and 5G networks. This mechanism applies lightweight shift and XOR bitwise operations to match the execution and storage capacity of NFC tags. Moreover, it uses pseudonyms instead of real identity to provide the feature of device anonymity.

4.2.3 Two-factor authentication

In smart cities, every car needs to be connected with IoT devices to enable vehicular networks. The connected devices offer various services to the cooperative networks, such as traffic information, road safety, time management, localization, and energy supplies. Nowadays, electric vehicles are challenging to design a suitable authentication framework the advanced vehicular communication systems. Chan et al. (2016) devised a 2FA mechanism for electric vehicles that use distant locations as a unique context feature to track the connected vehicles. Generally, the vehicles connect to the trusted authority using VANET to offer an intelligent charging system using a charging cable. Therefore, it demands the physical connectivity of the device to verify the identities of the vehicular communications.

Lalli and Graphy (2017) devised a prediction-based authentication (PBA) mechanism for VANETs. This mechanism can protect the vehicular system from DoS attacks and also withstands packet loss. They utilized the Merkle hash tree (MHT) to verify self-organized MAC storage (Roberts et al. 2017) instantly. To authenticate a secret message between the vehicles, this mechanism applies ECDSA and TESLA mechanisms which deliver a robust and efficient authentication (Rekik et al. 2017). Yu et al. (2018) devised a secure mutual authentication mechanism for VANET. This mechanism uses a CHAP scheme to achieve authentication and authorization to enable vehicle-to-vehicle charging through converter cable. Moreover, the improved two-way authentication and key agreement mechanism allow a better verification process for VANET. This mechanism allows the vehicles to achieve a system efficiency to protect vehicle privacy. It does not invoke a phase of re-verification when the vehicle transits from one coverage location to another location.

Lee et al. (2019) designed a 2FA and key agreement scheme using automotive sensory systems in vehicular communications. Their mechanism proves that it can withstand various attacks, such as user impersonation, replay, trace, and smartcard stolen to improve security efficiencies. Also, their protocol utilizes dynamic values to achieve mutual authentication and user anonymity. Figure 8 shows an overview of the vehicular communication system. Sharma et al. (2019) presented a remote user authentication for e-governance. Their mechanism uses lightweight cryptographic operators to minimize the computation overheads. Moreover, it utilizes a strategy of formal verification to confirm the standard requirements of smart cities. Sharma et al. (2017) proposed a robust, lightweight authentication and key agreement mechanism for e-governance applications (Alotaibi

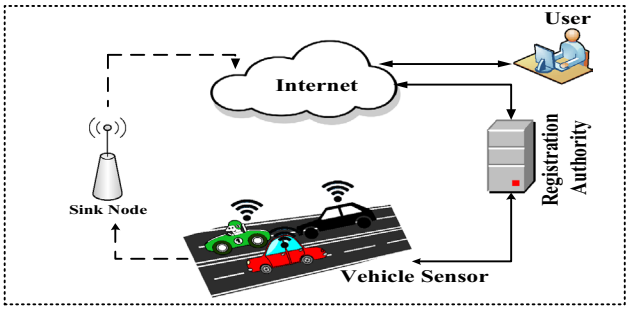

Fig. 8 Overview of vehicular communication system

2018). This strategy prefers hashing operators and exclusive-or to achieve desirable attributes such as key freshness and user anonymity.

Haseeb et al. (2020) developed a cloud-based authentication framework for intelligent IoT. This architecture uses unsupervised machine learning and weighted-based centroids to achieve boundless storage and consistent delivery. Also, it uses a network simulator known as NS-3 to examine the communication metrics such as network lifetime, energy consumption, and packet dropping ratio. Merabet et al. (2020) developed two communication modules such as machine-to-machine and machine-to-cloud, to revolutionize the connectivity of real-time objects. These modules invoke the connected objects to collect and process the potential parameters to provide a high level of security and privacy. Naranjo et al. (2019) presented a multi-tier architecture for the management of the fog computing environment. This architecture uses a resource allocation model to improve the energy consumption ratio and to meet the service qualities of the Internet of everything. Ghahramani et al. (2020) developed a biometric-based secure authentication for mobility networks. This mechanism tries to promote the quality of life and the utilization of natural resources in smart cities. Moreover, it uses a BAN logic analysis to analyze the security properties such as proper mutual authentication and session key agreement. Table 6 summarizes the key assessments of various recent research works in smart IoT environments.

4.2.4 Three-factor authentication and context-aware services

In smart cities, IoT supports people to communicate and securely acquire mobile services quickly. However, various key issues like resource-constrained device security, scalability, impenetrable problems of security and privacy, and malicious attacks are cautiously chosen to analyze the extensive growth of IoT services in smart cities users. The IoT services prefer an authentic gateway to process massive amounts of information to offer reliable and secure communication between the real-time entities. It is worthy to note that users and gateways demand proper mutual authentication via a control server to provide secure communication and to minimize computation costs. Yu et al. (2018) devised a secure 3FA mechanism using a multi-gateway for IoT environments. It can ensure to withstand various known attacks such as spoofing, user impersonation, offline password guessing, gateway impersonation, session key disclosure attacks to improve security efficiencies. Das et al. (2016) proposed a robust and lightweight 3FA mechanism for cloud-enabled IoT domains. This mechanism can resolve the security vulnerabilities of various existing protocols to improve the security level of the sensory systems.

Their mechanism achieves mutual authentication and user anonymity to withstand potential attacks, such as session key disclosure and relay attack, impersonation attack, and gateway spoofing attacks. Mohsin et al. (2017) devised an efficient multi gateway-based 3FA and key agreement mechanism for hierarchical WSNs in a smart city environment. This mechanism assure that it can resist node capture attacks to prevent network and data hazards. In the past few years, numerous authentication mechanisms have been proposed for IoT-based e-healthcare systems (Mohsin et al. 2017; Ostad-Sharif et al. 2019; Jiang et al. 2021; Far et al. 2021; Chen and Chen 2021). The main objective is to provide enough security level against the potential vulnerabilities. However, few authentication mechanisms cannot withstand various known attacks, including local password change attacks, forward secrecy, user anonymity, gateway spoofing attack, and stolen smart card attacks. Wu et al. (2018a, b) proposed a secure 2FA for WMSNs using ECC with forwarding secrecy. Their mechanism uses a fuzzy commitment method to handle the biometric information. Also, they showed a fuzzy verifier and honey_list mechanisms to withstand local password verification, and mobile device lost attacks.

Ostad-Sharif et al. (2019) designed a secure, lightweight authentication for IoT-based sensory environments. This mechanism tries to achieve a better storage cost to improve the efficiency rate of the system. A formal analysis proves that this mechanism has better performance evaluation, such as computation and communication to the reliable sensor nodes. Jiang et al. (2021) introduced a secure authentication and key exchange protocol to eliminate the storage of secret information of any computing device. It applies three basic techniques such as password-based, biometric, and a physical unclonable function to offer device protection and access control. Far et al. (2021) designed a lightweight privacy-preserving authentication for sensor-based IIoT environments. This mechanism includes dynamic registration, biometric verification, and key revocation to protect the system security and data privacy. Chen and Chen (2021) proposed a secure three-factor authentication and key agreement mechanism for

Table 6 Key assessments of various recent research works in smart IoT environments

Papers	Mechanism	Purpose	Merits	Demerits	New findings
Haseeb et al. (2020)	Secure sensor cloud architecture For consistent service delivery	Smart cities Intelligent IoT systems	Boundless Storage Scalable Efficient Secure	Privacy Not evaluated Not cost-effective	SSCA Architecture
Sanchez-Gomez et al. (2020)	Authentication and key establishment for narrowband ~ IoT (NBIoT) and 5G networks	Smart agriculture monitoring	Secure High flexibility Scalability	Latency Large payload size High cost Reliability not evaluated	NBIoT Authentication and Key management mechanism
Merabet et al. (2020)	Efficient M2C and M2M authentication	Smart cities Smart healthcare applications	Secure Lightweight Efficient	Not scalable It suits 256-bit security Moderate execution time	Algorithm
Naranjo et al. (2019)	Fog enabled network architecture for Application management in IoE	Internet of everything in Smart city	Less power consumption High scalability Improved latency	Not evaluated cost parameters	FOCAN Architecture
Ghahramani et al. (2019)	The biometric-based authentication mechanism for global mobility networks (GLOMONET)	Smart cities	Secure Low latency Improved execution time Improved Efficiency	Not cost-effective Not scalable	Secure Biometric-based authentication protocol
Sharma et al. (2019)	Secure user authentication for E-Governance	Smart cities	Low latency Improved execution time Minimum response time	High cost	Multi-factor user authentication mechanism
Sharma et al. (2019)	Remote user authentication for E-Governance	smart cities	Lightweight Low latency Improved efficiency	High cost Reliability not evaluated	Mutual authentication mechanism
Gope et al. (2018a, b)	Secure localization service distributed IoT environment	Smart cities	Secure Improved efficiency Minimum response time Reasonable execution time	Privacy not considered High cost	Algorithm
Lee et al. (2018)	Probabilistic data fusion architecture for scalable heterogeneous data streams	Weather monitoring service	Works well for large scale applications Improved efficiency	High cost Response time not evaluated	Two-layered Architecture
Zeng et al. (2017)	IoT simulation for BIG data processing in cloud environment	Smart city applications using Clod storage	Works on top of CloudSim simulator Improved existing functions of CloudSim	Stream Processing not supported	"IoTSim"-simulator
Urbieta et al. (2017)	Adaptive computation offloading for IoT	Smart city offloading Applications Adaptive computing	Improving quality of Service (QoS) quality of outcome Reduce the execution time	Not scalable Not supported for a massive number of user tasks Decision modules	Framework for adaptive computation modeling
Lee et al. (2017)	QoS-aware service composition architecture based on open service gateway initiative (OSGi)	Smart homes Smart buildings	Lower resource consumption Minimum response time The efficient CPU utilization ratio	Scalability Not suitable for large-scale environments	A framework built upon OSGi Platform

Table 6 (continued)

Papers	Mechanism	Purpose	Merits	Demerits	New findings
Sun and Ansari (2017)	Dynamic resource re-caching load balancing management	Smart parking	Minimum response time Low power consumption	High cost Not applicable for large scale inputs	Algorithm
Robert et al. (2017)	Open IoT ecosystem for enhanced interoperability in smart cities	Smart cities (Brussels and Helsinki)	Interoperability High scalability	Privacy not included High cost	Smart city pilot Ecosystem together developed with "Metropole De Lyon"
Seo et al. (2016)	Context-aware infrastructure for mobile applications	M2M vehicular monitoring service	Provides high performance and low latency for mobile applications	Reliability Privacy	Context-aware Cloud Infrastructure Framework model
Chai et al. (2015)	Enhance secure mobility data management service	Smart IoT environments	Improves mobility and stability Provides high Security Improved latency	High cost Execution time and response time	Mobility management scheme
Distefano et al. (2015)	Mobile crowdsensing (MCS) management	Evaluate QoS metrics of MCS	Improving quality of service (QoS) Improving reliability, cost, Response time	Not evaluated efficiency parameters	Framework model based on stochastic pertinet
Li et al. (2014)	QoS-aware service Composition architecture	Smart buildings Smart homes	High reaction time Improved cost	Not evaluated reliability and privacy	Algorithm

the development of e-Health. It uses elliptic-curve cryptography and fuzzy extractor to improve the computation efficiency of the systems (Wang et al. 2017). Moreover, it uses the BAN logic tool to analyze the security and performance efficiency of the e-Health.

Montori et al. (2017) designed a collaborative IoT architecture for smart cities and environmental monitoring systems. This architecture uses SenSquare to deal with the classification of heterogeneous data and the management of mobile crowdsensing. Distefano et al. (2015) introduced an analytical modeling framework to evaluate the quality of crowdsensing services. It may exploit the opportunistic sensing and geolocalized data to formalize a dependency of context semantics. Zeng et al. (2017) utilized the functionalities of CloudSim to design batch-oriented IoT applications. It uses a MapReduce model to analyze the execution cost and to examine the energy-aware computation resources. Urbieta et al. (2017) adopted a framework of novel service composition to analyze user behaviors and dynamic task allocation. It uses the functionalities of semantic service-oriented architecture to integrate the system variants to meet the standard requirements of smart cities. Seo et al. (2016) integrated cloud infrastructure management and cloud-distributed data processing to design a context-aware infrastructure. It utilizes a powerful framework and ubiquitous environment to analyze and control the interoperability features of IoT systems. Li et al. (2014) constructed a multi-criteria goal programming model to integrate the properties of quality services.

It introduces a multi-population genetic algorithm not only to determine the service composition but also to analyze the constraints of scalability and performance efficiency. Lee et al. (2017) developed a novel service framework to diverse the interaction patterns, including service discovery, composition, and tracking. It has a declarative blueprint of cloud applications and service interconnections to design a composite framework that has a realistic topology to interlink the service composition of cloud computing resources. Akbar et al. (2018) presented an optimized solution using an open-source platform for large-scale IoT applications. It uses a generic interface to analyze state-of-the-art events using Bayesian networks. Sun and Ansari (2017) proposed a re-cache/re-allocate strategy to stabilize the traffic loads among the contents of computing resources. It can design a latency-aware resource re-caching to solve the problem of energy consumption and loading efficiency. Chai et al. (2015) designed an inter-domain handover scheme to examine the handover latency. Robert et al. (2017) discussed the implications of enhanced interoperability for the global IoT ecosystems. It can build an innovative framework to regulate the practices of service providers.

4.3 Privacy-preserving in smart IoT

Today, privacy protection is one of the critical concepts of security research that leads to property loss, resulting in severe causes to compromise human safety. Moreover, a massive amount of private information can be stored in the IoT systems, including passwords, time automatic on/off lights, blood pressure, and heart rate. The collected data cannot be stored in the IoT devices permanently due to their storage constraints. As a result, IoT utilizes the cloud to perform effective analysis such as storage and processing. The private information stolen by third-party applications or adversaries could lead to severe damages and also put life on a threat. For instance, adversaries can infer whether the owner has a smartphone or tablet to control the lights, appliances, and other devices over a dedicated wireless channel. In this case, the adversary may set up an exposure level to understand the situation based on the uploaded data to the cloud and subsequently commit theft or other related crime, as depicted in Fig. 9. The data processing and privacy-preservation techniques are generally categorized into three types, such as privacy-preserving, data aggregation, and data analysis.

However, data collection and analysis mechanisms can preserve privacy protection using encryption and key management mechanisms. Various existing approaches utilize data aggregation to preserve data privacy. In this connection, a massive amount of data can be handled in distant locations; thus, it is tough to accomplish privacy-preserving using heavyweight security solutions. Most of the proposed solutions are based on data aggregation and can be categorized into three types, such as anonymity-based privacy preservation, encryption-based privacy preservation, and perturbation-based privacy preservation (Wu et al. 2016). IoT environment enables anonymity and encryption to achieve privacy protection through the authentication protocol. Two-factor authentication (2FA) mechanisms mostly utilize wireless sensor networks (WSN) to offer reliable data transmission in healthcare applications (Wu et al. 2014; Srinivas et al. 2017). User-authentication and key establishment mechanism applied the Biohash technique to examine the selection criteria of multi-biometric cryptosystems (Jiang

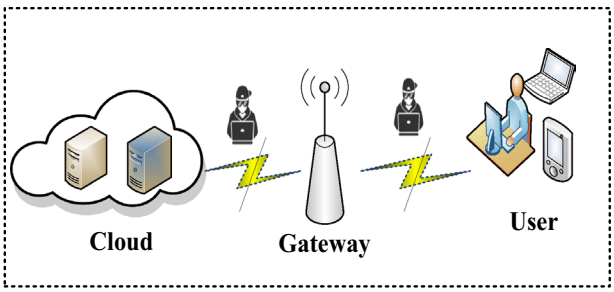

Fig. 9 Privacy disclosure

et al. 2017; David 2017). Moreover, a secure and anonymous biometric-based user authentication mechanism was proposed to provide secure communication in e-healthcare applications (Gope et al. 2018a, b). Their scheme ensured that an adversary cannot impersonate as a legitimate user to offer a robust authentication system.

The Biohash mechanism has unique advantages compared with other biometric features, and extensively increases the accuracy of biometric recognition, and protects user privacy. The 2FA mechanism devised the IoT devices to ensure privacy protection that preserves anonymous communication between connecting IoT devices and cloud storage (Li et al. 2018). Cui et al. (2018a, b) designed a blockchain-based authentication protocol to secure local IoT devices, which use a private blockchain to isolate the local network from the Internet. Lightweight mutual authentication mechanisms devised a mechanism using ECC encryption to achieve privacy protection with user anonymity (Karla and Sood 2015; Kumari et al. 2018; Zhang et al. 2017a, b; Yang et al. 2019; Rao and Prema 2019). Vijayakumar et al. (2017) and Liu et al. (2019) devised an efficient privacy protection authentication mechanism for vehicular mobile ad-hoc networks using anonymous certified ring signatures.

In the cloud computing (CC) domain, users cannot obtain control over the software, hardware, and data. The inefficient transparency and lack of control over the data lead to raise various security vulnerabilities and create organizations to mistrustfulness on their IT infrastructure. The private information is stored in distributed cloud services to determine the legitimacy of user access. However, to ensure security and privacy, various related authentication schemes have been proposed for the protection of data privacy (Samarati et al. 1998; Park and Park 2016; Chang et al. 2015; Amin et al. 2018). Samarati et al. (1998) introduced a syntactic privacy model where the problem of releasing person-specific data prevents user anonymity. Park and Park (2016) demonstrated that Chang et al. (2015) cannot achieve the standard security requirements of WSN. Also, their scheme fails to ensure system accuracy using the phase of system authentication. Moreover, their proposed scheme provides enhanced authentication and key establishment protocol using biometric-based information and ECC to address security vulnerabilities. Amin et al. (2018) devised a lightweight authentication mechanism for IoT-enabled devices. Their scheme prefers distributed multi-cloud environments to secure private information from cloud servers.

5 Countermeasures and validation tools

In this section, we focus on various counteractants and performance measures to withstand multiple attacks. Also, we present formal verification methods used in the authentication mechanisms that can make available for smart city applications (Ferrag et al. 2017). To secure the entire IoT system, authentication, and its essential security services, namely mutual authentication, key management, anonymity, untraceability, and perfect forward secrecy, are highly preferred. Moreover, the authentication mechanism uses both cryptographic and non-cryptographic counteractants to improve security efficiencies. Of late, various authentication mechanisms have been designed to withstand several malicious attacks, namely reply, user identity guessing, smart card loss/fraud, password guessing/detection, identity verification, and sensor-node impersonation.

5.1 Countermeasures

In the past few decades, various authentication and key management mechanisms have been designed to withstand several known and malicious attacks. Based on the classification of cryptosystems, the authentication schemes are categorized into three types; symmetric key cryptographic systems, asymmetric key cryptographic mechanisms, and hybrid mechanisms such as secure hashing mechanisms. As shown in Tables 5 and 6, an individual or real-time entity prefers a suitable mechanism to secure the communication system and to prevent potential attacks. However, very few mechanisms use a hybrid model such as secure hashing to improve the efficiency of the protocol. Reddy et al. (2018) proposed robust and secure pseudo-identity-based device authentication for smart cities. Their work addresses the use of secure authentication between mobile clients and IoT gateway. It uses a formal analysis to ensure the feature of robustness and efficiencies, including security and performance. Li et al. (2018) designed a lightweight authentication mechanism for IoT-enabled devices in distributed CC environments.

In this protocol design, they used a smartcard for the authentication process where the authenticated user can access all the services from the cloud anywhere. They formally analyzed their protocol using AVISPA and BAN-Logic to prove the security levels of the proposed protocol.

Moreover, informal cryptanalysis ensured that their protocol could withstand various possible security threats. Similarly, numerous RFID-based authentication protocols have been proposed to ensure secure communication while using RFID systems in smart cities. However, RFID systems have limited computing resources such as energy and bandwidth. It is evident that the traditional authentication framework is not suitable for massive connectivity. As a result, several lightweight authentication schemes have been proposed using secure hashing and symmetric encryption techniques to address the key factors such as resource limitation and security vulnerabilities. However, few security mechanisms are still challenging to prevent potential threats and to satisfy key requirements of the systems.

Gope et al. (2018a, b) devised a secure, lightweight privacy-preserving RFID-based authentication for distributed IoT platforms in smart city environments. This mechanism ensures reliable localization services to provide minimum execution time. It can achieve user anonymity, forward secrecy, secure localization, and untraceability to improve security efficiencies. Jiang et al. (2017) devised a new lightweight 3FA and key agreement scheme for integrated WSNs. They conducted a formal verification using the ProVerif tool to demonstrate that their protocol satisfies the standard requirements of the sensory networks. Li et al. (2013) proposed MFA and key agreement protocol using bilinear-paring for the IoT environments. It uses ECC to minimize the computation cost and to offer the security features such as mutual authentication, multi-factor authentication, shared session key, untraceability, and non-repudiation. Moreover, the formal verification using BAN-Logic proves that their mechanism can achieve the desired goals such as proper mutual authentication and session key agreement. Lee et al. (2019) proposed a secure 3FA mechanism for multi-gateway IoT environments. It uses fuzzy extraction and multi-gateway technique to provide secure and reliable IoT connectivity. Moreover, it uses analytical tools such as BAN logic and AVISPA to prove its security efficiencies, such as session key disclosure and gateway spoofing.

Most smart cities/industries operate a new generation of information technology to manage the systematic process of the computing networks. It may integrate various network functions such as asset tracking, occupancy detection, consumable monitoring to offer high-quality planning, development, and management. The integrated platform may provide a sustainable development to exploit the key features of the existing technologies such as mobile Internet, data mining, and artificial intelligence. Most sustainable environments facilitate data collection and processing to organize the process of real-time transmission (Martínez et al. 2017). It may even transform the computing services such as intelligence, interaction, and autonomy to meet the design perceptive of the smart environment. The summary of the development is as follows:

Innovation-driven It may offer an innovative path to emerge information systems and network technologies as one core to explore the functional components such as connectivity, computing service, device management, and network interface.

Industry-driven It may represent a development path to discover constructive guidance and to operate an intelligent form as a core driving tool to produce information services.

Sustainable-driven It may show a protective path to manage the sustainable resources that form intelligent management to discover a high-tech industrial system.

Service-driven It may derive a technological path to upgrade and optimize the management service and its relevant system function.

Multi-objective driven It may develop a comprehensive path to improve the management services and sustain the growth of constructive development.

5.1.1 Access control and secure authentication

IoT technology adopts access control and secure authentication to authorize system requests. It may design an intelligent IoT application to gain system access that verifies the authenticity of the real-time objects using key agreement techniques. The common techniques are role-based access control and attribute-based access control to ensure a valid authorization of any real-time object. The former technique converts the system privileges into a set of attributes to any real-time object, whereas the latter converts the system privileges into a set of functional roles to any real-time object. In addition, a technique known as authentication and authorization for constrained environments ensures the authenticity of real-time objects. Martínez et al. (2017) integrated a user-centric platform to secure sensitive data of IoT in smart cities. It uses a strategy of architecture reference model for IoT, which discovers a genuine platform to instantiate a set of application tools and to promote the quality guidelines. He et al. (2018) studied the concepts of access control and authentication to transplant the paradigm of IoT systems. It constructs an environment of single-user per device to achieve the access-control policies within an IoT. Zeng and Roesner (2019) derived the access control policies to design a suitable guideline that creates an access controller to the smart IoT environments. The classification of access control is as follows:

Role-based access control Each object is assigned with some specific roles such as administrator and guest to change the design policies and to organize the device connectivity.

Location-based access control The real-time entity is restricted from using the communication devices as long as it is not available nearby the IoT device.

Reactive access control An object tries to gain device access; unfortunately, it cannot acquire any system privilege to access the application service. In real-time, the user sends a connection request to an application server to approve or deny the networking services.

Supervisory access control A system may disallow or restrict the device connectivity if any unauthorized user is nearby to gain the device access.

5.1.2 IoT security and privacy-awareness

This work emphasizes the design features of security and privacy for smart IoT environments. The system applications may predominate the primary use cases of the business services to countermeasure IoT security, intrusion detection, single user sign-on, trust and security awareness, and privacy-by-design.

IoT security Most communication system applies a security framework to create a data message format among the real-time objects. It can prefer a platform using an embedded system to explore the core functionalities such as security, privacy, and trust. The encryption techniques such as lightweight symmetric, and asymmetric are utilized to make an appropriate mechanism known as the trivial file transfer protocol, which offers a reliable mechanism to the sensing platform. Li et al. (2018a, b, c) designed a key-free communication method to utilize a challenge-response mechanism. This mechanism offers a proper mutual authentication between the smart devices and a dedicated gateway to prevent key issues such as message forgery and man-in-the-middle attacks.

Intrusion detection This system operates in the network layer to design an effective IoT system that assesses malicious activities and policy violations to offer an event management system. Moreover, it regulates technical and administrative provisions to prevent unauthorized access. It may protect the source of electronic information and communication system to offer confidentiality and privacy of personal data (Chaabouni et al. 2019). At present, cybersecurity is playing a crucial role in evaluating the deficiency factors of electronic devices such as desktops, smartphones, servers, and networks.

Single user sign-on The certain IoT applications use a single user sign-on mechanism to offer seamless connectivity between the smart devices (Deebak and Al-Turjman 2021). It may exploit the features of the mechanism to provide better interactivity between the computing devices to gain information access.

Establishing trust with clients Trust-awareness is so crucial to gain device connectivity to determine the application services in a smart IoT environment (Sato et al. 2016). It may provide a state of control to enable a reliable transition that utilizes an access-control framework to present the conceptual idea of mutual trust to operate the transmission phase of IoT devices.

Security awareness The security measurement guarantees the growth of the IoT framework to access the components of IoT devices such as a printer, camera, and traffic controller (Zhang et al. 2014). The device can publicly use the core functionalities of cybersecurity to manage IoT enterprises, such as physical security, device monitoring, firmware update, and end-to-end encryption.

Privacy-by-design The device manufacturers consider the design strategies to protect the user information in the IoT environment (Foukia et al. 2016). It may integrate the functional elements such as sensor, actuator, and wireless connectivity to offer high-quality data features such as identity, trust, time, and chain of custody.

Device security, data privacy, and trustworthiness are assessed through the specific requirements of a smart IoT environment. These assessments are openly challenging to meet the standard requirements of next-generation computing systems. Each computing system may have minor breaches of policies and procedures that lead to unauthorized access to control the communication devices such as smartphones and laptops via a third-party application.

As to prevent any unauthorized access, the privacy information of smart computing devices should be well protected. Moreover, the privacy policies hold a legal statement to construct an effective policy agreement to collect, handle and process the generated data in smart IoT networks. Thus, essential factors such as reliable communication, risk assessment and mitigation, and preventing cyberattacks can be amalgamated to ensure better endpoint protection.

5.2 Formal validation tools

Cryptographic protocols cannot secure the generated keys using standard cryptographic schemes. The techniques such as verification and validation are necessitated to formalize the proof of security. Of late, several analytical tools have been designed for the analysis of cryptographic protocols. A formal analysis is becoming a standard mechanism to evaluate the proof of correctness of the security protocols. The analytical tools offer system feedback in terms of execution time and attack scenario to enhance security and performance efficiency. The formal analysis includes logical analysis or process algebra to test the performance factors and security deficiencies. The other analytical tools are emerging to standardize the process of functional verification, including security model, attack model, and performance evaluation. Lately, various formal mechanisms have been utilized to enhance the performance of the security protocol (Chai et al. 2015; Robert et al. 2017; Nikravan and Reza 2020; Wang et al. 2017). Few verification tools are depicted in Fig. 10 (Korba et al. 2013). They are as follows:

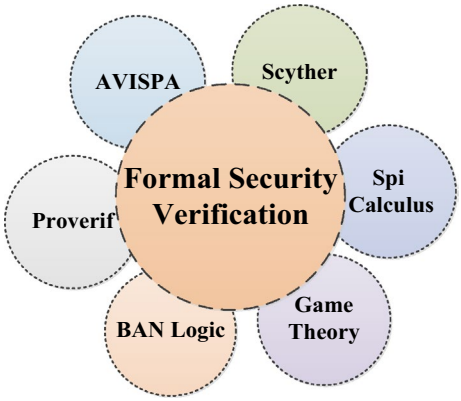

Fig. 10 Formal security verification tools

spi-calculus (analysis by process), "BAN-Logic" (Burrows et al. 1989), Automated Validation of Internet Security Protocols (AVISPA-Automatic Verification) (Armando et al. 2006), Game theory (Blanchet et al. 2018), and ProVerif (automatic reasoning) (Blanchet et al. 2010).

BAN-logic It includes three sequential steps, such as authentication of message source, freshness, and source trustworthiness, to define and analyze the exchange of transmissions. Burrows et al. (1989) constructed BAN logic to prove whether the security mechanism can withstand numerous malicious attacks.

ProVerif It is an automatic security protocol analyzer, which provides a fully automated technique to verify the security protocols using a formal method known as the Dolev-Yao Model (Dolev and Yao 1983). The connections are the system properties to describe events that can execute the symbolic models to translate the protocol description into the Horn clauses. The descriptive events formulate a comprehensive property using a logical formula that comprises conjunctions and disjunctions. ProVerif tool (Gil et al. 2019; Rao et al. 2019) proved that their mechanisms can implement mutual authentication and key agreement between the devices and other networks simultaneously. Also, it can use the Dolev-Yao model to prove whether the authentication mechanism can pass the verification or not.

Scyther It is a push-button tool enabled with GUI that analyzes, verifies, and falsifies the cryptographic schemes. Scyther (Nadeem and Howarth 2013; Cremers 2008) has various characteristics to provide unbounded verification with guaranteed termination that analyzes an infinite number of traces in patterns and supports multi-protocol analysis. Also, the working principle of Scyther is based on a pattern refinement algorithm. The command-line interface and python scripting libraries design the security protocol to examine the standard requirements such as key impersonation, replay, and password-guessing.

AVISPA It is a push-button tool consisting of various back-end tools which use state-of-the-art techniques to automate the protocol validation. It can employ a verification method to exhibit the scope of robustness, scalability, and performance. HLPSL (Von Oheimb 2005) is a modular and expressive formal language that can define protocol description and security evaluation. AVISPA integrates various back-end tools include Constraint Logic-based Attack Searcher (CL-AtSe), On-the-Fly-Model-Checker (OFMC), Tree Automata based on Automatic Approximations for the Analysis of Security Protocols (TA4SP), and SAT-based Model Checker (SATMC) to assess the proofs-of-concept. AVISPA (Armando et al. 2006) proves that the authentication mechanisms can protect from several known attacks, such as man-in-the-middle, replay, node capture, and desynchronization, to improve security efficiencies.

6 Research summary

The existing projects present an ethical solution to categorize two basic approaches: (1) adopts the emerging features to meet the standard requirements of a smart IoT environment; and (2) proposes a new conceptual idea to classify the specification of IoT devices and communication. In this work, various authentication mechanisms such as SFA, 2FA, 3FA, and MFA have been studied for the evolution of IoT technologies such as healthcare, surveillance, smart grid, transportation, public safety, and automation network (Yao et al. 2020). Most innovative solutions prefer a service distribution model to handle device connection, rule distribution, and dynamic validation. The IoT devices systematically include authentication, authorization, identity, and service management to classify the elements of context-aware systems. Traditional authentication integrates technical strategies such as knowledge location, inherence, behavior, and location to enhance the features of system attributes rather than device identities. The authentication model includes cloud-based, edge-based, and fog-based to offer reliable computing services. It may apply a quick-response (QR) code to represent the identities such as service provider, digital signature, and application server (Al-Ghaili et al. 2020).

To achieve efficient authentication in a smart IoT environment, the emerging technologies include a security framework known as the architecture reference model (ARM) (Bassi et al. 2013). The IoT environments, including healthcare, automation, and surveillance, manage a massive amount of communication devices to classify the limited resources such as processing power, bandwidth, memory, sensing issues, privacy, and security. The real-time system considers three key factors of the authentication such as knowledge, biometric, and ownership to ensure data protection between the communication parties. The system

primitives such as password-based, biometric, and fuzzy-extractor are utilized to prevent the potential threats. The application domains such as mobility, governance, people, and utilities drive the building blocks of the service infrastructure to offer reliable public services such as gas, electric, water, and sewage. The advent of technologies strengthens the operation of smart utilities to embrace data analytics and service optimization. Moreover, the business models realize the use of operational technology, advanced information technology, real-time analytics, and system integration to meet public safety and customer benefits (Shilenge and Telukdarie 2021). The critical derivatives are as follows:

Improved system interaction The system will have a mini-computer processor to collect the sensing information via a dedicated wireless channel. It may empower the system utilities such as platform, device, connectivity, and application to explore the deployment templates of IoT.

Improved system optimization The assistive technologies such as low power wide area network, Zigbee, and Bluetooth to improve the key functionalities such as mobility, cost efficiency, social values, and information access.

Sustainable environment The principle of sustainability represents three basic pillars such as environment, society, and economy to minimize the cost of ownership and to identify the IoT opportunities in a sustainable environment.

Improved system administration The smart cities address various technological challenges such as social, organization, and managerial to re-shape the relationship between the public and the governance.

Open-data [policy and standards] Smart cities can investigate the scope of global infrastructure to enable advanced computing services such as licensing, spectrum regulation, data protection, and traffic regulation.

Social impacts of IoT The emerging IoT devices can analyze the multi-dimensional approaches to represent the impact of social innovations. It may interconnect various physical devices to automate the business opportunities such as productivity, transparency, and competitiveness.

The security and privacy issues address the scope of the smart IoT environment. The IoT systems demand secure authentication techniques to assess the key features such as integrity, confidentiality, and authenticity. The systems may testify to the applications of IoT and CPS to realize the significance of existing authentication techniques. The detailed study reveals that lightweight authentication consumes one-way hashing, XOR operation, and perpetual hashing to design an effective mechanism. The operational strategies of lightweight authentication can be considered to develop a resource-constrained IoT device. This authentication can offer better robustness to analyze the potential attacks using the AVISPA tool. However, IoT devices demand a physical testbed to analyze the memory requirements and their nature of applicability. To provide better security and privacy in IoT, system integration, including authorization and authentication, is so crucial and effective. Most of the existing schemes prefer lightweight authentication to present a scenario of secure co-design hardware and software systems. It uses memory-based attestation and PUF-based authentication to offer mutual authentication and to prevent potential threats. The research findings demonstrate various security solutions to address the necessities of a secure authentication mechanism.

7 Conclusion and research directions

In this study, a rigorous systematic literature review was conducted to analyze the critical aspects of smart IoT environments, such as security and privacy. Most of the IoT environments focus on security issues to address the challenges of physical objects such as flexible, dynamic, and lightweight key management techniques. Most of the review articles extensively analyzed a secure platform, safety assurance, and heterogeneous environments to improve the emerging computing paradigms. As a result, in this study, several security threats and vulnerabilities have been identified for various computing paradigms such as distributed, cloud, fog, edge, and grid. In the adoption of IoT technologies, the key features such as device heterogeneity, identification, and authentication were cautiously examined to analyze the potential attacks such as spoofing, password-guessing, denial-of-service, and Sybil. On the other hand, the IoT applications highlight privacy risks and regulatory issues to signify the use of confidentiality and data integrity between the interconnected devices. Also, the applications deal with some potential threats such as presentation, profiling, tracking, location, and identification to make sure that the sensitive data cannot tamper when it is in transit between the connected devices.

As to analyze key vulnerabilities of smart IoT systems, in this survey, a comprehensive review has been conducted in the management of authentication and key agreement protocols. Moreover, this survey was organized to design a secure system, security requirements, malicious attacks, and perceptive of smart cities and industries to represent the integration of four distinct components as sensing, actuating, connecting, and processing the user interfaces. Moreover, the theoretical reviews, including security and privacy countermeasures, the recent techniques were thoroughly investigated to re-shape the development of innovative solutions and to signify the challenges of smart, intelligent systems. From the comparative analysis, the research gaps, technical defects, privacy-preserving issues, trustworthiness, and risk assessments were extensively investigated. Lastly, a study on formal verification tools was formulated to cover the use of mathematical transformation, including the correctness of hardware and

software behaviors. In the future, several open issues will be highlighted to discuss the challenges of security and privacy in emerging IoT environments.

References

Ahmed ME, Kim H (2017) DDoS attack mitigation in internet of things using software-defined networking. In: 2017 IEEE third international conference on big data computing service and applications (BigDataService). IEEE, pp 271–276

Akbar A, Kousiouris G, Pervaiz H, Sancho J, Ta-Shma P, Carrez F, Moessner K (2018) Real-time probabilistic data fusion for large-scale IoT applications. IEEE Access 6:10015–10027

Alaba FA, Othman M, Hashem IAT, Alotaibi F (2017) Internet of things security: a survey. J Netw Comput Appl 88:10–28

Al-Ghaili AM, Kasim H, Othman M, Hashim W (2020) QR code based authentication method for IoT applications using three security layers. Telkomnika 18(4):2004–2011

Alomair B, Poovendran R (2014) Efficient authentication for mobile and pervasive computing. IEEE Trans Mob Comput 13(3):469–481

Alotaibi SS (2018) Registration center-based user authentication scheme for smart e-governance applications in smart cities. IEEE Access 7:5819–5833

Al-Turjman F, Ever YK, Ever E, Nguyen HX, David DB (2017) Seamless key agreement framework for mobile-sink in IoT based cloud-centric secured public safety sensor networks. IEEE Access 5:24617–24631

Al-Turjman F, Nawaz MH, Ulusar UD (2020) Intelligence in the Internet of medical things era: a systematic review of current and future trends. Comput Commun 150:644–660

Al-Turjman F, Zahmatkesh H, Shahroze R (2019) An overview of security and privacy in smart cities' IoT communications. Trans Emerg Telecommun Technol e3677

Amin R, Biswas GP (2016) A secure lightweight scheme for user authentication and key agreement in multi-gateway based wireless sensor networks. Ad Hoc Netw 36:58–80

Amin R, Kumar N, Biswas GP, Iqbal R, Chang V (2018) A lightweight authentication protocol for IoT-enabled devices in distributed cloud computing environment. Future Gener Comput Syst 78:1005–1019

Analytics I (2014) Why the Internet of things is called internet of things: definition, history, disambiguation

Anttiroiko AV (ed) (2008) Electronic government: concepts, methodologies, tools, and applications: concepts, methodologies, tools, and applications, vol 3. IGI Global

Appio FP, Lima M, Paroutis S (2019) Understanding smart cities: innovation ecosystems, technological advancements, and societal challenges. Technol Forecast Soc Change 142:1–14

Armando A, Basin D, Cuellar J, Rusinowitch M, Viganò L (2006) Avispa: automated validation of internet security protocols and applications. ERCIM News 64(January)

Astill J, Dara RA, Fraser ED, Roberts B, Sharif S (2020) Smart poultry management: smart sensors, big data, and the Internet of things. Comput Electron Agric 170:105291

Atzori L, Iera A, Morabito G (2010) The internet of things: a survey. Comput Netw 5415:2787–2805

Banoth R, Arunakranthi G, Vachhani P, Kalaria S, Rathod R (2021) Implementation and mitigation for cyber attacks with proposed OCR process model. NVEO-NATURAL VOLATILES & ESSENTIAL OILS Journal| NVEO, 2149–2160

Batty M, Axhausen KW, Giannotti F, Pozdnoukhov A, Bazzani A, Wachowicz M, Portugali Y (2012) Smart cities of the future. Eur Phys J Spec Top 214(1):481–518

Bassi A, Bauer M, Fiedler M, Kramp T, van Kranenburg R, Lange S, Meissner S (eds) (2013) Enabling things to talk: designing IoT solutions with the IoT architectural reference model. Springer

Bibri SE, Krogstie J (2017) Smart sustainable cities of the future: an extensive interdisciplinary literature review. Sustain Cities Soc 31:183–212

Biggs J (2020) BrickerBot is a vigilante worm that destroys insecure IoT devices. https://techcrunch.com/2017/04/25/brickerbot-is-a-vigilante-worm-that-destroys-insecure-iot-devices/. Accessed June 2020

Blanchet B, Cheval V, Allamigeon X, Smyth B (2010) ProVerif: cryptographic protocol verifier in the formal model

Blanchet B, Smyth B, Cheval V, Sylvestre M (2018) ProVerif 2.00: automatic cryptographic protocol verifier, user manual and tutorial Version from, 05–16

Braun T, Fung BC, Iqbal F, Shah B (2018) Security and privacy challenges in smart cities. Sustain Cities Soc 39:499–507

Burrows M, Abadi M, Needham RM (1989) A logic of authentication. Proc R Soc Lond Math Phys Sci 426(1871):233–271

Butt TA, Afzaal M (2019) Security and privacy in smart cities: issues and current solutions. In: Al-Masri A, Curran K (eds) Smart technologies and innovation for a sustainable future. Advances in science, technology & innovation (IEREK interdisciplinary series for sustainable development). Springer, Cham. https://doi.org/10.1007/978-3-030-01659-3_37

Cahyadi EF, Yang CY, Wu NI, Hwang MS (2021) The study on the key management and billing for wireless sensor networks. Int J Netw Secur 23(6):937–951

Cardullo P, Kitchin R (2019) Being a "citizen" in the smart city: up and down the scaffold of smart citizen participation in Dublin, Ireland. GeoJournal 84(1):1–13

Chaabouni N, Mosbah M, Zemmari A, Sauvignac C, Faruki P (2019) Network intrusion detection for IoT security based on learning techniques. IEEE Commun Surv Tutor 21(3):2671–2701

Chahal RK, Kumar N, Batra S (2020) Trust management in social Internet of Things: a taxonomy, open issues, and challenges. Comput Commun 150:13–46

Chai HS, Choi JY, Jeong J (2015) An enhanced secure mobility management scheme for building IoT applications. In: FNC/MobiSPC. pp 586–591

Challa S, Wazid M, Das AK, Kumar N, Reddy AG, Yoon EJ, Yoo KY (2017) Secure signature-based authenticated key establishment scheme for future IoT applications. IEEE Access 5:3028–3043

Chan ACF, Zhou J (2014) Cyber-physical device authentication for the smart grid electric vehicle ecosystem. IEEE J Sel Areas Commun 32(7):1509–1517

Chang IP, Lee TF, Lin TH, Liu CM (2015) Enhanced two-factor authentication and key agreement using dynamic identities in wireless sensor networks. Sensors 15(12):29841–29854

Chatterjee S, Nandan M, Ghosh A, Banik S (2022) DTNMA: identifying routing attacks in delay-tolerant network. In: Tavares JMRS, Dutta P, Dutta S, Samanta D (eds) Cyber intelligence and information retrieval. Lecture notes in networks and systems, vol 291. Springer, Singapore. https://doi.org/10.1007/978-981-16-4284-5_1

Chaturvedi K, Kolbe TH (2019) Towards establishing cross-platform interoperability for sensors in smart cities. Sensors 19(3):562

Chen Y, Chen J (2021) A secure three-factor-based authentication with key agreement protocol for e-Health clouds. J Supercomput 77(4):3359–3380

Chen K, Zhang S, Li Z, Zhang Y, Deng Q, Ray S, Jin Y (2018) Internet-of-things security and vulnerabilities: taxonomy, challenges, and practice. J Hardw Syst Secur 2(2):97–110

Chin J, Callaghan V, Allouch SB (2019) The internet-of-things: reflections on the past, present and future from a user-centered and smart environment perspective. J Ambient Intell Smart Environ 11(1):45–69

Choi YJ, Kang HJ, Lee IG (2019) Scalable and secure internet of things connectivity. Electronics 8(7):752

Chourabi H, Nam T, Walker S, Gil-Garcia JR, Mellouli S, Nahon K, Scholl HJ (2012) Understanding smart cities: an integrative framework. In: 2012 45th Hawaii international conference on system sciences. IEEE, pp 2289–2297

Clarke R (1994) Human identification in information systems. Information Technology & People

Cremers CJ (2008) The Scyther tool: verification, falsification, and analysis of security protocols. In: International conference on computer-aided verification. Springer, Berlin, pp 414–418

Cui L, Xie G, Qu Y, Gao L, Yang Y (2018a) Security and privacy in smart cities: challenges and opportunities. IEEE Access 6:46134–46145

Cui J, Zhang Z, Li H, Sui R (2018b) An improved user authentication protocol for IoT. In: 2018 international conference on cyber-enabled distributed computing and knowledge discovery (CyberC). IEEE, pp 59–593

Da Xu L, He W, Li S (2014) Internet of things in industries: a survey. IEEE Trans Ind Inform 10(4):2233–2243

Danny T (2017) MFA (Multi-Factor Authentication) with biometrics. https://www.bayometric.com/mfa-multi-factor-authentication-biometrics/ Accessed June 2020

Das AK, Sutrala AK, Kumari S, Odelu V, Wazid M, Li X (2016) An efficient multi-gateway-based three-factor user authentication and key agreement scheme in hierarchical wireless sensor networks. Secur Commun Netw 9(13):2070–2092

David DB (2017) Mutual authentication scheme for multimedia medical information systems. Multimed Tools Appl 76(8):10741–10759

Deakin M, Al Waer H (2011) From intelligent to smart cities. Intell Build Int 3(3):140–152

Deebak BD (2020) Lightweight authentication and key management in mobile-sink for smart IoT-assisted systems. Sustain Cities Soc 63:102416

Deebak BD, Al-Turjman F (2020) A hybrid secure routing and monitoring mechanism in IoT-based wireless sensor networks. Ad Hoc Netw 97:102022

Deebak BD, Al-Turjman F (2021) Secure-user sign-in authentication for IoT-based eHealth systems. Complex Intell Syst 1–21

Deebak BD, Al-Turjman F, Mostarda L (2020) Seamless secure anonymous authentication for cloud-based mobile edge computing. Comput Electr Eng 87:106782

Deebak BD, Al-Turjman F, Nayyar A (2021) Chaotic-map based authenticated security framework with privacy preservation for remote point-of-care. Multimed Tools Appl 80(11):17103–17128

Department of Economic and Social Affairs (2014) World Urbanization Prospects: the 2014 revision, highlights. United Nations Population Division, New York

Devarakonda S, Halgamuge MN, Mohammad A (2019) Critical issues in the invasion of the Internet of Things (IoT): security, privacy, and other vulnerabilities. In: Kaur G, Tomar P (eds) Handbook of research on big data and the IoT. IGI Global, pp 174–196. https://doi.org/10.4018/978-1-5225-7432-3.ch010

Diane Vautier (2019) Smart Security for Smart cities. https://www.globalsign.com/en/blog/smart-security-for-smart-cities. Accessed May 2019.

Distefano S, Longo F, Scarpa M (2015) QoS assessment of mobile crowdsensing services. J Grid Comput 13(4):629–650

Dolev D, Yao A (1983) On the security of public-key protocols. IEEE Trans Inf Theory 29(2):198–208

Dora JR, Nemoga K (2021) Clone node detection attacks and mitigation mechanisms in static wireless sensor networks. J Cybersecur Priv 1(4):553–579

Eckhoff D, Wagner I (2017) Privacy in the smart city—applications, technologies, challenges, and solutions. IEEE Commun Surv Tutor 20(1):489–516

Eggers WD, Skowron J (2020) Forces of change: amart cities. https://www2.deloitte.com/insights/us/en/focus/smart-city/overview.html. Accessed June 2020.

El-hajj M, Fadlallah A, Chamoun M, Serhrouchni A (2019) A survey of internet of things (IoT) authentication schemes. Sensors 19(5):1141

Fadi AT, David DB (2020) Seamless authentication: for IoT-big data technologies in smart industrial application systems. IEEE Trans Ind Inform 17:2919–2927

Fan K, Gong Y, Liang C, Li H, Yang Y (2016) Lightweight and ultralightweight RFID mutual authentication protocol with cache in the reader for IoT in 5G. Secur Commun Netw 9(16):3095–3104

Fan K, Song P, Yang Y (2017) ULMAP: ultralightweight NFC mutual authentication protocol with pseudonyms in the tag for IoT in 5G. Mob Inf Syst 2017:2349149

Far HAN, Bayat M, Das AK, Fotouhi M, Pournaghi SM, Doostari MA (2021) LAPTAS: lightweight anonymous privacy-preserving three-factor authentication scheme for WSN-based IIoT. Wirel Netw 27(2):1389–1412

Farahat IS, Tolba AS, Elhoseny M, Eladrosy W (2019) Data security and challenges in smart cities. In: Hassanien A, Elhoseny M, Ahmed S, Singh A (eds) Security in smart cities: models, applications, and challenges. Lecture notes in intelligent transportation and infrastructure. Springer, Cham. https://doi.org/10.1007/978-3-030-01560-2_6

Ferrag MA, Maglaras LA, Janicke H, Jiang J, Shu L (2017) Authentication protocols for the internet of things: a comprehensive survey. Secur Commun Netw 2017:6562953

Foukia N, Billard D, Solana E (2016) PISCES: a framework for privacy by design in IoT. In: 2016 14th annual conference on privacy, security and trust (PST). IEEE, pp 706–713

Garcia-Carrillo D, Marin-Lopez R (2018) Multihop bootstrapping with EAP through COAP intermediaries for IoT. IEEE Internet Things J 5(5):4003–4017

Garcia-Font V, Garrigues C, Rifà-Pous H (2017) Attack classification schema for smart city WSNs. Sensors 17(4):771

Ghahramani M, Javidan R, Shojafar M (2020) A secure biometric-based authentication protocol for global mobility networks in smart cities. J Supercomput 1–27

Ghani A, Mansoor K, Mehmood S, Chaudhry SA, Rahman AU, Najmus Saqib M (2019) Security and key management in IoT-based wireless sensor networks: an authentication protocol using symmetric key. Int J Commun Syst 32(16):e4139

Gharaibeh A, Salahuddin MA, Hussini SJ, Khreishah A, Khalil I, Guizani M, Al-Fuqaha A (2017) Smart cities: a survey on data management, security, and enabling technologies. IEEE Commun Surv Tutor 19(4):2456–2501

Ghazal TM (2021) Internet of things with artificial intelligence for health care security. Arab J Sci Eng 1–12

Gil D, Johnsson M, Mora H, Szymański J (2019) Review of the complexity of managing big data of the internet of things. Complexity 2019:1–12

Gope P, Sikdar B (2018) Lightweight and privacy-preserving two-factor authentication scheme for IoT devices. IEEE Internet Things J 6(1):580–589

Gope P, Amin R, Islam SH, Kumar N, Bhalla VK (2018a) Lightweight and privacy-preserving RFID authentication scheme for

distributed IoT infrastructure with secure localization services for a smart city environment. Future Gener Comput Syst 83:629–637
Gope P, Lee J, Quek TQ (2018b) Lightweight and practical anonymous authentication protocol for RFID systems using physically unclonable functions. IEEE Trans Inf Forensics Secur 13(11):2831–2843
Grammatikis PIR, Sarigiannidis PG, Moscholios ID (2019) Securing the internet of things: challenges, threats and solutions. Internet Things 5:41–70
Gubbi J, Buyya R, Marusic S, Palaniswami M (2013) Internet of things (IoT): a vision, architectural elements, and future directions. Future Gener Comput Syst 29(7):1645–1660
Gupta A, Tripathi M, Shaikh TJ, Sharma A (2019) A lightweight anonymous user authentication and key establishment scheme for wearable devices. Comput Netw 149:29–42
Habeeb RAA, Nasaruddin F, Gani A, Hashem IAT, Ahmed E, Imran M (2019) Real-time big data processing for anomaly detection: a survey. Int J Inf Manag 45:289–307
Habibzadeh H, Soyata T, Kantarci B, Boukerche A, Kaptan C (2018) Sensing, communication and security planes: a new challenge for a smart city system design. Comput Netw 144:163–200
Habibzadeh H, Kaptan C, Soyata T, Kantarci B, Boukerche A (2019) Smart city system design: a comprehensive study of the application and data planes. ACM Comput Surv (CSUR) 52(2):1–38
Hammi B, Fayad A, Khatoun R, Zeadally S, Begriche Y (2020) A lightweight ECC-based authentication scheme for Internet of things (IoT). IEEE Syst J 14:3440–3450
Haseeb K, Almogren A, Ud Din I, Islam N, Altameem A (2020) SASC: secure and authentication-based sensor cloud architecture for intelligent internet of things. Sensors 20(9):2468
He W, Golla M, Padhi R, Ofek J, Dürmuth M, Fernandes E, Ur B (2018) Rethinking access control and authentication for the home internet of things (IoT). In: 27th {USENIX} security symposium {USENIX} security. USENIX, Baltimore, MD, pp 255–272
Heartfield R, Loukas G (2015) A taxonomy of attacks and a survey of defence mechanisms for semantic social engineering attacks. ACM Comput Surv (CSUR) 48(3):1–39
Hernandez-Castro JC, Tapiador JM, Peris-Lopez P, Quisquater JJ (2008) Cryptanalysis of the SASI ultralightweight RFID authentication protocol with modular rotations. arXiv preprint arXiv:0811.4257
Hernandez-Castro JC, Peris-Lopez P, Phan RCW, Tapiador JM (2010) Cryptanalysis of the David-Prasad RFID ultralightweight authentication protocol. In: International workshop on radio frequency identification: security and privacy issues. Springer, Berlin, pp 22–34
Hodo E, Bellekens X, Hamilton A, Tachtatzis C, Atkinson R (2017) Shallow and deep networks intrusion detection system: a taxonomy and survey. arXiv preprint arXiv:1701.02145
Hu VC, Ferraiolo D, Kuhn R, Friedman AR, Lang AJ, Cogdell MM, Scarfone K (2013) Guide to attribute-based access control (abac) definition and considerations (draft). NIST Spec Publ 800(162):1–54
Iqbal MA, Olaleye OG, Bayoumi MA (2017) A review on internet of things (IoT): security and privacy requirements and the solution approaches. Glob J Comput Sci Technol 16(7):1–9
Jan MA, Nanda P, He X, Tan Z, Liu RP (2014) A robust authentication scheme for observing resources in the internet of things environment. In: 2014 IEEE 13th international conference on trust, security and privacy in computing and communications. IEEE, pp 205–211
Jeschke S, Brecher C, Song H, Rawat DB (eds) (2016) Industrial Internet of Things: cybermanufacturing systems. Springer
Jiang Q, Zeadally S, Ma J, He D (2017) Lightweight three-factor authentication and key agreement protocol for internet-integrated wireless sensor networks. IEEE Access 5:3376–3392
Jiang Y, Yin S, Kaynak O (2018) Data-driven monitoring and safety control of industrial cyber-physical systems: basics and beyond. IEEE Access 6:47374–47384
Jiang Q, Zhang X, Zhang N, Tian Y, Ma X, Ma J (2021) Three-factor authentication protocol using physical unclonable function for IoV. Comput Commun 173:45–55
Jin J, Gubbi J, Marusic S, Palaniswami M (2014) An information framework for creating a smart city through internet of things. IEEE Internet Things J 1(2):112–121
Jurcut AD, Ranaweera P, Xu L (2020) Introduction to IoT security. IoT Secur Adv Authentication 27–64
Kalra S, Sood SK (2015) Secure authentication scheme for IoT and cloud servers. Pervasive Mob Comput 24:210–223
Kashyap S (2019) 10 real world applications of internet of things (IoT). https://www.analyticsvidhya.com/blog/2016/08/10-youtube-videos-explaining-the-real-world-applications-of-internet-of-things-iot/. Accessed May 2019
Khalid M, Mujahid U, Park H, Najam-ul-Islam M (2019) Cryptanalysis of the ultralightweight MAC protocol. In: 2019 13th international conference on open source systems and technologies (ICOSST). IEEE, pp 1–4
Khan R, Khan SU, Zaheer R, Khan S (2012) Future Internet the Internet of things architecture, possible applications and key challenges. In: 2012 10th international conference on frontiers of information technology. IEEE, pp 257–260
Korba AA, Nafaa M, Salim G (2013) Survey of routing attacks and countermeasures in mobile ad hoc networks. In: 2013 UK Sim 15th international conference on computer modelling and simulation. IEEE, pp 693–698
Kraijak S, Tuwanut P (2015) A survey on IoT architectures, protocols, applications, security, privacy, real-world implementation and future trends
Kumari S, Karuppiah M, Das AK, Li X, Wu F, Kumar N (2018) A secure authentication scheme based on elliptic curve cryptography for IoT and cloud servers. J Supercomput 74(12):6428–6453
Lalli M, Graphy GS (2017) Prediction based dual authentication model for VANET. In: 2017 international conference on computing methodologies and communication (ICCMC). IEEE, pp 693–699
Lee C, Wang C, Kim E, Helal S (2017) Blueprint flow: a declarative service composition framework for cloud applications. IEEE Access 5:17634–17643
Lee J, Yu S, Park K, Park Y, Park Y (2019) Secure three-factor authentication protocol for multi-gateway IoT environments. Sensors 19(10):2358
Li H, Lu R, Zhou L, Yang B, Shen X (2013) An efficient Merkle-tree-based authentication scheme for smart grid. IEEE Syst J 8(2):655–663
Li Q, Dou R, Chen F, Nan G (2014) A QoS-oriented Web service composition approach based on a multi-population genetic algorithm for Internet of things. Int J Comput Intell Syst 7(sup2):26–34
Li W, Song H, Zeng F (2017) Policy-based secure and trustworthy sensing for Internet of things in smart cities. IEEE Internet Things J 5(2):716–723
Li D, Aung Z, Williams JR, Sanchez A (2012) Efficient authentication scheme for data aggregation in smart grid with fault tolerance and fault diagnosis. In: 2012 IEEE PES innovative smart grid technologies (ISGT). IEEE, pp 1–8
Li Y, Lin Y, Geertman S (2015) The development of smart cities in China. In: Proceedings of the 14th international conference on computers in urban planning and urban management. AESOP, Massachusetts USA, pp 7–10
Li W, Li B, Zhao Y, Wang P, Wei F (2018a) Cryptanalysis and security enhancement of three authentication schemes in wireless sensor networks. Wirel Commun Mob Comput 2018:8539674
Li D, Peng W, Deng W, Gai F (2018b) A blockchain-based authentication and security mechanism for IoT. In: 2018 27th international

conference on computer communication and networks (ICCCN). IEEE, pp 1–6
Li C, Ji X, Zhou X, Zhang J, Tian J, Zhang Y, Xu W (2018c) HlcAuth: key-free and secure communications via home-limited channel. In: Proceedings of the 2018 on Asia conference on computer and communications security. ASIACCS'18, Incheon, Republic of Korea, pp 29–35
Lin J, Yu W, Zhang N, Yang X, Zhang H, Zhao W (2017) A survey on Internet of things: architecture, enabling technologies, security and privacy, and applications. IEEE Internet Things J 4(5):1125–1142
Liu W, Liu H, Wan Y, Kong H, Ning H (2016) The yoking-proof-based authentication protocol for cloud-assisted wearable devices. Pers Ubiquit Comput 20(3):469–479
Liu J, Yu Y, Jia J, Wang S, Fan P, Wang H, Zhang H (2019) Lattice-based double-authentication-preventing ring signature for security and privacy in vehicular Ad-Hoc networks. Tsinghua Sci Technol 24(5):575–584
Lloyd E, Ibbotson G, Pournouri S (2021) An Investigation into the impact Covid-19 has had on the cyber threat landscape and remote working for UK Organizations. In: Information security technologies for controlling pandemics. Springer, Cham, pp 151–170
Lohachab A, Lohachab A, Jangra A (2020) A comprehensive survey of prominent cryptographic aspects for securing communication in post-quantum IoT networks. Internet Things 9:100174
Luo E, Bhuiyan MZA, Wang G, Rahman MA, Wu J, Atiquzzaman M (2018) Privacy protector: privacy-protected patient data collection in IoT-based healthcare systems. IEEE Commun Mag 56(2):163–168
Mabkhot MM, Al-Ahmari AM, Salah B, Alkhalefah H (2018) Requirements of the smart factory system: a survey and perspective. Machines 6(2):23
Mahmood Z (ed) (2020) Connected vehicles in the internet of things: concepts, technologies, and frameworks for the IoV. Springer Nature, Berlin
Malhi AK, Batra S, Pannu HS (2020) Security of vehicular ad-hoc networks: a comprehensive survey. Comput Secur 89:101664
Maresch D, Gartner J (2018) Make disruptive technological change happen—the case of additive manufacturing. Technol Forecast Soc Change 155:119216
Martínez JA, Hernández-Ramos JL, Beltrán V, Skarmeta A, Ruiz PM (2017) A user-centric internet of things platform to empower users for managing security and privacy concerns in the internet of energy. Int J Distrib Sens Netw 13(8):1550147717727974
Masters G (2020) New IoT bot Persirai ensnaring IP cameras. https://www.scmagazineuk.com/new-iot-bot-persirai-ensnaring-ip-cameras/article/1474692. Accessed June 2020
McAfee (2017) McAfee Labs Threats Report; Technical Report; McAfee: Santa Clara
Merabet F, Cherif A, Belkadi M, Blazy O, Conchon E, Sauveron D (2020) New efficient M2C and M2M mutual authentication protocols for IoT-based healthcare applications. Peer Peer Netw Appl 13(2):439–474
Miettinen M, Nguyen TD, Sadeghi AR, Asokan N (2018) Revisiting context-based authentication in IoT. In: Proceedings of the 55th annual design automation conference. IEEE, San Francisco, CA, USA, pp 1–6
Ming Y, Cheng H (2019) Efficient certificateless conditional privacy-preserving authentication scheme in VANETs. Mob Inf Syst 2019:7593138
Mohsin JK, Han L, Hammoudeh M, Hegarty R (2017) Two factor vs multi-factor, an authentication battle in mobile cloud computing environments. In: Proceedings of the international conference on future networks and distributed systems. ACM, NY, US, pp 1–10
Montori F, Bedogni L, Bononi L (2017) A collaborative internet of things architecture for smart cities and environmental monitoring. IEEE Internet Things J 5(2):592–605
Moustaka V, Theodosiou Z, Vakali A, Kounoudes A, Anthopoulos LG (2019) Enhancing social networking in smart cities: privacy and security borderlines. Technol Forecast Soc Change 142:285–300
Mujahid U, Najam-ul-Islam M, Khalid M (2018) Efficient hardware implementation of KMAP+: an ultralightweight mutual authentication protocol. J Circuits Syst Comput 27(02):1850033
Mujahid U, Unabia G, Choi H, Tran B (2020) A review of ultralightweight mutual authentication protocols. Int J Electr Comput Eng 14(4):96–101
Nadeem A, Howarth MP (2013) A survey of MANET intrusion detection and prevention approaches for network layer attacks. IEEE Commun Surv Tutor 15(4):2027–2045
Nam T, Pardo TA (2011) Conceptualizing smart city with dimensions of technology, people, and institutions. In: Proceedings of the 12th annual international digital government research conference: digital government innovation in challenging times. ACM, NY, US, pp 282–291
Naranjo PGV, Pooranian Z, Shojafar M, Conti M, Buyya R (2019) FOCAN: a Fog-supported smart city network architecture for management of applications in the internet of everything environments. J Parallel Distrib Comput 132:274–283
Newaz AKM, Sikder AK, Rahman MA, Uluagac AS (2020) A survey on security and privacy issues in modern healthcare systems: attacks and defenses. arXiv preprint arXiv:2005.07359
Nicanfar H, Jokar P, Leung VC (2011) Smart grid authentication and key management for unicast and multicast communications. In: 2011 IEEE PES innovative smart grid technologies. IEEE, pp 1–8
Nikravan M, Reza A (2020) A multi-factor user authentication and key agreement protocol based on bilinear pairing for the Internet of Things. Wirel Pers Commun 111(1):463–494
Ometov A, Bezzateev S, Mäkitalo N, Andreev S, Mikkonen T, Koucheryavy Y (2018) Multi-factor authentication: a survey. Cryptography 2(1):1
Ometov A, Petrov V, Bezzateev S, Andreev S, Koucheryavy Y, Gerla M (2019) Challenges of multi-factor authentication for securing advanced IoT applications. IEEE Netw 33(2):82–88
Ostad-Sharif A, Arshad H, Nikooghadam M, Abbasinezhad-Mood D (2019) Three-party, secure data transmission in IoT networks through design of a lightweight, authenticated key agreement scheme. Future Gener Comput Syst 100:882–892
Park Y, Park Y (2016) Three-factor user authentication and key agreement using elliptic curve cryptosystem in wireless sensor networks. Sensors 16(12):2123
Paul A, Jeyaraj R (2019) Internet of things: a primer. Hum Behav Emerg Technol 1(1):37–47
Pellicer S, Santa G, Bleda AL, Maestre R, Jara AJ, Skarmeta AG (2013) A global perspective of smart cities: a survey. In: 2013 seventh international conference on innovative mobile and internet services in ubiquitous computing. IEEE, pp 439–444
Perera P, Patel VM (2019) Deep transfer learning for multiple class novelty detection. In: Proceedings of the IEEE conference on computer vision and pattern recognition. IEEE, Long Beach, CA, USA, pp 11544–11552
Phan RCW (2008) Cryptanalysis of a new ultralightweight RFID authentication protocol—SASI. IEEE Trans Dependable Secur Comput 6(4):316–320
Porambage P, Schmitt C, Kumar P, Gurtov A, Ylianttila M (2014) PauthKey: a pervasive authentication protocol and key establishment

scheme for wireless sensor networks in distributed IoT applications. Int J Distrib Sens Netw 10(7):357430
Qin W, Chen S, Peng M (2020) Recent advances in industrial internet: insights and challenges. Digit Commun Netw 6(1):1–13
Radu AI, Garcia FD (2016) LeiA: a lightweight authentication protocol for CAN. In: European symposium on research in computer security. Springer, Cham, pp 283–300
Ragab A, Selim G, Wahdan A, Madani A (2019) Robust hybrid lightweight cryptosystem for protecting IoT smart devices. In: International conference on security, privacy and anonymity in computation, communication and storage. Springer, Cham, pp 5–19
Rao V, Prema KV (2019) Lightweight hashing method for user authentication in internet-of-things. Ad Hoc Netw 89:97–106
Raza U, Kulkarni P, Sooriyabandara M (2017) Low power wide area networks: an overview. IEEE Commun Surv Tutor 19(2):855–873
Reddy AG, Suresh D, Phaneendra K, Shin JS, Odelu V (2018) Provably secure pseudo-identity based device authentication for smart cities environment. Sustain Cities Soc 41:878–885
Rekik M, Meddeb-Makhlouf A, Zarai F, Obaidat MS (2017) Improved dual authentication and key management techniques in vehicular ad hoc networks. In: 2017 IEEE/ACS 14th international conference on computer systems and applications (AICCSA). IEEE, pp 1133–1140
Robert J, Kubler S, Kolbe N, Cerioni A, Gastaud E, Främling K (2017) Open IoT ecosystem for enhanced interoperability in smart cities—example of Métropole De Lyon. Sensors 17(12):2849
Roberts B, Akkaya K, Bulut E, Kisacikoglu M (2017) An authentication framework for electric vehicle-to-electric vehicle charging applications. In: 2017 IEEE 14th international conference on mobile ad hoc and sensor systems (MASS). IEEE, pp 565–569
Roggema R (2020) The convenient city: smart urbanism for a resilient city. In: Data-driven multivalence in the built environment. Springer, Cham, pp 37–55
Roman R, Lopez J, Mambo M (2018) Mobile edge computing, fog et al.: a survey and analysis of security threats and challenges. Future Gener Comput Syst 78:680–698
Rouse M (2018) IoT Security (Internet of things Security). https://internetofthingsagenda.techtarget.com/definition/IoT-security-Internet-of-Things-security. Accessed June 2020
Sabri C, Kriaa L, Azzouz SL (2017) Comparison of IoT constrained devices operating systems: a survey. In: 2017 IEEE/ACS 14th international conference on computer systems and applications (AICCSA). IEEE, pp 369–375
Safkhani M, Bagheri N (2016) Generalized desynchronization attack on UMAP: application to RCIA, KMAP, SLAP and SASI+ protocols. IACR Cryptol 2016:905
Samarati P, Sweeney L (1998) Protecting privacy when disclosing information: k-anonymity and its enforcement through generalization and suppression (p. 19). Technical report, SRI International
Sanchez-Gomez J, Garcia-Carrillo D, Marin-Perez R, Skarmeta AF (2020) Secure authentication and credential establishment in narrowband IoT and 5G. Sensors 20(3):882
Sato H, Kanai A, Tanimoto S, Kobayashi T (2016) Establishing trust in the emerging era of Iot. In: 2016 IEEE symposium on service-oriented system engineering (SOSE). IEEE, pp 398–406
Scroxton A (2020) Robust security and consumer buy-in needed for smart city success. https://www.computerweekly.com/news/2240240594/Robust-security-and-consumer-buy-in-needed-for-smart-city-success. Accessed June 2020
Sengupta J, Ruj S, Bit SD (2020) A Comprehensive survey on attacks, security issues and blockchain solutions for IoT and IIoT. J Netw Comput Appl 149:102481
Seo D, Jeon YB, Lee SH, Lee KH (2016) Cloud computing for ubiquitous computing on M2M and IoT environment mobile application. Clust Comput 19(2):1001–1013
Sharma G, Kalra S (2017) A secure remote user authentication scheme for smart cities e-governance applications. J Reliab Intell Environ 3(3):177–188
Sharma G, Kalra S (2019) Advanced multi-factor user authentication scheme for E-governance applications in smart cities. Int J Comput Appl 41(4):312–327
Sharma V, You I, Jayakody DNK, Atiquzzaman M (2017) Cooperative trust relaying and privacy preservation via edge-crowdsourcing in social internet of things. Future Gener Comput Syst 92:758–776
Shilenge M, Telukdarie A (2021) 4IR integration of information technology best practice framework in operational technology. J Ind Eng Manag 14(3):457–476
Smart Cities Mission (2020) A step towards Smart India. https://www.india.gov.in/spotlight/smart-cities-mission-step-towards-smart-india. Accessed June 2020
Sookhak M, Tang H, He Y, Yu FR (2018) Security and privacy of smart cities: a survey, research issues and challenges. IEEE Commun Surv Tutor 21(2):1718–1743
Srinivas J, Mukhopadhyay S, Mishra D (2017) Secure and efficient user authentication scheme for multi-gateway wireless sensor networks. Ad Hoc Netw 54:147–169
Sudqi Khater B, Abdul Wahab AWB, Idris MYIB, Abdulla Hussain M, Ahmed Ibrahim A (2019) A lightweight perceptron-based intrusion detection system for fog computing. Appl Sci 9(1):178
Sun X, Ansari N (2017) Traffic load balancing among brokers at the IoT application layer. IEEE Trans Netw Serv Manag 15(1):489–502
Sun HM, Ting WC, Wang KH (2009) On the security of Chien's ultralightweight RFID authentication protocol. IEEE Trans Dependable Secur Comput 8(2):315–317
Tewari A, Gupta BB (2020) Security, privacy and trust of different layers in internet-of-things (IoTs) framework. Future Gener Comput Syst 108:909–920
Townsend AM (2013) Smart cities: big data, civic hackers, and the quest for a new utopia. WW Norton & Company, New York
Trappe W, Howard R, Moore RS (2015) Low-energy security: limits and opportunities in the Internet of things. IEEE Secur Priv 13(1):14–21
Urbieta A, González-Beltrán A, Mokhtar SB, Hossain MA, Capra L (2017) Adaptive and context-aware service composition for IoT-based smart cities. Future Gener Comput Syst 76:262–274
Vembu V (2020) Smart cities mission: welcome to tomorrow's world. 28th January 2016, http://www.thehindubusinessline.com/economy/smart-cities-mission-welcome-to-tomorrowsworld/article8163690.ece Accessed June 2020
Vijayakumar P, Azees M, Chang V, Deborah J, Balusamy B (2017) Computationally efficient privacy-preserving authentication and key distribution techniques for vehicular ad hoc networks. Clust Comput 20(3):2439–2450
Vinayakumar R, Alazab M, Soman KP, Poornachandran P, Al-Nemrat A, Venkatraman S (2019) Deep learning approach for intelligent intrusion detection system. IEEE Access 7:41525–41550
Von Oheimb D (2005) The high-level protocol specification language HLPSL developed in the EU project AVISPA. In: Proceedings of APPSEM 2005 workshop. APPSEM'05, Tallinn, Estonia, pp 1–17
Wang C, Xu G, Sun J (2017) An enhanced three-factor user authentication scheme using elliptic curve cryptosystem for wireless sensor networks. Sensors 17(12):2946
Wang Y, Su Z, Ni J, Zhang N, Shen X (2021) Blockchain-empowered space-air-ground integrated networks: opportunities, challenges, and solutions. IEEE Commun Surv Tutor 2021:1–1

Watson SM (2017) What the UK can learn from Singapore's smart city. Will plans for urban innovation hubs cure the UK's anxiety over an uncertain future? Just ask Singapore. https://www.wired.co.uk/article/sara-watson-singapore-smart-cities. Accessed June 2020

Wu L, Zhang Y, Wang F (2009) A new provably secure authentication and key agreement protocol for SIP using ECC. Comput Stand Interfaces 31(2):286–291

Wu M, Lu TJ, Ling FY, Sun J, Du HY (2010) Research on the architecture of the internet of things. In: 2010 3rd international conference on advanced computer theory and engineering (ICACTE), vol 5. IEEE, pp V5–484

Wu L, Zhang Y, Li L, Shen J (2016) Efficient and anonymous authentication scheme for wireless body area networks. J Med Syst 40(6):134

Wu F, Xu L, Kumari S, Li X, Shen J, Choo KKR, Das AK (2017) An efficient authentication and key agreement scheme for multi-gateway wireless sensor networks in IoT deployment. J Netw Comput Appl 89:72–85

Wu J, Guo S, Huang H, Liu W, Xiang Y (2018a) Information and communications technologies for sustainable development goals: state-of-the-art, needs and perspectives. IEEE Commun Surv Tutor 20(3):2389–2406

Wu F, Li X, Sangaiah AK, Xu L, Kumari S, Wu L, Shen J (2018b) A lightweight and robust two-factor authentication scheme for personalized healthcare systems using wireless medical sensor networks. Future Gener Comput Syst 82:727–737

Xu H, Ding J, Li P, Zhu F, Wang R (2018) A lightweight RFID mutual authentication protocol based on physical unclonable function. Sensors 18(3):760

Xu X, Xue Y, Qi L, Yuan Y, Zhang X, Umer T, Wan S (2019) An edge computing-enabled computation offloading method with privacy preservation for internet of connected vehicles. Future Gener Comput Syst 96:89–100

Yang Y, Wu L, Yin G, Li L, Zhao H (2017) A survey on security and privacy issues in internet-of-things. IEEE Internet Things J 4(5):1250–1258

Yang T, Zhang G, Liu L, Yang Y, Zhao S, Sun H, Wang W (2019) New features of authentication scheme for the IoT: a survey. In: Proceedings of the 2nd international ACM workshop on security and privacy for the internet-of-things. ACM, New York, NY, United States, pp 44–49

Yao X, Farha F, Li R, Psychoula I, Chen L, Ning H (2020) Security and privacy issues of physical objects in the IoT: challenges and opportunities. Digit Commun Netw 7:373–384

Yu S, Park K, Park Y (2019) A secure lightweight three-factor authentication scheme for IoT in cloud computing environment. Sensors 19(16):3598

Zeng E, Roesner F (2019) Understanding and improving security and privacy in multi-user smart homes: a design exploration and in-home user study. In: 28th {USENIX} security symposium ({USENIX} security 19). USENIX, Santa Clara, CA, USA, pp 159–176

Zeng X, Garg SK, Strazdins P, Jayaraman PP, Georgakopoulos D, Ranjan R (2017) IOTSim: a simulator for analyzing IoT applications. J Syst Archit 72:93–107

Zhang ZK, Cho MCY, Wang CW, Hsu CW, Chen CK, Shieh S (2014) IoT security: ongoing challenges and research opportunities. In: 2014 IEEE 7th international conference on service-oriented computing and applications. IEEE, pp 230–234

Zhang K, Ni J, Yang K, Liang X, Ren J, Shen XS (2017a) Security and privacy in smart city applications: challenges and solutions. IEEE Commun Mag 55(1):122–129

Zhang W, Lin D, Zhang H, Chen C, Zhou X (2017b) A lightweight anonymous mutual authentication with key agreement protocol on ECC. In: 2017 IEEE Trustcom/BigDataSE/ICESS. IEEE, pp 170–176

Zhao C, Huang L, Zhao Y, Du X (2017) Secure machine-type communications toward LTE heterogeneous networks. IEEE Wirel Commun 24(1):82–87

Zhou J, Li P, Zhou Y, Wang B, Zang J, Meng L (2018) Toward new-generation intelligent manufacturing. Engineering 4(1):11–20