International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 04 April 2026
Page No: 2079-2098
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0278

Exploration of International IoT Standards for Smart Cities Security, Privacy, and Trust Management

Durga Prasad Palla[1]
[1]*PhD Scholar, and Sabout Nagaraju, Associate Professor, Department of Computer Science, PUCC, Pondicherry University.*
Email ID: *durgaprasadpalla96@pondiuni.ac.in*[1]

Abstract
Over the years, the urban population has grown relentlessly. This growth brings new socio- economic and environmental hazards. In recent evolution, to overcome the present and future challenges of urban crowding, the world is heading toward the Internet of Things (IoT)-based intelligent solutions. These solutions endeavor urban socio-economic devel-opment with the most significant opportunities to improve the quality and ease of life. Inevitably, IoT data security, privacy, and trust threat issues and legislation are the main challenges that may hamper the adoption and growth of intelligent solutions. However, adopting appropriate international standards is mandatory to tackle the abovementioned barriers. International technical standards help organizations and individuals produce sustainable and reliable technology, products, and services. The existing literature discussed the international standards for IoT technologies and did not focus on security, privacy, and trust standards. To fill this gap, we narrowed down and explored ISO, IETF, ITU-T, and IEEE international standards that help to create a legislative landscape and to build security, privacy, and trust measures in smart city use cases.
Keywords: *Smart city; International standards; Internet of Things; trust, security; privacy.*

1. Introduction
In India, cities are growing relentlessly. Rural populations are steadily shifting to cities for employment opportunities and socioeconomic growth. According to the World Population Review report 2021, among 139.9 crores of the Indian population, urban occupies more than 35% [1]. As per the smart city report 2021 [2], 40% of the Indian population will live in cities by 2030. Experts also estimated that, by 2050, 50% of the In-dian population would be urbanized. As per the United Nations Department of Economic and Social Affairs (DESA) report 2021, 86% of the developed countries' population and 64% of the developing countries people will be urbanized [3]. This rapid growth in the urban population will lead to financial and infrastructural com-plications, inadequate natural resources, environmental hazards, poverty, and health problems. Moreover, conventional information and communication technology (ICT) solutions are insufficient to meet day-to-day urban challenges intellectually. Hence, making a city more intelligent using IoT-based technologies is the so-lution. An IoT-based smart city is paramount for building more responsive, affordable, equitable, transparent, and resilient cities for the day- to-day life of the citizens. A smart city is a framework that affords quality and ease of life in urban areas. Through innovative smart technologies, cities can promote efficient government, adequate natural resources, intelligent transportation, a clean and sustainable environment, and healthy urban life. In building heterogeneous IoT networks for smart environments, M.Rothmuller et al [4] predicted that the number of smart gadgets may increase from 35 billion in 2020 to 83 billion by 2024. These intelligent de-vices may interact with each other and transfer the collected data to cloud storage through the internet for fur-ther exploration. Moreover, IoT devices may gather massive amounts of sensitive information from individu-als and organizations without their consent. Some types of IoT devices, like smart appliances, may record the location of individuals. An attacker may extract sensitive details from the IoT data to host the cyber attacks. Shi-Cho et al. [5] discussed that whenever people use the services provided by the IoT, sensors can collect personal

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 04 April 2026
Page No: 2079-2098
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0278

information, which is sent to the cloud for further exploration. Thereafter, an attacker can extract sensitive information from a location. So the smart device must be aware of tracking. The sensitive information gathered and transmitted by the IoT devices could be used by an attacker or a third party to host cyber attacks. So any smart device must be free from cyber attacks. Shachar et al. [6] reviewed and analyzed the possible network layer security attacks of IoT devices. The major cyber attacks identified are spoofing, unau-thorized access, man-in-the- middle, DoS (Denial of Service), and Sybil. Andrea et al. [7] analysed some of the well-known physical layer attacks, such as malicious code injection, sleep deprivation, node tampering, and jamming. Brittany et al. [8] presented security and vulnerability issues in some of the smart home ven-dors, like Leeo Smart Alert, Google Home Mini, Philips Hue Smart Lighting, etc. Le costa et al. Le Costa et al. [9] investigated the various encryption attacks that may happen on smart devices, such as side-channel attacks, MITM (man-in-the-middle), and cryptanalysis. To overcome IoT data security, privacy, and trust threats and legislation issues, international standards such as ISO (International Standard Organisation), IETF (Internet Engineering Task Force), IEEE (Institute of Electrical and Electronics Engineers), ITU (International Tele-communication Union), etc., have proposed various guidelines. Many papers presented in the literature discuss the traditional standards in smart cities, but very few IETF, IEEE, ITU-T security and privacy standards were discussed. This is the only paper that provides a systematic review of international standards that discusses the security, privacy, and trust standards in critical smart city services like smart hospitals, smart homes, smart grids, smart parking, etc.

- Explored ISO, IETF, ITU-T, and IEEE international standards that address the security, privacy, and trust issues in critical smart services.
- Discussed the international standards for security and privacy guidelines for LoRaWAN and NB-IOT communications technologies, which are deployed in smart cities.

The rest of this paper is summarized as follows. Section 2 discusses survey research on security, priva-cy, and standardization related to smart city services. Section 3 presents international standards for security, privacy, and trust issues.

2. Related Work

This section describes the existing literature contributions, focus, and Limitations. Chai K. Toh [22], Abdul Rahaman et al. [25], and Tanweer et al. [26] discussed the security threats in smart city services like smart grids and smart hospitals, security aspects in cloud services, and the security techniques available to guard against various threats. However, security, privacy, and trust standardization are not discussed. Anton [29] began with a review of the smart education definition that defines the perspectives adopted and describes the supplementary features of the user. The author presents a detailed note on security and privacy threats in smart education platforms. Eskhita et al. [33] compare Dubai and Barcelona city according to the security and privacy of the user data collected by various sensors in smart city services. The results show that in Barcelona smart city services, the privacy of the user data is preserved, and it is not shared with any service providers. The author recommends the same best practices to be followed in Dubai smart city projects. Kashif et al. [31] provided an overview of the definition of a smart grid and discussed various threats associated with smart grid services like on-off, bad-mouthing, and DoS. The author experimented using ma-chine learning algorithms to evaluate the trustworthiness to secure the data in the smart grid service. Harper et al. [34] discussed the data collected by various sensors in the smart home might lead to privacy concerns. The author also urged that authorities adopt necessary regulations, standards, and policies to overcome the privacy concern in a smart home. Muhammad et al. [41] explained the layer-wise security attacks and their preventive techniques in smart healthcare services and also presented the privacy issues of patient data. The author ex-plores the attacks in the following layers: the network layer (DoS, DDoS, Wormhole attack) and the applica-tion layer (repudiation and non-repudiation attack, malicious code injection). However, the author does not discuss

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 04 April 2026
Page No: 2079-2098
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0278

the standardization in health care smart city services. The authors of [24], [23], [35], and [36] describe various international standards like ITU-T and IEEE that covers traditional standards and security. The major drawback of these studies is very few standards were discussed. Chun et al. [12] aim to clarify the need for IEEE international standards in smart city services. The author points out that implementing the standards in smart cities will lead to sustainable development. Dapeng et al. [21] conceptualized standardization in China's smart city projects, industry best practices, and the indi-cators for the smart city were discussed. The authors of [13], [14], [16], [19], and [20] analyzed various secu-rity threats in smart services like smart grids, smart hospitals, smart homes, and a few international standards such as IEEE 21451.001 (way of transmitting the data to the server in a secure manner), IEC 62351 (security in smart grid service), ISO/IEEE 11073 (international standard for healthcare patient data) and ISO/IEEE 802.15.4 (standard for the transmission of data in a trusted manner). This paper investigates the security, pri-vacy, and trust standards in various international standards issued by ISO, IETF, and ITU-T IEEE.

3. International Standards

The concept of smart cities is ambitious, standard, and sophisticated. For deploying smart city technol-ogies, the taxonomy of international standards presented in Figure 1 can help to reduce investment and opera-tional costs and benefits to implement industry best practices [42]. National and international officials should accept the standards in smart city development. This paper presents four technical standards that help to create a legislative landscape and to build security, privacy, and trust measures in smart city use cases. (Figure 1)

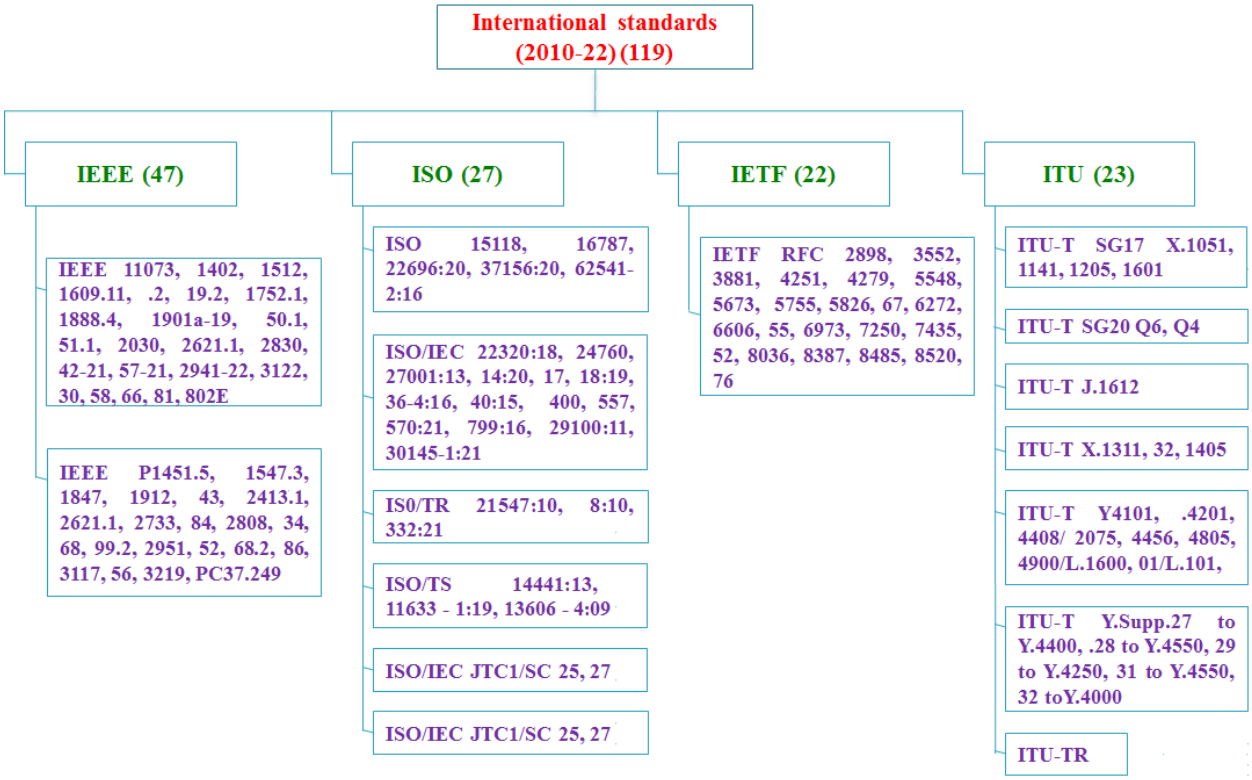

Figure 1 Taxonomy of International IoT standards

3.1.International Standard Organization

An ISO (International Standard Organization) is a service-providing organization whose intention is to minimize the number of technical definitions. ISO standards are applied in many applications: quality control, environmental control, energy control, Information Technology (IT) security, and safety.

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 04 April 2026
Page No: 2079-2098
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0278

ISO/IEC 27001 [24] gives a detailed description of storage security. Thereby, the integrity of data is preserved. IEC 62351 1-8 [42] and ISO 6254 1-2: 2016 [61][62] discusses the security and privacy considerations in smart grid service. ISO/IEC 27017:2015 [46][48], ISO/IEC 29100:2011 [53], ISO/IEC 27018:2019 [56], ISO/TR 21332:2021 [67] and ISO/IEC 27036 - 4 :2016 [70] defines the security and privacy requirements for cloud service providers to mitigate threats and privacy breach. ISO/IEC 27570:2021 [51], ISO/IEC 27799:2016 [52], ISO/IEC 27557 [57], ISO 22696:2020 [63], ISO/TS 13606 - 4: 2009 [64], ISO/TS 11633 - 1: 2019 [65], ISO/TS 14441 : 2013 [66], ISO/TR 21547:2010 [68] delineate the integrity of patient data, security and privacy requirements and threats associated with the smart hospital service. ISO/IEC 30145-1:2021 [54] and ISO 37156:2020 [55] exemplify the business framework and secure data transfer in smart city services. ISO/IEC JTC1/ SC25 [59] discusses the security and privacy of the devices in smart home service. ISO 15118 [58] and ISO 16787 [60] define the var-ious assistants deployed in parking slots for ease of parking and secure bi- directional communication in e-vehicles. Table 1 demonstrates a simple view of various ISO/IEC standards related to security, privacy, and trust.

Table 1 ISO/IEC standards for Smart City Services Security, Privacy, and Trust

Standard	Scope	Reference
ISO IEC JTC1/SC27	Covers the security aspects of improving the availability, integrity, and confidentiality through cryptographic and other security mechanisms.	[17] [43]
ISO/IEC 24760	Standard present identity management (ensure integrity, confidentiality, and availability of data) for an individual and for an organization.	[44]
ISO/IEC 27001:2013	It specifies the guidelines for the implementation of continuous improvement in information and security management.	[45]
ISO/IEC 27040:2015	Standard applies to the implementation of storage security, preserves the integrity and security of data whenever it is transferred in communication channels and deals with application security.	[46] [47]
ISO/IEC 27017:2015	Provides detailed guidelines for cloud service providers to implement security controls in cloud computing services.	[46] [48]
ISO/IEC 27400	This standard provides guidance on principles and information risks coupled with information security and mitigates the risks.	[46] [49]
ISO/IEC 22320:2018	Guidelines for organizations that help mitigate threats.	[50]
ISO/IEC 27570:2021	Provide guidelines for privacy management, privacy breach management, transparency management, and privacy assurance in smart cities.	[51]
ISO/IEC 27799:2016	Describe confidentiality and integrity of patient data is preserved, and it also ensures the minimum level of security in the health care domain.	[52]
ISO/IEC 29100:2011	Delineate the privacy control for outsourced data and also mention the privacy terminology for all applications.	[53]
ISO/IEC 30145-1	Represent the business process framework for smart city services that include health care, transportation, smart home,	[54]

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 04 April 2026
Page No: 2079-2098
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0278

:2021	etc.	
ISO 37156:2020	Specify the efficient and secure infrastructure for data exchange, maintenance, and monitoring in smart city services.	[55]
ISO/IEC 27018:2019	Provides detailed guidelines for cloud service providers to implement privacy controls in the cloud computingenvironment.	[56]
ISO/IEC 27557	This standard guides any individual/organization against privacy risks.	[57]
ISO 15118	Define secure bi-directional communication and smart charging in e-vehicle transportation.	[58]
ISO/IEC JTC1/SC25	Addresses the safety, security, and privacy of the connected devices in smart home applications.	[59]
ISO 16787	Describe the need for an assistant for vacant parking areas, recognizing obstacles, trajectory calculation, and vehicle map in ITS service.	[60]
ISO 62541 - 2:2016	Discuss the common threats in hardware and software components in smart grids.	[61] [62]
ISO 22696:2020	Delineate the threats, vulnerabilities, and security measures needed to be implemented in the health care industry.	[63]
ISO/TS 13606 - 4: 2009	Represent a technique for accessing health care data by using various privileges, and it also mentions the security requirements of data access.	[64]
ISO/TS 11633 - 1: 2019	Define data privacy and suggest risk assessment procedures for accessing health care data in a remote manner.	[65]
ISO/TS 14441: 2013	Describe the security and privacy prerequisite in smart health care technology.	[66]
ISO/TR 21332:2021	This standard addresses the security and privacy requirements in choosing a centralized model (i.e.) cloud computing given by the service provider.	[67]
ISO/TR 21547:2010	Characterize the fundamental standards required to securely protect health care records.	[68]
ISO/TR 21548:2010	Provides an outline of processes andcomponents to consider in organizations wishing to satisfy prerequisites set by ISO/TR 21547.	[69]
ISO/IEC 27036 - 4 :2016	Define the rules supporting the usage of information security for the utilization of cloud services.	[70]
ISO/IEC 27014:2020	This standard gives direction on concepts and processes for the administration of data security, by which an organization can assess, coordinate and communicate the data security-related process inside the organization.	[71]

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 04 April 2026
Page No: 2079-2098
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0278

3.2.Internet Engineering Task Force

The mission of the Internet Engineering Task Force (IETF) is to create quality, suitable engineering, and technical documentation. IETF RFC 4279 [73], IETF RFC 6655 [75], IETF RFC 7250 [76] and IETF RFC 7435 [93] deal with various encryption techniques are deployed for the authentication mechanism. IETF RFC 7452 [77] and IETF RFC 5673 [86] exemplify the various attacks and mitigation measures in smart devices and in-dustrial plants. Table IV shows IETF security privacy and trust standards. IETF RFC 6272 [78] and IETF RFC 8036 [84] discuss the various threats and define the security and privacy considerations in smart grid service. IETF RFC 5826 [81] and IETF RFC 3881 [83] delineate preventing attacks in smart homes and security review of healthcare data. IETF RFC 5548 [79], IETF RFC 8520 [80], IETF RFC 8576 [89], IETF RFC 3552 [90], IETF RFC 6973 [91] exemplify the various security threats and to guard against the security threats in smart city services like smart metering and various smart gadgets. IETF RFC 4251 [85] discusses the importance of data integrity, confidentiality, encryption, and authentication in various applications. IETF RFC 8485 [92] defines the trust evaluation between communication devices. Table 2 lists various IETF standards in critical smart services that encompass security, privacy, and trust.

Table 2 IETF Security, Privacy, And Trust Standards for Smart City Services

Standard	Scope	Refer.
IETF RFC 2898	The standard provides guidelines for the implementation of password-based cryptography contains encryption and message authentication schemes.	[72]
IETF RFC 4279	Suggests new cipher-suite techniques to be implemented in TLS during authentication.	[73]
IETF RFC 5755	Defines the use of an X.509 certificate for authorization and is used in several applications.	[74]
IETF RFC 6655	The standard describes the use of AES along with Cipher Block chaining to be implemented for message authentication.	[75]
IETF RFC 7250	This suggests a new certificate for exchanging public keys during authentication.	[76]
IETF RFC 7452	Describe the trust model to be used against physical attacks and the necessity of hardware-based random number generation during the design process.	[77]
IETF RFC 6272	Delineate the necessary protocols for the smart grid, and it also discussed the various threats that may occur in the smart grid.	[78]
IETF RFC 5548	Exemplify the need for routing protocol requirements that defend against various attacks in various applications like smart metering, pollution monitoring, etc.	[79]
IETF RFC 8520	Represent the secure deployment of IoT smart gadgets using Manufacturer Usage Description, which overcomes escalation attacks.	[80]
IETF RFC 5826	This standard encompasses the necessitate of routingrequirements in smart homes and automation that would prevent attacks.	[81]
IETF RFC 8387	Defines the smart object security requirements like firmware update.	[82]
IETF RFC 3881	Describe the format of information to be collected and the lastset of properties that have to be captured for security reviewing in the	[83]

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 04 April 2026
Page No: 2079-2098
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0278

	healthcare domain.	
IETF RFC 8036	This standard examines the routing protocol in metering and also discusses the security and privacy considerations of thedeployment of smart grid metering.	[84]
IETF RFC 4251	Discuss the importance of a Secure shell protocol that includes various functionalities like data integrity, confidentiality,encryption, and authentication.	[85]
IETF RFC 5673	Defines functional requirements in routing protocol that should be implemented against outsider attacks and insider attacks in industrial plants.	[86]
IETF RFC 5867	Delineate the implementation of a Building Management System (BMS) that reduce operation costs and security policies to be implemented.	[87]
IETF RFC 6606	Exemplify the design of LOWPAN, which is characterized by limited memory, moderate processing power, and rechargeable batteries, and also discuss multi-path routing in LOWPAN to guard against various attacks.	[88]
IETF RFC 8576	Discussed challenges and guard against security threats in intelligent devices.	[89]
IETF RFC 3552	Explain layer-wise security threats that might occur in intelligent devices and provides a guideline on implementingsecurity aspects.	[90]
IETF RFC 6973	Clarify various privacy threats that might occur in intelligent devices and provides a guideline on implementing privacy aspects.	[91]
IETF RFC 8485	This standard defines vectors of trust (an endeavor to give information for a client to make a choice), which is to be utilized between the communication devices.	[92]
IETF RFC 7435	Define opportunistic encryption to be utilized in situations where back for encryption isn't known in advance or not at allneeded.	[93]

3.3.International Telecommunication Union

The International Telecommunication Union (ITU) improves information and Communication Tech-nologies (ICTS) access for the global community. The purpose of the ITU is to coordinate telecommunications businesses, such as managing radio spectrum and satellite orbits around the world. ITU-T X.1311 deals with the minimum security requirements required in the implementation of any smart city services. ITU-T Y.4805 [101], ITU-T Y.4201 [102], ITU-T Y.4408/ 2075 [103], ITU-T Y.4805 [105], ITU-T Y.4900/L.1600 [106], ITU-T Y.4101 [108], ITU-TR [114] discusses confidentiality, integrity, security, privacy, interoperability, adaptability, data protection, resilience, intercommunication between devices and environment sustainability of smart city services. ITU-T SG 17 X.1205 [17], ITU-T X.1332 [99], and ITU-T X.1405 [100] delineate the various security threats that occur in smart city services like a smart meter, digital ledger, and network layer. ITU-T SG 20 Q6 [95] exemplifies the need for trustworthiness in IoT smart devices. ITU-T Y.4456 [104] rep-resents parking guidance, access control, and method of payment in parking service in smart transport service. ITU-T Y.Supp.31 to Y.4550 [112], ITU-T Y.Sup32 to Y.4000 [113] defines the minimum security require-ments in a smart home and proper

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 04 April 2026
Page No: 2079-2098
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0278

recommendations for any smart city service. Table 3 highlights the ITU-T standards for smart city services.

Table 3 ITU standards for Smart City Services Security, Privacy, and Trust

Standard	Scope	Ref.
ITU-T SG 17 X.1601	Provide an overview of the security framework for the sensor data stored in the cloud.	[17] [94]
ITU-T SG 20 Q6	Mitigate the threats associated with the smart device, help preserve the integrity, security, and privacy, and to improve the trustworthiness of IoT devices.	[17] [95]
ITU-T SG 20 Q4	Any sensor data which is transmitted via wireless communication technologies must be secure.	[96]
ITU-T X.1311	Standard encompasses the security threats and the needed security requirements in a sensor network.	[97]
ITU-T J.1612	Define the architecture of a smart home gateway and alsodescribe the secure communication between end devices and gateway.	[98]
ITU-T X.1332	Describe security requirements against security threats andattacks in smart meter applications.	[99]
ITU-T X.1405	Delineate on security requirements against threats and attacks in digital ledger technology.	[100]
ITU-T Y.4201	Represent the high-level requirements such as inter-system communication, security, resilience, and interoperability in the smart city platform.	[101] [102]
ITU-T Y.4408/2075	Exemplify the capability framework to support the security capabilities like Authentication, Authorization, Confidentiality, Integrity, and Access control.	[101] [103]
ITU-T Y.4456	Provide parking guidance, parking lot reservation, automatic access control, and payment service in smart parking.	[101] [104]
ITU-T Y.4805	Describe the identifier service requirements to ensure security and interoperability in smart cities.	[101] [105]
ITU-TY.4900/ L.1600	Represent the overview of key performance indicators in smart cities like information security, privacy, quality of life, and environment sustainability.	[101] [106]
ITU-TY.4901 /L.101	Delineate the key performance indicators related to the impacts of ICT and ensure online child protection against cyber harassment.	[107]
ITU-T Y.4101	Exemplify the capabilities and requirements of gateway like security support, adaptability, scalability, communication, and QoS in smart city services.	[108]
ITU-TY.Supp.27 to Y.4400	Define the ICT architecture framework, namely fault-tolerant, inter-operability, and flexibility insmart cities like data protection, data resilience, and privacy.	[109]
ITU-TY.Supp.28 to Y.4550	Describe an integrated management solution for sensors, nodes,and models with the objective of making a smart city a sustainable one.	[110]

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 04 April 2026
Page No: 2079-2098
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0278

ITU-TY.Supp.29 to Y.4250	Standard encompasses a variety of infrastructure needed forsmart city services, viz. Resilience and reliability, vulnerabilities need to be addressed, etc.	[111]
ITU-T .Supp.31to Y.4550	Define the requirements of intelligent building, which encompasses data security schemes, communication systems, QoS, and networking infrastructure.	[112]
ITU-T Y.Sup32 to Y.4000	Delineate the recommendation on smart city functions and their future development.	[113]
ITU-TR	Describe the data protection, cyber vulnerabilities, and resilience of smart city services.	[114]

3.4.Institute of Electrical and Electronics Engineers

The Institute of Electrical and Electronics Engineers (IEEE) helps organizations and individuals produce new standards, products, and services. By refining IEEE standards guidelines/toolsets about rapidly changing technologies, developers can build their own systems. IEEE P2621.1 and IEEE 11073 standards are with smart hospital services, where the patient data are transmitted to the hospital servers with the help of sensors that must be secure and safer. IEEE 1888.4 [120], IEEE 2621.1 [132], IEEE P2733 [156] delineate the security, privacy, trust and guidelines for health care data. IEEE 2030 [121], IEEE P1547.3 [122], IEEE 2857-2021 [124], IEEE 1402 [131], IEEE P2808 [157], IEEE PC37.240 [159] exemplify the cyber security considerations, security threats in smart meter and smart grid. IEEE P2899.2 [130] and IEEE P2413.1 [158] delineate security and privacy guidelines in smart home application devices. IEEE P2621.1 [39], IEEE 11073 [116], IEEE 2621.1 [132], IEEE 1752.1 [140], IEEE P1847 [144], IEEE P2968.2 [145], IEEE P2733 [156] describe the privacy, integrity of patient data, cyber security guidelines in hospital electronic devices, and standardization of health care data. IEEE 3130 [137], IEEE 1609.2 [151], and IEEE P2413.1 [158] discuss the various threats in the smart vehicle, guard against those threats, and the message format in transportation service. IEEE P1451.5.5 [141] and IEEE P1451.5.10 [142] delineate the security, privacy, design, and specification of LoRa and NB-IoT communication technologies that are deployed in smart cities. IEEE 2941-2021 [123], IEEE 2857-2021 [124], IEEE P3156 [133], IEEE PC37.249 [135] represents networking specifications, privacy of sensitive data, security requirements in smart city services. IEEE P3219 [125], IEEE 3181 [127], IEEE 3158 [129], IEEE P2952 [147], IEEE P2733 [156] discuss blockchain-based trust framework, trust calculation for communicating nodes in a network in smart hospital. IEEE P2899.2 [130] exemplifies the safety, security, and privacy in speech recognition smart home devices. In Table IV, we provide a summary of IEEE standards in critical smart city services to provide a better understanding for researchers and smart city builders.

Table 4 IEEE standards for Smart City Services Security, Privacy, and Trust

Standard	Scope	Reference
IEEE P2621.1	The standard ensures the integrity, safety, and privacy of patient data for developing secure and safer products.	[115]
IEEE 11073	Suggest the patient medical data can be retrieved, transferred, and processed without any loss of sensitive patient data.	[116]
IEEE P2834	Focus on secured and trusted Smart Education Systems.	[117][118]
IEEE 1609.2	The standard ensures that only the intended recipient received the data (or) not when the data is transmitted in a wireless	[119]

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 04 April 2026
Page No: 2079-2098
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0278

	medium.	
IEEE 1888.4	Defines function, data type, and default unit for Security-Alarm in the green smart home.	[120]
IEEE 2030	Provides guidelines for minimizing security concerns in smart meters.	[121]
IEEE P1547.3	Facilitates cyber-security guidelines for distributed power grid systems.	[122]
IEEE 2941-2021	Protects business-sensitive information in smart cities.	[123]
IEEE 2857-2021	Defines mesh networking specifications for securing smart utility services (smart parking, street lighting, smart grid, etc.) ina smart city	[124]
IEEE P3219	Defines blockchain-based zero-trust framework for IoT applications security and trust.	[125]
IEEE P1943	Explain the need to implement post-quantum cryptographic algorithms against cryptanalytic attacks.	[126]
IEEE 3181	Specify a technical framework for the trusted environment in computational nodes.	[127]
IEEE 3166	Elucidate the technical terminologies in smart city services such as renewable energy and electrical energy storage system.	[128]
IEEE 3158	Facilitate a secure, transparent, and trusted way of data sharing.	[129]
IEEE P2899.2	Exemplify the safety, information security, and privacy in speech recognition smart home devices.	[130]
IEEE 1402	Specify the need for security in power stations against unauthorized access and vandalism.	[131]
IEEE 2621.1	Represent the framework for security assurance and guidelines in smart hospital electronic devices.	[132]
IEEE P3156	Defines the privacy requirements and security requirements in the privacy-preserving platforms.	[133]
IEEE P3117	Exemplify the framework to be adopted in privacy-preserving.	[134]
IEEE PC37.249	Categorize the files, such as protection and automation, based on content, use, and disclosure.	[135]
IEEE 3122	Construe a defined framework for compression, decompression, and encryption of data (video and audio).	[136]
IEEE 3130	Identifies the threats target OS in smart vehicles and defines the smart vehicle's minimal security requirements.	[137]
IEEE 2842-2021	Building trust and data protection using secure multi-party computation.	[138]
IEEE 2830	The machine learning model is trained using encrypted data and processed by a rusted party during computation.	[139]
IEEE 1752.1	Standardization of mobile health care data that includes sharing and aggregation.	[140]

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 04 April 2026
Page No: 2079-2098
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0278

IEEE P1451.5.5	Defines the design and specification in LoRa, and it also provides a set of guidelines in security, privacy, and quality of service aspects in smart systems.	[141]
IEEE P1451.5.10	Describe the design and specification in NB-IoT, and it also represents a set of guidelines in security, privacy, and quality of service aspects in a smart system.	[142]
IEEE P2986	Illustrate the best practices of security and privacy aspects in Federated learning.	[143]
IEEE P1847	Exemplify the framework of location service in health care.	[144]
IEEE P2968.2	Represent a set of considerations and requirements to be followed in cyber security and data privacy of the protocol design in clinical applications	[145]
IEEE P2951	Describe a set of standards for a smart home device that encompasses capabilities like motion, system security, and coordination.	[146]
IEEE P2952	Formulate a framework for a trusted execution environment in secure computing.	[147]
IEEE 802E	Provide guidelines on the protection of privacy threats in 802 protocols.	[148]
IEEE 1609.11	Explain the payment service layer, profiling, and identity authentication in the intelligent transportation system.	[149]
IEEE 1619.2	Delineate EME2-AES and XCB-AES wide-block encryption to reduce the granularity of the security attack.	[150]
IEEE 1609.2	Represent the message formats and their processing techniques in intelligent transportation systems.	[151]
IEEE 1951.1	Describe identity management for entities, message passing format, and interfaces in smart cities.	[152]
IEEE P2868	Exemplify the technical requirements that include security and privacy in smart display boards.	[153]
IEEE P1912	Explain the privacy aspects to be adopted when the applications are implemented on edge, fog, and cloud computing.	[154]
IEEE 1950.1	Delineate the architectural, functional framework, and communication system aspects in smart city management.	[155]
IEEE P2733	Defines the framework in security, privacy, and trust for clinical IoT devices like wearables and health care records.	[156]
IEEE P2808	Represent cyber security controls and measures against security threats in electric power systems.	[157]
IEEE P2413.1	Describe the security aspects and architectural blueprint in various smart city services like smart parking, waste management, eHealth, etc.	[158]
IEEE PC37.240	Provides cyber security technical requirements in power systems.	[159]
IEEE P2784	Gives a framework that outlines the process, required technology standards, and planning framework for evolving a smart city.	[160]

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 04 April 2026
Page No: 2079-2098
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0278

IEEE 1512	The objective of this standard is to bolster proficient communication for real-time in intelligent transportation.	[161]

The table 5 consolidates key international standards across ISO/IEC, IETF, ITU-T, and IEEE, mapping them to the core security, privacy, and trust functions required in smart-city ecosystems. It highlights how different standards families collectively address data protection, privacy governance, device authentication, identity management, trust evaluation, and sector-specific needs such as smart-grid resilience, healthcare data security, intelligent transport assurance, and smart-home protection. By organizing the standards according to functional domains, the table illustrates how each contributes distinct yet complementary capabilities, enabling city planners and system integrators to align technical requirements with robust, interoperable, and trustworthy smart-city deployments.

Table 5 Mapping of Security, Privacy, and Trust Standards to Core Smart-City Functional Domains

Functional Domain	Representative Standards	Illustrative Focus
Data Protection & Storage Security	ISO/IEC 27001, ISO/IEC 27040, ISO/IEC 27017, ISO/IEC 27018	Information-security governance; storage security; cloud-security and privacy controls.
Privacy Management & Compliance	ISO/IEC 29100, ISO/IEC 27570, ISO/IEC 27799, IEEE P3156, IETF RFC 6973	Privacy frameworks; breach management; healthcare confidentiality; privacy-preserving computation.
Device Authentication & Security	IETF RFC 4279, RFC 7250, RFC 8520; ITU-T X.1311; IEEE 1609.2	TLS cipher-suites; secure IoT onboarding; sensor network requirements; vehicular authentication.
Identity & Access Management	ISO/IEC 24760, ISO/TS 13606-4, IEEE 1951.1	Identity governance; controlled access to health records; cross-domain identity management.
Trust Management & Assurance	IETF RFC 8485, IEEE P3219, IEEE 3158, ITU-T SG20 Q6	Trust vectors; blockchain-based zero-trust; trusted data-sharing; device trustworthiness.
Smart-Grid & Utility Security	IEC/ISO 62351, IETF RFC 6272, IEEE 2030, IEEE PC37.240	Secure grid communication; metering hardening; interoperability and cyber-security.
Healthcare Data Protection & Clinical IoT Security	ISO/IEC 27799, ISO/TS 14441, IEEE 11073, IEEE P2733, IETF RFC 3881	Patient data confidentiality; EHR security; clinical IoT trust and audit logging.
Smart-Home & IoT Security	ISO/IEC JTC1/SC25, IETF RFC 5826, RFC 5548, IEEE P2899.2	Home device protection; routing security; spoofing mitigation; voice-system privacy.
Intelligent Transport & Vehicular Security	ISO 15118, ISO 16787, IEEE 1609.2/1609.11, IEEE 3130	Secure EV charging; parking assistance; authenticated vehicular messaging.
Platform Interoperability &	ISO/IEC 30145-1, ISO 37156, ITU-T Y.4201, Y.4408/2075, IEEE P2413.1	Reference architectures; secure data exchange; authentication/authorization frameworks.
Wireless IoT (LoRa, NB-IoT) Security	IEEE P1451.5.5, IEEE P1451.5.10	Security, privacy, and QoS guidelines for LPWAN technologies.

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 04 April 2026
Page No: 2079-2098
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0278

Conclusion

International standards provide a robust foundation for developing secure, privacy-preserving, and trustworthy smart city ecosystems. By strategically combining complementary frameworks—ranging from ISMS governance (ISO/IEC 27001 family) and cloud/privacy controls to IETF operational device guidance, ITU-T platform requirements, and IEEE device- and sector-specific specifications—city authorities and system integrators can establish deployments that are both defensible and interoperable. Furthermore, standardisation efforts must increasingly address the realities of next-generation smart city infrastructures. Key priorities include aligning constrained-device security models, adopting machine-readable and AI-driven trust frameworks that can automate assurance across heterogeneous systems, and integrating blockchain-based or distributed-ledger mechanisms to enhance data provenance and privacy preservation in multi-party data-sharing environments. By presenting a consolidated mapping of applicable standards, this paper aims to equip planners, engineers, and policy-makers with the insight needed to select and integrate the standards best aligned with their operational risks, architectural constraints, and service objectives as cities evolve toward more autonomous and data-intensive futures.

References

[1] World Population Review (2021) India, [Online] Available: https://worldpopulationreview.com/countries/cities/india

[2] Smart Cities Mission, Ministry of Housing and Urban Affairs, Government of India (2021), "Making a Smart City: Learning from the Smart City Mission", [Online] Available:https://smartnet.niua.org/sites/default/files/resources/making_a_city_smart_mar2021.pdf

[3] Allied Telesis (Blog), ICT: The Fundamental Enabler for Smart Cities. [Online] Available: https://www.alliedtelesis.com/in/en/blog/ict-fundamental-enabler-smart-cities

[4] M. Rothmuller, S. Barker. : IoT–The Internet of transformation 2020. Basingstoke, *U.K., Juniper Res.*, White Paper, (2020).

[5] Shi-Cho Cha, Tzu-Yang Hsu, Yang Xiang, Kuo-HuiYeh. : Privacy Enhancing Technologies in the Internet of Things: Perspectives and Challenges. *IEEE Internet of Things Journal*, vol. 6, no. 2, pp.2159 - 2187, (2019).

[6] ShacharSiboni, VinaySachidananda, YairMeidan, Michael Bohadana, Yael Mathov, SuhasBhairav, AsafShabtai, Yuval Elovici. : Security Testbed for Internet-of-Things Devices. *IEEE Transactions on Reliability*, vol. 68, no. 1, pp.23 - 44, (2019).

[7] I. Andrea, C. Chrysostomou, G. Hadjichristofi. : Internet of Things: Security vulnerabilities and challenges. *IEEE Symposium on Computers and Communication (ISCC)*, pp. 180-187,(2015).

[8] Brittany D. Davis, Janelle C. Mason, Mohd Anwar. : Vulnerability Studies and Security Postures of IoT Devices: A Smart Home Case Study. *IEEE Internet of Things Journal*, vol. 7, no.10, pp. 10102 - 10110, (2020).

[9] L. Costa, J. Barros, and M. Tavares. : Vulnerabilities in IoT Devices for Smart Home Environment. 5th*International Conference on Information Systems Security and Privacy (ICISSP)*, (2019).

[10] "IEEE Approved Draft Standard for Wireless Smart Utility Network Field Area Network (FAN)," in IEEE P2857/D3, vol., no., pp.1-177, (2021).

[11] N. M. Karie, N. M. Sahri, W. Yang, C. Valli, V. R. Kebande. : A Review of Security Standards and Frameworks for IoT-Based Smart Environments. *IEEE Access*, vol. 9, pp. 121975- 121995, (2021).

[12] C. Sing Lai et al.:A Review of Technical Standards for Smart Cities. *Clean Technologies*, Vol 2 pp 290 - 310, MDPI, (2020).

[13] F. Laamarti, H. F. Badawi, Y. Ding, F. Arafsha, B. Hafidh, A. E. Saddik. : An ISO/IEEE 11073 Standardized Digital Twin Framework for Health and Well-Being in Smart Cities. *IEEE Access*, vol. 8, pp. 105950-

105961, (2020).

[14] Dae. -m. Han and J. -h. Lim.: Smart home energy management system using IEEE 802.15.4 and Zigbee. *IEEE Transactions on Consumer Electronics,* vol. 56, no. 3, pp. 1403 - 1410, (2010).

[15] The Internet of Things: Key Applications and Protocols Hardcover, Olivier Hersent et al. (2012).

[16] Roman Schlegel, Sebastian Obermeier, Johannes Schneider. : Assessing the Security of IEC 62351. *Journal of Information Security and Applications*, (2016).

[17] Euijong Lee, Young-DukSeo, Se-Ra Oh, and Young-Gab Kim. : Survey on Standards for Interoperability and Security in the Internet of Things. *IEEE Communications Surveys & Tutorials*, vol. 23, no. 12, pp. 1020 – 1047, (2021).

[18] Maria Stoyanova et al. : A Survey on the Internet of Things (IoT) Forensics: Challenges, Approaches, and Open Issues. *IEEE COMMUNICATIONS SURVEYS & TUTORIALS*, vol. 22, no. 2, pp. 1191– 1221, (2021).

[19] Z. Liu, F. Banakhr, G. Monte and V. Huang. : Using Algorithms on Smart Transducer: An IEEE Standard Perspective. *IEEE Sensors Journal*, vol. 15, no. 5, pp. 2523-2530, (2015).

[20] K. E. Martin et al. : IEEE Standard for Synchrophasors for Power Systems. *IEEE Transactions on Power Delivery*, vol. 13, no. 1, pp. 73-77, (1998).

[21] Dapeng Zhang, Xi Wang, Wenge Rong, Yu Yang. : China's practice of smart city standardisation and assessment," *IET SMART CITIES*, vol. 3, no. 4, pp. 211–218, (2021).

[22] Chai K. Toh. : Security for smart cities. *IET SMART CITIES*, vol. 2, no. 2, pp. 95–104, (2020).

[23] M.J.Mulquin.: Roles of IEC in supporting effective Smart City standards. *IET SMART CITIES*, vol. 1, no. 1, pp. 1–9, (2019).

[24] Sang, Z., Li, K. : ITU-T standardisation activities on smart sustainable cities. *IET Smart Cities*, vol. 1, no. 1, pp 3 - 9, (2019).

[25] Abdul rahaman Okino Otuoze,Mohd Wazir Mustafa,Olatunji Obalowu Mohammed, Muhammad Salman Saeed,Nazmat Toyin Surajudeen-Bakinde,Sani Salisu. Electricity theft detection by sources of threats for smart city planning. *IET SMART CITIES*, vol. 1, no. 2, pp. 52 – 60, (2019).

[26] Tanweer Alam. : Cloud-Based IoT Applications and Their Roles in Smart Cities. *Smart Cities*, vol. 4, no. 3, pp. 11960 - 1219, (2021).

[27] Abbas Shah Syed , Daniel Sierra-Sosa, Anup Kumar and Adel Elmaghraby. : IoT in Smart Cities: A Survey of Technologies, Practices and Challenges. *Smart Cities*, vol. 4, no. 3, pp. 429 - 475, (2021).

[28] Alkiviadis Giannakoulias. : Cloud computing security: protecting cloud-based smart city applications. *Journal of Smart Cities*, vol. 2, no. 1, pp. 66 - 77, (2017).

[29] Anton Kamenskih. : The analysis of security and privacy risks in smart education environments. *Journal of Smart Cities*, vol. 1, no. 1, pp. 17 - 29, (2022).

[30] Choenni, Sunil et al. "Data Governance in Smart Cities: Challenges and Solution Directions," *Journal of Smart Cities*, vol. 1, no. 1, pp. 31 - 51, 2022.

[31] Kashif Naseer Qureshi, Muhammad Najam ul Islam and Gwanggil Jeon. : A trust evaluation model for secure data aggregation in smart grids infrastructures for smart cities," *Journal of Ambient Intelligence and Smart Environments*, vol. 13, no. 3, pp. 235 - 252, (2021).

[32] Khan, Jalaluddin et al.: Efficient Secure Surveillance on Smart Healthcare IoT System through Cosine-transform Encryption. *Journal of Intelligent & Fuzzy Systems*, vol. 40, no. 1, pp.1 - 26, (2021).

[33] Eskhita, Radwan, Manda, Vijaya Kittu, Hlali, Arbia. : Dubai and Barcelona as Smart Cities: Some Reflections on Data Protection Law and Privacy. *Environmental Policy and Law*, vol. 51, no. 6, pp. 403 - 407, (2021).

[34] Harper, Scott, Mehrnezhad, Maryam, and Mace, John. User Privacy Concerns in Commercial Smart Buildings. *Journal of*

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 04 April 2026
Page No: 2079-2098
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0278

Computer Security, vol. 30, no. 3, pp. 465 - 497, (2021).

[35] José Joaquín Peralta Abadía, Christian Walther, Ammar Osman, Kay Smarsly. : A systematic survey of Internet of Things frameworks for smart city applications. *Sustainable Cities and Society*, vol. 83, pp. 1 - 19, (2022).

[36] Huiying Zhu,Liyin Shen,Yitian Ren. : How can smart city shape a happier life? The mechanism for developing a Happiness Driven Smart City. *Sustainable Cities and Society*, vol. 80, pp. 1 - 15, (2022).

[37] B D Deebak, Fida Hussain Memon, Xiaochun Cheng, Kapal Dev, Jia Hu, Sunder Ali Khowaja, Nawab Muhammad Faseeh Qureshi, Kyung Huyn Choi. : Seamless privacy-preservation and authentication framework for IoT-enabled smart eHealth systems," *Sustainable Cities and Society*, vol. 80, pp. 1 - 20, (2022).

[38] P. Muralidhara Rao, Fadi Al-Turjman, B.D. Deebak. : Smart grid metering: security, privacy, and open challenges. *Sustainable Networks in Smart Grid, Academic Press*, Chapter 11, pp. 255 - 272, (2022).

[39] Muralidhar Patruni, Deebak. : Security and privacy issues in smart cities/industries: technologies, applications, and challenges. *Journal of Ambient Intelligence and Humanized Computing*, pp. 1 - 20, (2022).

[40] B. D. Deebak, F. Al-Turjman, M. Aloqaily and O. Alfandi. : An Authentic-Based Privacy Preservation Protocol for Smart e-Healthcare Systems in IoT. *IEEE Access*, vol. 7, pp. 135632- 135649, (2019).

[41] Muhammad Adil , Muhammad Khurram Khan. : Emerging IoT Applications in Sustainable Smart Cities for COVID-19: Network Security and Data Preservation Challenges with Future Directions. *Sustainable Cities and Society*, vol. 75, pp. 1 - 12, (2021).

[42] White paper on Smart Cities in India: Framework for ICT Infrastructure, (2020). https://www.trai.gov.in/sites/default/files/White_Paper_22092020pdf.pdf

[43] ISO/IEC JTC 1/SC 27 Information Security and Privacy protection https://www.iso.org/committee/45306.html

[44] ISO/IEC 24760: Security techniques and framework for Identity management, (2011) https://www.iso.org/obp/ui/#iso:std:iso-iec:24760:-1:ed-1:v1:en

[45] ISO/IEC 27001: Information security management systems, (2013). https://www.iso.org/standard/54534.html

[46] Maria Stoyanova et al.: A Survey on the Internet of Things (IoT) Forensics: Challenges, Approaches, and Open Issues. *IEEE COMMUNICATIONS SURVEYS & TUTORIALS*, vol. 22, no. 2, pp. 1191–1221, (2021).

[47] ISO/IEC 27040:Security Techniques and Storage security, (2015). https://www.iso.org/standard/44404.html

[48] ISO/IEC 27017:Code of practice for Information security controls, (2015) https://www.iso.org/standard/43757.html

[49] ISO/IEC 27400:IoT privacy and security guidelines. https://www.iso.org/standard/44373.html

[50] ISO/IEC 22320:Security and resilience and guidelines for incident. (2018) https://www.iso.org/standard/67851.html

[51] ISO/IEC standards for privacy guidelines for smart cities. https://www.iso.org/standard/71678.html

[52] ISO/IEC standards for Health informatics Information security management in health. https://www.iso.org/standard/62777.html

[53] ISO/IEC standards for Security techniques - Privacy framework. https://www.iso.org/standard/45123.html

[54] ISO/IEC standards for Smart city business process framework. https://www.iso.org/standard/76371.html

[55] ISO/IEC standards for Guidelines on data exchange and sharing for smart community infrastructures. https://www.iso.org/standard/69242.html

[56] ISO/IEC standards for Code of practice for protection of personally identifiable information(PII) in public clouds acting as PII

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 04 April 2026
Page No: 2079-2098
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0278

processors. https://www.iso.org/standard/76559.html
[57] ISO/IEC standards for Information security, cyber security and privacy protection. https://www.iso27001security.com/html/27557.html
[58] ISO standard 15118. https://en.wikipedia.org/wiki/ISO_15118
[59] ISO standard for Interconnection of information technology equipment. https://www.iso.org/committee/45270.html
[60] ISO standard for ITS and assisted parking system. https://www.sis.se/api/document/preview/80000028/
[61] IEC TR 62541-2:2016 OPC unified architecture security model. https://webstore.iec.ch/publication/25996
[62] Eugene Y, Cuong, Avi. : Review of Smart Grid Standards for Testing and Certification Landscape Analysis https://www.govinfo.gov/content/pkg/GOVPUB-C13-07a38b2d2765d644a920888880b8101a.pdf
[63] Guidance on the identification and authentication of connectable Personal Healthcare Devices (PHDs). https://www.iso.org/obp/ui/#iso:std:73696:en
[64] ISO standards for Electronic health record communication" [Online] Available: https://www.iso.org/standard/50121.html
[65] ISO standards for Information security management for remote maintenance of medical devices and medical information systems. https://www.iso.org/standard/69336.html
[66] ISO standards for Security and privacy requirements of EHR systems for use in conformity assessment. https://www.iso.org/standard/61347.html
[67] ISO standards for Cloud computing considerations for the security and privacy of health information systems. https://www.iso.org/standard/70568.html
[68] ISO standards for Cloud Security requirements for archiving of electronic health records. https://www.iso.org/standard/44479.html
[69] ISO standards for Security requirements for archiving of electronic health records. https://www.iso.org/standard/44480.html
[70] ISO standards for Guidelines for security of cloud services. https://www.iso.org/standard/59689.html
[71] ISO standards for Governance of information security. https://www.iso.org/standard/74046.html
[72] IETF RFC 2898: Password-Based Cryptography Specification. https://datatracker.ietf.org/doc/html/rfc2898
[73] IETF RFC 4279: Pre - Shared Key Ciphersuites for Transport Layer Security. https://datatracker.ietf.org/doc/html/rfc4279
[74] IETF RFC 5755: An Internet Attribute Certificate Profile for Authorization. https://datatracker.ietf.org/doc/html/rfc5755
[75] IETF RFC 6655: AES – CCM Cipher Suites for Transport Layer Security. https://datatracker.ietf.org/doc/html/rfc6655
[76] IETF RFC 7250: Using Raw Public Keys in Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS). https://datatracker.ietf.org/doc/html/rfc7250
[77] IETF standards for architectural Considerations in Smart Object Networking https://datatracker.ietf.org/doc/html/rfc7452
[78] IETF standards Internet Protocols for the Smart Grid. https://tools.ietf.org/search/rfc6272
[79] IETF standards for Urban WSNs Routing Requirements in Low Power and Lossy Networks. https://datatracker.ietf.org/doc/html/draft-ietf-roll-urban-routing-reqs
[80] IETF standards for Manufacturer Usage Description Specification. https://datatracker.ietf.org/doc/html/rfc8520
[81] IETF standards for Home Automation Routing Requirements in Low Power and Lossy Networks. https://datatracker.ietf.org/doc/html/draft-ietf-roll-home-routing-reqs
[82] IETF standards Practical Considerations and

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 04 April 2026
Page No: 2079-2098
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0278

Implementation Experiences in Securing Smart Object Networks. https://www.rfc-editor.org/rfc/rfc8387

[83] IETF standards for Security Audit and Access Accountability Message XML Data Definitions for Healthcare Applications. https://datatracker.ietf.org/doc/html/rfc3881

[84] IETF standards for Applicability Statement for the Routing Protocol for Low-Power and Lossy Networks (RPL) in Advanced Metering Infrastructure (AMI) Networks. https://www.rfc- editor.org/rfc/rfc8036.html

[85] IETF standards for Secure Shell (SSH) Protocol Architecture. https://datatracker.ietf.org/doc/html/rfc4251

[86] IETF standards for Industrial Routing Requirements in Low-Power and Lossy Networks. https://www.rfc-editor.org/rfc/rfc5673

[87] IETF standards for Building Automation Routing Requirements in Low-Power and Lossy Networks. https://datatracker.ietf.org/doc/html/rfc5867

[88] IETF standards for Problem Statement and Requirements forIPv6 over Low-Power WirelessPersonal Area Network (6LoWPAN) Routing. https://www.rfc-editor.org/rfc/rfc6606

[89] IETF standards for Internet of Things (IoT) Security: State of the Art and Challenges. https://datatracker.ietf.org/doc/html/rfc8576

[90] IETF standards Guidelines for Writing RFC Text on Security Considerations. https://datatracker.ietf.org/doc/html/rfc3552

[91] IETF standards Privacy Considerations for Internet Protocols. https://datatracker.ietf.org/doc/html/rfc6973

[92] IETF standards on Vectors of Trust. https://datatracker.ietf.org/doc/html/rfc8485

[93] IETF standards on Opportunistic Security: Some Protection Most of the Time. https://datatracker.ietf.org/doc/html/rfc7435

[94] ITU-T X.205 Overview of Cyber security Standards. https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=9136

[95] ITU-TSG 20 Q6. Framework for IoT device authentication in smart city. https://www.itu.int/ITU-T/workprog/wp_search.aspx?sg=20&q=6

[96] ITU-T SG 20 Q4. Data analytics processing and management. https://rb.gy/5ohjmq

[97] ITU X.1311 Security framework for ubiquitous sensor network. https://www.itu.int/rec/T- REC-X.1311/en

[98] ITU-T Standard J.1612 : The architecture for a smart home gateway. https://www.itu.int/rec/T-REC-J.1612-202201-I

[99] ITU-T Standard X.1332:Securityguidelines for smart metering services in smart grids. https://www.itu.int/rec/T-REC-X.1332-202003-I/en

[100] ITU-T Standard for Security threats and requirements for digital payment services based on distributed ledger technology. https://www.itu.int/rec/T-REC-X.1405-202106-I

[101] Sang, Z., Li, K. : ITU-T standardisation activities on smart sustainable cities. *IET SmartCities*, vol. 1, no. 1, pp 3 - 9, (2019).

[102] ITU-T Standard for High-level requirements and reference framework of smart city platforms. https://www.itu.int/rec/T-REC-Y.4201-201802-I/en

[103] ITU-T Standard for Capability framework for e-health monitoring services. https://www.itu.int/rec/T-REC-Y.2075-201509-I/en

[104] ITU-T Standard for Requirements and functional architecture for smart parking lots insmart cities. https://www.itu.int/rec/T-REC-Y.4456-201803-I/en

[105] ITU-T Standard for Identifier service requirements for the interoperability of smart city applications. https://www.itu.int/rec/T-REC-Y.4805/en

[106] ITU-T Standard for Overviewof key performance indicators in smart sustainable cities. https://www.itu.int/itu-t/recommendations/rec.aspx?rec=12627&lang=en

[107] ITU-T Standard for Key performance indicators related to the use of information

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 04 April 2026
Page No: 2079-2098
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0278

technology in smart sustainable cities. https://standards.globalspec.com/std/10042160/itu-t-y- 4901

[108] ITU-T Standard for Y.4101: Common requirements and capabilities of a gateway for Internet of things applications. https://www.itu.int/rec/T-REC-Y.4101-201710-I/en

[109] ITU-T Standard for Smart sustainable cities – Setting the framework for an ICT architecture. https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-Y.Sup27-201601-I!!PDF-E&type=items

[110] ITU-T Standard Y.4550 series - Smart sustainable cities - Integrated management" [Online] Available. https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-Y.Sup28- 201601-I!!PDF-E&type=items

[111] ITU-T Standard for Y. Sup29 : ITU-T Y.4250 series - Smart Sustainable Cities - Multi-service infrastructure in new-development areas. https://www.itu.int/rec/T-REC-Y.Sup29/en

[112] ITU-TStandard Y.Sup31 : ITU-T Y.4550 series - Smart sustainable cities - Intelligent sustainable buildings. https://www.itu.int/rec/T-REC-Y.Sup31-201601-I/en

[113] ITU-TStandard Y.Sup32 : ITU-T Y.4000 series - Smart sustainable cities - A guide for city leaders. https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-Y.Sup32-202007-I!!PDF-E&type=items

[114] ITU-T technical report on Cyber security, data protection and cyber resilience in smart sustainable cities. https://www.itu.int/en/ITU-T/focusgroups/ssc/Pages/default.aspx

[115] Chun Sing Lai et al. : A Review of Technical Standards for Smart Cities. *Clean Technologies*, Vol 2 pp 290 - 310, MDPI, (2020).

[116] H. F. Badawi, F. Laamarti, and A. El Saddik. ISO/IEEE 11073 personal health device (X73-PHD) standards compliant systems: A systematic literature review. *IEEE Access*, vol. 7, pp. 3062 - 3073, (2019).

[117] IEEE P2834 Standard for Secure and Trusted Learning systems. https://sagroups.ieee.org/2834/

[118] Chun Sing Lai et al.: A Review ofTechnical Standards for Smart Cities. *Clean Technologies*, Vol 2 pp 290 - 310, MDPI, (2020). [119]1609.2 - 2016-IEEE Standard for Wireless Access in Vehicular Environments-Security Services for Applications and Management Messages, *IEEE Vehicular Technology Society*,(2016).

[119] IEEE Standard for Green Smart Home and Residential Quarter Control N/w Protocol. *IEEE Std 1888.4-2016*, vol., no., pp.1-32, 16, (2017).

[120] IEEE Guide for Smart Grid Interoperability of Energy Technology and Information Technology Operation with the Electric Power System (EPS), End-Use Applications, and Loads.*IEEE Std 2030-2011*, (2011).

[121] IEEE Draft Guide for Cyber security of Distributed Energy Resources Interconnected withElectric Power Systems. *P1547.3/D3.08*, vol., no., pp.1 - 155, (2022).

[122] IEEE Standard for AI model representation, compression, distribution, and management. *IEEE Std 2941-2021* , vol., no., pp.1-226, (2022).

[123] IEEE Standard for Broadband over Power Line Networks: Medium Access Control and Physical Layer Specifications -- Amendment 1: Enhancement for Internet of Things Applications. *IEEE Std 1901a-2019 (Amendment to IEEE Std 1901-2010)*, vol., no., pp.1-118, (2019).

[124] IEEE Standard for Blockchain-based Zero-Trust Framework for Internet of Things (IoT). https://standards.ieee.org/ieee/3219/10608/.

[125] IEEE Standard for Post-Quantum Network Security. https://standards.ieee.org/ieee/1943/10957/

[126] IEEE Standard for Trusted Environment Based Cryptographic Computing. https://standards.ieee.org/ieee/3181/10958/

[127] IEEE Standards for Smart Cities Terminology.

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 04 April 2026
Page No: 2079-2098
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0278

https://standards.ieee.org/ieee/3166/10938/
[128] IEEE Standards for Trusted Data Matrix System Architecture https://standards.ieee.org/ieee/3158/10881/
[129] IEEE Standard for Speech Recognition and Interaction System for Smart Home – Safety Requirements for Speech Control. https://standards.ieee.org/ieee/2899.2/10888/
[130] IEEE Standard for Recommended Practice for Physical Security of Electric Power Substations. https://standards.ieee.org/ieee/1402/10901/
[131] IEEE Standard for Wireless Diabetes Device Security Assurance Evaluation–Connected Electronic Product Security Evaluation Programs. https://standards.ieee.org/ieee/2621.1/10601/
[132] IEEE Standard for Requirements of Privacy-preserving Computation Integrated Platforms https://standards.ieee.org/ieee/3156/10834/
[133] IEEE Standard for Interworking Framework for Privacy-Preserving Computation https://standards.ieee.org/ieee/3117/10785/
[134] IEEE Guide for Categorizing Security Needs for Protection, Automation, and Control Related Data Files. https://standards.ieee.org/ieee/C37.249/10784/
[135] IEEE Standard for Data Processing and Compression Framework for Internet of Things. https://standards.ieee.org/ieee/3122/10748/
[136] IEEE Standard for Security Requirements and Testing Methods of Operating Systems in Connected Vehicles. https://standards.ieee.org/ieee/3130/10757/
[137] IEEE Standard for Recommended Practice for Secure Multi-Party Computation. https://standards.ieee.org/ieee/2842/7675/
[138] IEEE Standard for Technical Framework and Requirements of Trusted Execution Environment based Shared Machine Learning. https://standards.ieee.org/ieee/2830/10231/
[139] IEEE Standard for Open Mobile Health Data Representation of Metadata, Sleep, and Physical Activity Measures. https://standards.ieee.org/ieee/1752.1/6982/
[140] IEEE Standard for a Smart Transducer Interface for Sensors and Actuator -- Wireless Communication Protocols and Transducer Electronic Data Sheet (TEDS) Formats – LoRa Protocol. https://standards.ieee.org/ieee/1451.5.5/10611/
[141] IEEE Standard for a Smart Transducer Interface for Sensors and Actuator -- Wireless Communication Protocols and Transducer Electronic Data Sheet (TEDS) Formats – NB-IoT Protocol. https://standards.ieee.org/ieee/1451.5.10/10613/
[142] IEEE Standard for Recommended Practice for Privacy and Security for Federated Machine Learning. https://standards.ieee.org/ieee/2986/10564/.
[143] IEEE Standard for Recommended Practice for Common Framework of Location Services for Healthcare. https://standards.ieee.org/ieee/1847/10584/
[144] IEEE Standard for Trial Use Recommended Practice for Decentralized Clinical Trials Threat Modeling, Cybersecurity, and Data Privacy. https://standards.ieee.org/ieee/2968.2/10533/
[145] IEEE Standard for Technical Requirements and Evaluation Methods for Intelligent Levels of Smart Home Devices. https://standards.ieee.org/ieee/2951/10386/
[146] IEEE Standard for Secure Computing Based on Trusted Execution Environment https://standards.ieee.org/ieee/2952/10389/
[147] IEEE Draft Recommended Practice for Privacy Considerations for IEEE 802 Technologies. https://standards.ieee.org/ieee/802E/6242/
[148] IEEE Standard for Wireless Access in Vehicular Environments (WAVE) – Over-the-Air Electronic Payment Data Exchange Protocol for Intelligent Transportation Systems. https://standards.ieee.org/ieee/1609.11/4950/
[149] IEEE Standard for Wide-Block Encryption for Shared Storage Media. https://standards.ieee.org/ieee/1619.2/10252/

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 04 April 2026
Page No: 2079-2098
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0278

[150] IEEE Standard for Wireless Access in Vehicular Environments–Security Services for Applications and Management Messages. https://standards.ieee.org/ieee/1609.2/10258/
[151] IEEE Standard for Smart City Component Systems Discovery and Semantic Exchange of Objectives. https://standards.ieee.org/ieee/1951.1/10177/
[152] IEEE Standard for Architectural Framework and Technical Requirements for Smart Display System. https://standards.ieee.org/ieee/2868/10217/
[153] IEEE Standard for Privacy and Security Framework for Consumer Wireless Devices. https://standards.ieee.org/ieee/1912/10174/
[154] IEEE Standard for Communications Architectural Functional Framework for Smart Cities. https://standards.ieee.org/ieee/1950.1/10176/
[155] IEEE Standard for Clinical Internet of Things (IoT) Data and Device Interoperability with TIPPSS – Trust, Identity, Privacy, Protection, Safety, Security. https://www.embs.org/wp-content/uploads/2019/06/IEEE-P2733-Standard-Overview-June-11-2019.pdf
[156] IEEE Standard for Function Designations used in Electrical Power Systems for Cyber Services and Cyber security. https://standards.ieee.org/ieee/2808/7549/
[157] IEEE Standard for a Reference Architecture for Smart City (RASC) https://standards.ieee.org/ieee/2413.1/7331/
[158] IEEE Standard Cybersecurity Requirements for Power System Automation, Protection and Control Systems. https://standards.ieee.org/ieee/C37.240/7208/
[159] IEEE Guide for the Technology and Process Framework for Planning a Smart City. https://standards.ieee.org/ieee/2784/7138/
[160] IEEE Standard for Common Incident Management Message Sets for Use by Emergency Management Centers. https://standards.ieee.org/ieee/1512/3522/