Indonesian Journal of Computer Science
ISSN 2549-7286 (*online*)
Jln. Khatib Sulaiman Dalam No. 1, Padang, Indonesia
Website: ijcs.stmikindonesia.ac.id | E-mail: ijcs@stmikindonesia.ac.id

Exploring the Landscape of Smart Cities: A Comprehensive Review of IoT and Cyber-Physical Systems

Karwan M. Muheden, Prof. Dr. Shavan Askar, Mariwan Mohammed, Nura Jamal Bilal
karwan.muheden@epu.edu.iq, shavan.askar@epu.edu.iq
Information Systems Engineering Department, Erbil Technical Engineering College, Erbil Polytechnic University, Kurdistan, Iraq

Article Information

Submitted : 20 Mar 2024
Reviewed: 25 Mar 2024
Accepted : 8 Apr 2024

Keywords

Cyber Physical System, SDN, Snap4City, Internet of Things, Smart City

Abstract

- They focus on housing, well-being, equality, clean energy and fair conditions. The cyber-physical approach involves the development of IoT and Cyber-Things. Smart cities have a variety of use cases, including electricity and transportation. Automating is used for efficiency in industrial manufacturing. An integrated supply and demand side management system is required for the reliability, security and ability to manage the power grid. This paper introduces an integrated energy approach, enhances existing standards, and establishes a shared basis for multidisciplinary planning. It also introduces new semantic network ontologies to provide a comprehensive framework for solving resource-related challenges. This new approach aims to fill the gaps in current standards and create an integrated environment for multi-stakeholder collaboration, using a semantic web ontology for communication and improved decision making in energy systems Provides information integrated, including various forms of smart cities With flexibility for flexibility and inclusion in the energy industry, can accommodate the specific characteristics and needs of various smart city applications In this study, computing-physical system (CPS), software-defined network (SDN), internet of things (IoT).), and analyze how smart cities are connected. CPS combines physical channels with electronic systems to provide increased network management efficiency and flexibility. SDN improves dynamic capacity and flexibility, while IoT is more connected for real-time data exchange and decision-making.

A. Introduction

Cyber-Physical Systems (CPS) in IoT effectively combine computer algorithms and physical processes, creating a mutually beneficial connection between the digital and physical domains. This convergence enables the simultaneous monitoring, analysis, and control of physical things via linked networks, hence enhancing efficiency and responsiveness. Within the realm of the Internet of Things (IoT), Cyber-Physical Systems (CPS) go beyond simple connection by integrating advanced decision-making capabilities and the ability to operate autonomously [1]. By synergizing information technology with physical processes, CPS in IoT revolutionizes diverse domains such as healthcare, transportation, and industrial automation, ushering in a new era of interconnected smart systems that enhance overall functionality, adaptability, and innovation. cities worldwide are developing smart strategies to improve citizens' wellbeing, create economic development, and manage modern cities sustainably [2]. The Internet of Things (IoT) refers to the interconnectedness and interdependence of devices with integrated sensing, actuating, and communication capabilities. Technological developments like ATMs, WSNs, and M2M systems have made this possible. However, not all connected devices are IoT devices. The IoT signifies the ability of things to sense their surroundings and generate outcomes [3]. The most popular approach to using IoT data is a centralized processing: sensors send their data to a centralized or cloud-based server, where the results are analyzed and returned [4]. There are, however, drawbacks to this strategy as it involves connecting computers to the cloud directly, which is not cost-effective. Additionally, it needs plenty of storage and processing power from the computer. Second, sending all the data to a single cloud becomes impractical when computers proliferate exponentially in a specific location. With the exception of the unprocessed data, all of the raw data would be submitted to a centralized location [5]. a novel paradigm that incorporates the Internet of Things, and Big Data principles We not only show the basic components of an IoT scheme, but also the advantages of many other alternatives as well [3]. This IoT architecture strives to allow for maximum interoperability through using standards [6]. The Internet of Things (IoT) has enabled smart cities, managing infrastructure like energy, traffic, and water supplies. However, the reliability, accessibility, and uniformity of this data can impact individuals' lives. Cyber security is crucial for ensuring authentication and authorization, but lack of uniform standards is a concern [7]. IoT sensors and gadgets used within a residential setting. However, it is imperative to ensure the security of smart home networks to protect against potential security threats and attacks [8].

Cyber-Physical Systems (CPSs) offer new approaches in resource management, intelligent transportation systems, business, energy management, education, commerce, industries, smart manufacturing, and environmental monitoring, integrating smart computing and physical processes for future smart cities [9]. The Internet of Things (IoT) is transforming urban living by integrating devices into everyday objects and providing ample address space for sensors. Low-Power Wide Area Networks (LPWAN) products are widely deployed. SigFox and Semtech's LoRa technologies have gained interest and are widely deployed globally. Short-range IoT devices, like IEEE 802.15.4 or Bluetooth Low Energy

(BLE), support applications like smart homes, energy metering, and industrial automation. The introduction of 5G devices and services is generating anticipation in networking IoT technologies, as it is seen as a ground-breaking application in urban areas [10].

The Internet of Things (IoT) is transforming traditional infrastructure environments with smart objects, requiring security solutions at various levels. However, IoT technology has unique characteristics, including resource constraints and heterogeneous network protocol requirements. As a result, DDoS attacks are increasing, necessitating attention to address the consequences in the IoT industry [11]. "Instrumented" refers to the integration of live data from IoT devices, "interconnected" involves data exchange between services, and "intelligent" involves complex analysis, modeling, optimization, and visualization services [12]. IoT frameworks organize data processing among entities like devices, edges, and cloud processes. They may require IoT Applications to define user-component logic while hiding infrastructure complexity. These applications can manage open and private data, producing private results for some users [13].

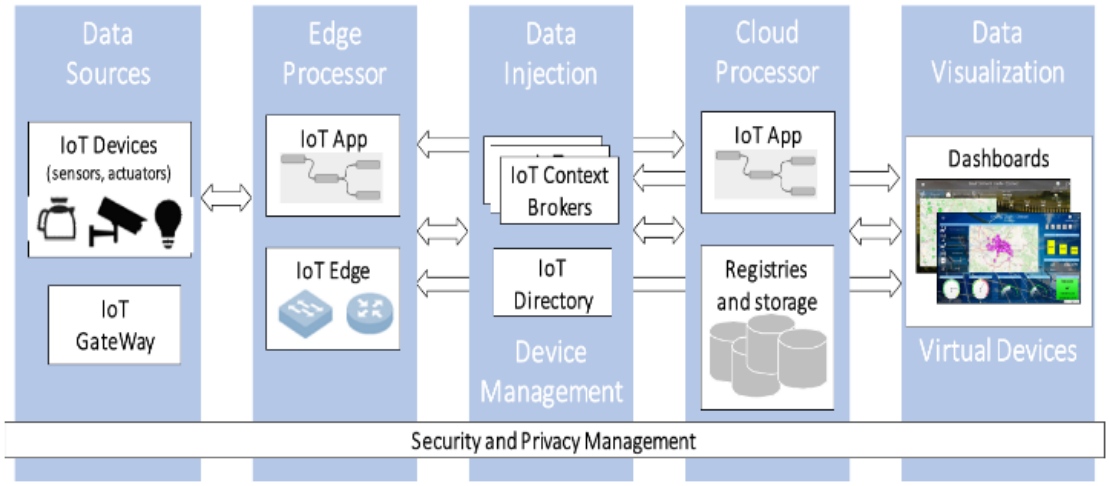

Figure 1. IoT platform general architecture.

B. Related Work or Smart City Overview

The Smart City IoT Platform should be accessible to developers, operators, and users with minimal computer programming and communication skills. However, navigating technical complexity while adhering to GDPR and data protection remains a challenge for various user categories. A system that is easy to use and understand is essential [14].

A. Smart Home Challenges

ensuring the security of communication between IoT devices within a smart home and mobile networks (MNs) is of utmost importance. Cloud computing enables the deployment of diverse platforms to facilitate this. Studies have mostly examined the security and privacy consequences of Internet of Things (IoT) devices in smart homes, specifically addressing issues such as confidentiality,

integrity, and access control [15]. Cloud-based platforms have the potential to serve as the fundamental infrastructure for future smart homes, offering dependable and effective services. Tao et al. introduced a multilayer cloud architecture to facilitate dependable communication among diverse IoT devices, presented a privacy and security framework for smart homes. emphasized the occurrence of cyber-attacks targeting smart home devices, with a specific focus on the VPN filter virus. Conducted a study on vulnerability assessment of smart houses that use Internet of Things (IoT) technology, as well as strategies to reduce the associated risks. Contemporary smart houses and their networks are susceptible to a range of threats, rendering one-way security improvements inadequate [16].

2.1 Distributed Ip Mobility Management

Centralized mobility management systems such as MIPv6 and PMIPv6 have disadvantages since they concentrate traffic on a single anchor point, which might result in network failure. The expansion of the network on the anchor can be restricted because to the exponential growth of signaling messages and data traffic. Transmission of data traffic through the anchor can result in suboptimal routing. In order to tackle these concerns, the IETF initiated the establishment of the Distributed IP Mobility Management Working Group in 2012. DMM decentralizes the functionality of the centralized anchor to enable independent network functions, thereby segregating the data plane from the control plane. The decentralization of this system offers increased flexibility, decreased overburden, and enhanced performance due to minimal communication delay. DMM is anticipated to establish itself as the prevailing benchmark for 5G/6G networks [8].

B. Route Optimization Security

The Static Shared Key (SSK) scheme was introduced in 2006 as a route optimization standard for MIPv6, the first IPv6 mobility management solution. However, the SSK scheme faces issues in key distribution and management, as each node must establish trust relations in advance with its associated CN. To address this, TBUA was proposed, a ticket-based binding renewal authentication protocol that employs HA as a ticket issuer. caTBUA was later enhanced using a context-aware authentication approach to balance security and efficiency [16].

The Return Route Ability (RR) scheme is included as a basic route optimization security option in MIPv6, but it has weaknesses in terms of security and performance. The Enhanced Route Optimization (ERO) scheme was proposed as an alternative, involving the exchange of binding management keys based on address-based public-key encryption schemes [17]. The ERO scheme efficiently executes route optimization based on the negotiated strong key, minimizing binding update latency. However, this creates a trade-off between performance and security [18].

In the smart home environment, the SSK scheme is necessary to establish a pre-trust relationship between the involved nodes. The SSK scheme assumes a shared secret is established between the nodes in advance, and an optimized binding update is executed based on the pre-shared key [8].

C. Smart Cities and TCPS

Smart cities utilize advanced technologies to create and execute intelligent solutions for promoting equitable development, optimizing community infrastructure, and fostering a sustainable environment. These solutions stimulate economic expansion by increasing infrastructure, generating employment opportunities, and boosting overall quality of life. Smart city applications depend on intelligent sensing, real-time monitoring, and decision-making. Consequently, future cities will increasingly rely on Central Processing Stations (CPSs) [19].

The Transport Cyber-Physical System (TCPS) is expected to undergo a significant transformation in future smart cities, particularly in the domain of transport. The correlation between the growth of urban structures, functionality, and prosperity is closely tied to the manner in which a city plans and constructs its mobility infrastructure [20]. Artificial intelligence has the potential to revolutionize transportation systems globally by effectively integrating large amounts of data, providing user-driven solutions, making real-time decisions, and utilizing machine learning to produce more advanced adaptive solutions [21].

D. Architecture for Internet of Things (IoT) in Smart Cities

Various architectures have been developed to stay abreast of the progress in smart city development. As far as we know, there is currently no standardized IoT architecture. Given that the main focus of this study is to provide a concise overview of security and privacy concerns in smart cities, the architectural framework presented here is derived from the widely recognized three-layer architecture and the commonly accepted design suggested in Figure 2 illustrates the architecture, which may be categorized into four distinct layers. A concise overview of each layer is shown below [22].

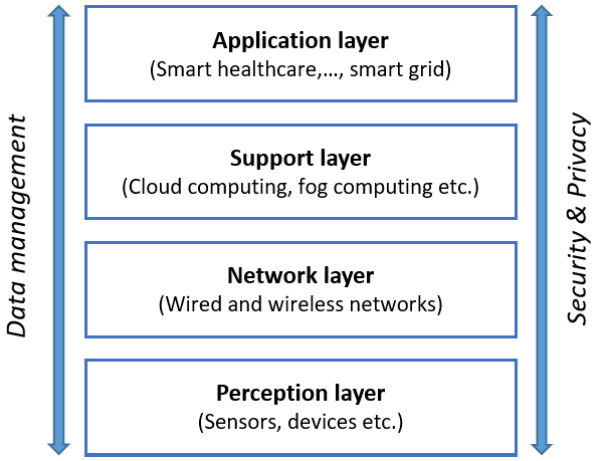

Figure 2. IoT-based architecture for a smart city.

Perception layer: The perception layer, also known as the sensing or recognition layer, collects real-world data from devices and transmits it to the network layer for further processing.

Network layer: The IoT core layer, reliant on basic networks like the Internet and WSNs, transmits data from the perception layer and connects smart things, devices, and servers.

Support layer: The application layer works in conjunction with advanced computing approaches such as cloud computing, edge computing, and fog computing to meet a wide range of application needs.

Application layer: The top layer is responsible for delivering intelligent and practical services or applications to users, tailored to their individual requirements. A comprehensive explanation is provided in the subsequent subsection.

E. SDN In Smart City Communication Infrastructures

Smart cities strive to incorporate a wide range of intelligent devices, applications, and systems into a unified setting. This includes integrating them into wearable devices, devices that enable action and automation, control systems in smart homes and buildings, and sensors integrated into vehicles to facilitate maintenance and prevent accidents. The gadgets, control systems, automation technologies, and network elements are integrated into a unified communication platform. Smart Data Networks (SDN) have played a crucial role in creating the concept of smart cities [12]. For example, He et al. introduced a service priority adaptive technique for managing emergency traffic in smart cities. Additionally, they developed an SDN-based solution that utilizes big data deep reinforcement learning to enhance mobile edge computing and caching in a smart city [23]. The popularity of SDN stems from its three distinct attributes: a logically centralized control plane that enables efficient global oversight and management, programmability that allows for on-site configuration, and virtualization that facilitates isolation and resource allocation among applications operating inside the same physical infrastructure [24].

F. DMM-based mobile networks

Cloud services in DMM-based mobile networks depend on the infrastructure designed for smooth mobility. During the first enrollment phase, the user's home gateway (HGW) plays a crucial role. Currently, the Home Gateway (HGW) enables a safe exchange of authentication and cipher keys, referred to as KHC and KEHC respectively, with the context mobility database (CMD) in DMM-based networks [8].

The exchange of keys is an important part of the registration process. It guarantees that the CMD contains the credentials and encryption keys necessary for successful authentication and communication with the user's home gateway. The use of KHC and KHC keys is generally used to establish a secure and reliable communication channel between the HGW and the CMD. The trust relationship is important for the future application of DMM-based mobile networks, especially in the context of navigation, handover and route efficiency [16].

Essentially, a shared key lays a foundation of trust between the user’s home door and the contextual navigation database, so secure key exchange is critical to preserving the integrity and confidentiality of the connection in the network improving the overall security and reliability of the DMM-based mobile network

infrastructure used. It lays the foundation for functionality and subsequent interaction between the user's device and the cloud service in a DMM environment [25].

C. TCPS Framework for Smart Cities

The TCPS (traffic control and parking system) framework for future smart cities provides a basic framework for the entire system, specifying the conceptual connections and connections between its modules This framework is a comprehensive toolkit for design, develop, implement and test the TCPS system in practical scenarios [19]. The interconnected modules address various challenges and efficiencies related to traffic management and control systems. These modules are driven by algorithms that filter heterogeneity, meet integrated standards, and feature different architectures, making them more flexible and efficient

Functional changes are packaged in different modules due to reliability and security issues [21]. The versatility of the TCPS system enables smart cities to address a wide range of situations and needs. The Framework provides a methodological framework for system architects and developers, presenting a comprehensive approach to designing, developing, and deploying TCPS systems to evaluate their performance in real-world applications information management [20].

The visual layout shown in Figure 3 is a visual example for stakeholders in implementing TCPS in smart cities [9]. The importance of transparent design definitions, algorithmic intelligence and scalable modules for developing robust and reliable TCPS systems for emerging urban environments has been emphasized [26].

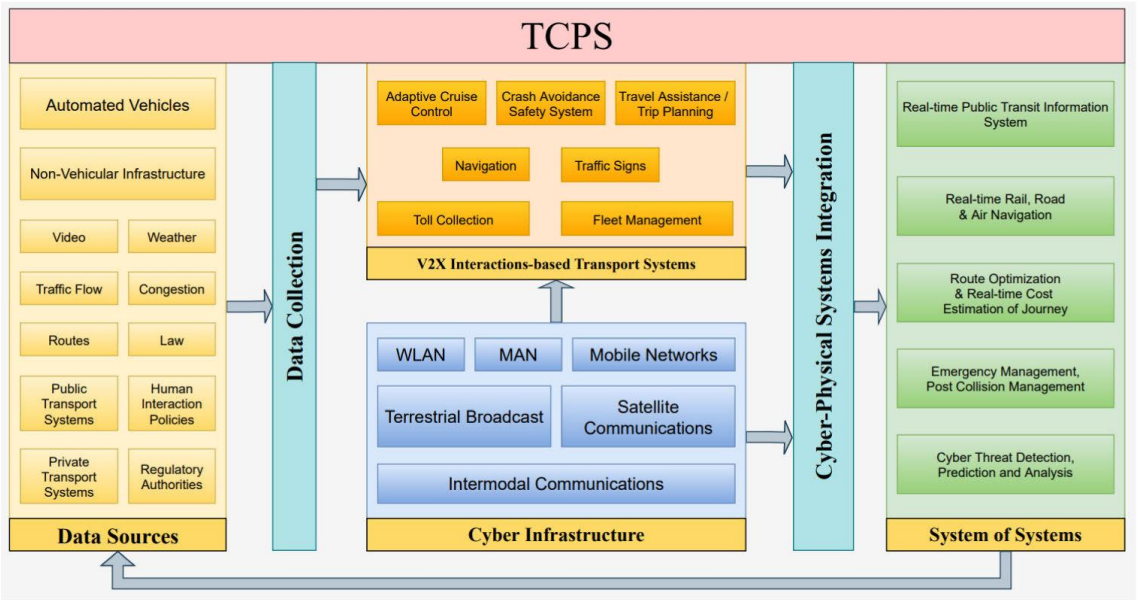

Figure 3. Suggested framework of TCPS for future smart cities.

A. Cryptographic algorithms They are essential in ensuring security and privacy for smart applications by preventing unauthorized access throughout the data life cycle. Conventional algorithms and encryption standards are unsuitable for devices with limited resources since they need significant processing power

and use a lot of energy. The use of lightweight encryption has become a fundamental need for using cryptographic technology in practical applications. In 2016, Mahmood [27] created a lightweight authentication solution for an Internet of Things (IoT) scenario that safeguards users' communications against Distributed Denial of Service (DDoS) assaults. Li et al. have recently introduced an innovative and efficient authentication mechanism designed to enhance the security of smart city applications.

Homomorphic encryption (HE) has garnered interest due to its capacity to link various services while safeguarding sensitive data. It may be used to safeguard the aggregation of power consumption in a smart grid system, provide privacy for healthcare monitoring, and address security concerns in cloud computing. Nevertheless, the approach is still limited by its significant computing cost. The concept of zero-knowledge proof was conceived by [28]. Allow one party to establish the fact or assertion without revealing further details [29]. applied zero-knowledge proofs to develop a very efficient authentication method for smart cards.

B. Blockchain technology However, the widely adopted and convenient nature of has sparked enough interest in recent years as it enables programs to be distributed [30]. Developed a blockchain-based security architecture that delivers secure communication in smart cities to improve the reliability and efficiency of systems [31]. Secrecy, Integrity and Availability have thus been ensured in a smart home environment using blockchain technology [32]. Used the blockchain architecture to address security issues associated with vehicle communication networks.

It is this use of blockchain, fog computing and software defined networking (SDN) technologies that makes possible a new distributed design based on principles such as resilience, efficiency; flexibility; scalability security etc.

C. Biometrics authentication is extensively used in IoT-based systems to identify people based on their distinct behavioral and biological traits. Biometric data may be obtained via fingerprints, facial features, vocal patterns, handwritten signatures, and other sources. Brainwave-based authentication is a prominent technique that achieves a high level of accuracy and efficiency. A key negotiation and mutual authentication system have been suggested to safeguard user information in storage devices, efficiently thwarting security threats while keeping communication costs and overhead at an acceptable level. Nevertheless, the incorrect utilization of bio-based techniques amplifies the likelihood of privacy breach. In order to tackle this issue, it is necessary to implement privacy-preserving biometric schemes (PPBSs), as proposed by [33]. Additionally, biometrics show great potential in e-business applications.

Table1. Examples a few instances of smart city security and privacy measures. [28]

Disciplines	Year	References	Applications scenario	Technologies
Cryptography	2017	[35]	Smart transportation	Two-level authentication key exchange scheme
	2016	[36]	Smart grid	Homomorphic encryption
	2017	[37]	Smart shopping	RFID
	2016	[38]	Smart card	Zero-knowledge proofs
Blockchain	2017	[39]	Smart home	Blockchain-based smart home architecture
	2017	[40]	Smart transportation	Network topology and decentralized blockchain-based framework
	2017	[49]	IoT architecture	Distributed architecture based on blockchain technique and fog computing
Biometrics	2016	[41]	Mobile sensors	Cascading bandpass filter for noise cancellation
	2017	[51]	Storage devices	Biometric based authentication and key negotiation protocol

D. Snap4city Platform Architecture

The Snap4City architecture is specifically developed to fulfill the demands of IoT domains, enabling implementation in various scenarios such as cloud, on premise, and mixed environments. It provides support for IoT edge devices running IoT applications, as well as IoT applications hosted on the cloud. Snap4City possesses the necessary flexibility to fulfill these requirements across a diverse array of IoT domains, allowing for both on-premise and cloud-based local processing, as well as a combination of the two. The system guarantees the confidentiality and security of the data it manages, in compliance with the GDPR, ENOLL, and Select4Cities regulations [34]. Snap4City.org functions as the cloud-based infrastructure of the system, serving as the foundation for gathering, analyzing, and presenting data through dashboards. Data produced by IoT applications can be reintegrated into storage and the knowledge base, rendering it accessible for microservices and dashboards. The subsequent paragraphs show various possibilities, assuming that all of them coexist simultaneously in real-world implementations.

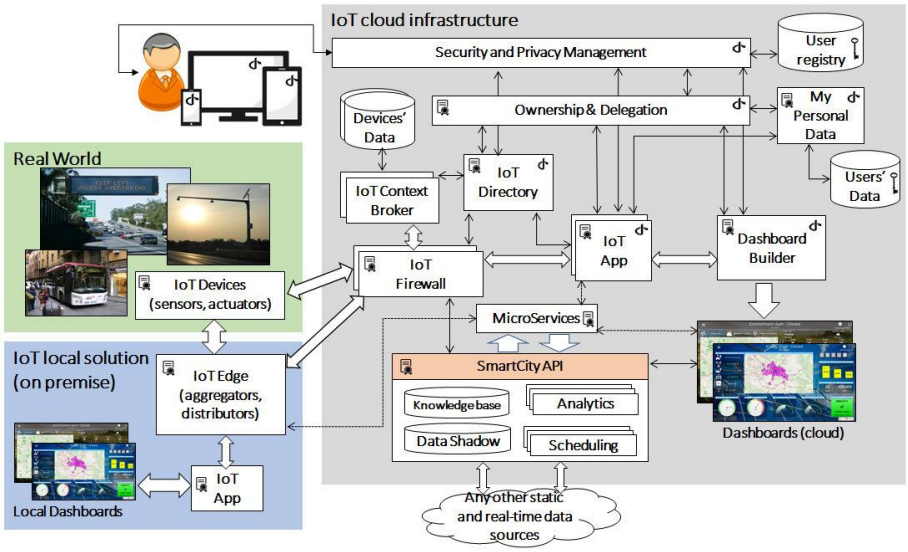

Figure 4. Snap4City architecture, main security aspects.

E. SDN Security in Smart City IOT

The Internet of Things (IoT) is a technology that facilitates the connection of network-enabled devices, including vehicles, lamps, and computers, regardless of their location or time. These items must have the capability to be identified, possess a distinct identifier, and establish a connection to the Internet [35]. The Internet of Things (IoT) ecosystems generate large volumes of data, which offer further advantages in many smart city applications, including industrial and home automation, automotive industry, intelligent energy management, smart grid control, and healthcare [36]. These smart apps and services can be advantageous for governments, people, and the industrial sector by offering quality of service (QoS) and streamlining administrative management overhead.

In order to create dependable, robust, and expandable smart cities, it is essential to have uncomplicated IoT ecosystems that provide a safe means of communication. Scalability and heterogeneity are two significant security problems in IoT infrastructure. Internet of Things (IoT) entities, such as mobile sensors, have limited resources and require an ecosystem that can facilitate and manage communication among billions of devices [37]. Additional security concerns, such as the administration of identities and the establishment of trust, must be resolved. The SDN framework provides a flexible and scalable network environment that can be used to solve IoT network design problems, in terms of scalability and heterogeneity researchers and service providers are increasingly interested in integrating SDN technologies into the IoT environment to increase flexibility especially through improving IoT bandwidth [12] [49-53].

F. Discussion

The summary table provides a detailed overview of various research contributions to Cyber-Physical Systems (CPS), Internet of Things (IoT), and Smart Cities Each entry contains specific objectives, approaches adopted, data types used, results, accuracy, and associated weaknesses or areas for improvement Notably, the authors jointly tackle a variety of important challenges related to security, privacy, scalability, and real-world applications in emerging technologies. The diverse spectrum of topics, from enhancing security in 5G-powered smart homes to investigating communication hotspots in smart cities, underscores the multidimensional nature of contemporary research endeavors. Despite varied methodologies, such as security testbed frameworks, behavioral power profiling, and conceptual framework analyses, common threads of ongoing refinement, scalability testing, and exploration of real-world implementation challenges emerge. The table serves as a valuable resource, offering a succinct comparative synthesis of key research contributions and paving the way for future endeavors that aim to fortify the foundations of CPS, IoT, and Smart City technologies.

Table2. Summarization of the Reviewed Studies

Authors	Objective	Method/Model Used/Dataset	Output and Accuracy	Weakness or Improvement
Daemin Shin (2019) [8]	Enhancing security in 5G-powered smart home networks	Distributed IP Mobility Management (DMM)	Secure route optimization protocol, verified for superiority	Potential vulnerability to security threats, requiring ongoing refinement and improvements
Amit Pundir (2022) [9]	Investigating the impact of Cyber-Physical Systems	Conceptual framework analysis, exploration of	Understanding CPS-enabled transportation	Susceptibility to cyber vulnerabilities, the need for

Authors	Objective	Method/Model Used/Dataset	Output and Accuracy	Weakness or Improvement
	(CPS) on smart city transport	connected vehicles	systems, paradigm shifts	effective model development in the domain
Lei Cui (2018) [28]	Assessing security and privacy challenges in smart cities	Survey methodology, overview of smart cities, identification of challenges	Overview of security and privacy issues, identification of requirements	Traditional cybersecurity strategies not directly applicable, call for novel solutions and exploration
Claudio Badii (2020) [10]	Introducing the Snap4City architecture for GDPR-compliant IoT in Smart Cities	Presentation of Snap4City architecture and security solutions	End-to-end secure solution, robustness in real-world scenarios	Addressing privacy and security aspects by design and default
Mohamed Rahouti (2020) [12]	Investigating the role of Software-Defined Networking (SDN) in smart cities	Comprehensive survey of SDN functionality, categorization of applications	Insights into SDN's role in secure communication infrastructure	The need for ongoing research to address evolving security threats and challenges
Akm Jahangir Alam Majumder (2020) [38]	Designing a CPS for security threat detection in IoT devices	Behavioral power profiling, statistical signal processing	Detection of potential security threats with high accuracy	Ongoing research needed for adapting to evolving IoT security landscape
Xiaofeng Hu (2020) [39]	Proposing a CPS framework for real-time monitoring and control in turbine assembly	Cyber-Physical Framework based on IoT, real-time data capture	Significantly improving quality and efficiency in turbine assembly	Implementation in large-scale assembly systems, scalability, and real-world application
Hirofumi Noguchi (2020) [40]	Introducing the concept of "Ephemeral-Cyber-Physical System (E-CPS)"	Proposal of E-CPS, optimization of actuator control for construction	Potential for dynamic adaptation in IoT networks	Potential challenges in real-world implementation and integration
Farhan Amin (2020) [41]	Analyzing communication hotspots in smart cities using big data and complex networks	Cyber-physical-social system model, graph construction and analysis	Identification and prioritization of high communication hotspot areas	Need for further validation and application in real-world urban planning
Arbab Waseem Abbas (2020) [42]	Emulating a scalable framework for Smart Logistics-based Cyber-Physical System	Development of IoT protocol stack, mathematical models for coverage	Enhanced network performance in smart logistics	Further validation and exploration in real-world logistics scenarios, scalability, and coverage improvements
Hao Peng (2020) [43]	Investigating the robustness of Cyber-Physical Systems (CPS)	Examination of CPS robustness, strategies for mitigating cascading failures	Enhancement of system reliability in interdependent networks	Optimization and customization based on different system structures
Shachar Siboni (2018) [44]	IoT device security testing	Security testbed framework	Detection of vulnerabilities and compromised IoT devices	-
Fariha Tasmin Jaigirdar (2023) [45].	Enhancing transparency and security in IoT systems	Integration of security metadata into provenance graph with predefined security policies	Greater transparency and security awareness, risk assessment	Evaluation under various real-world scenarios
Nader Mohamed (2020) [46]	Implementing data-driven security in smart cities	Data-driven security approaches	Enhanced security measures in smart city systems	Future research directions for effective integration
Aaesha Aldahmani (2023) [47]	Addressing security and privacy challenges in smart homes	Survey of smart home IoT security challenges	Identification of challenges and offered solutions	Emphasis on manufacturers' role in security
Dawei Wei (2021) [48]	Review of IoT dataflow management	Analysis of key challenges and overview of related techniques	Comparison of tools/platforms for IoT dataflow management	In-depth discussions and further study

G. Conclusion

In conclusion, the discussion reflects the evolving nature of research in smart systems, security, and communication infrastructure. There is a call for interdisciplinary collaboration, innovative solutions, and a cohesive understanding of the challenges posed by the integration of smart technologies in various domains. The future trajectory of this research field hinges on concerted efforts to

address these challenges and establish a secure foundation for the smart ecosystems of tomorrow.

The examined research papers collectively provide valuable insights into the complex landscape of smart systems, security, and communication infrastructure. The emphasis on securing smart systems, as highlighted in studies on smart home networks, transportation domains, and smart cities, underscores the critical role of robust security measures in ensuring the integrity and privacy of interconnected devices and services. The challenges of computer-physical systems (CPS), as discussed by various authors, shed light on the complexity of facilitating the integration of physical and digital resources the weaknesses identified in transportation CPS are the need for effective modeling and planning Secure and flexible planning for smart cities -reveals ongoing conceptual challenges in manufacturing

The specific focus on secure network infrastructure, especially in the case of software-defined networks (SDN), emphasizes the importance of tailoring solutions to the unique requirements of smart city applications. Throughout the research there is a clear call for comprehensive and integrated solutions. While the proposed security measures and policies are valuable, the lack of specific solutions to some challenges suggests the need for standardized actions and concerted efforts to address common vulnerabilities role, and the need for detailed comparative studies highlights the ongoing work needed to strengthen intelligent ecosystems against potential threats.

H. References

[1]. Li, Y., Lin, Y., & Geertman, S. (2015, July). The development of smart cities in China. In Proc. of the 14th International Conference on Computers in Urban Planning and Urban Management (pp. 7-10).

[2]. Zhang, K., Ni, J., Yang, K., Liang, X., Ren, J., & Shen, X. S. (2017). Security and privacy in smart city applications: Challenges and solutions. IEEE Communications Magazine, 55(1), 122-129.

[3]. Samann, F. E. F., Zeebaree, S. R., & Askar, S. (2021). IoT provisioning QoS based on cloud and fog computing. Journal of Applied Science and Technology Trends, 2(01), 29-40.

[4]. Cabrera, C., White, G., Palade, A., & Clarke, S. (2018). The Right Service at the Right Place: A Service Model for Smart Cities. 2018 IEEE International Conference on Pervasive Computing and Communications (PerCom), 1–10.

[5]. Ahmed, K. D., & Askar, S. (2021). Deep learning models for cyber security in IoT networks: A review. International Journal of Science and Business, 5(3), 61-70.

[6]. Abid, T., Zarzour, H., Laouar, M. R., & Khadir, M. T. (2016). Towards a smart city ontology. 2016 IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA), 1–6. https://doi.org/10.1109/AICCSA.2016.7945823.

[7]. Elsaeidy, A. A., Jamalipour, A., & Munasinghe, K. S. (2021). A hybrid deep learning approach for replay and DDoS attack detection in a smart city. IEEE Access, 9, 154864-154875.

[8]. Shin, D., Yun, K., Kim, J., Astillo, P. V., Kim, J. N., & You, I. (2019). A security protocol for route optimization in DMM-based smart home IoT networks. IEEE Access, 7, 142531-142550.
[9]. Pundir, A., Singh, S., Kumar, M., Bafila, A., & Saxena, G. J. (2022). Cyber-physical systems enabled transport networks in smart cities: Challenges and enabling technologies of the new mobility era. IEEE Access, 10, 16350-16364.
[10]. Badii, C., Bellini, P., Difino, A., & Nesi, P. (2020). Smart city IoT platform respecting GDPR privacy and security aspects. IEEE Access, 8, 23601-23623.
[11]. Bhayo, J., Hameed, S., & Shah, S. A. (2020). An efficient counter-based DDoS attack detection framework leveraging software defined IoT (SD-IoT). IEEE Access, 8, 221612-221631.
[12]. Rahouti, M., Xiong, K., & Xin, Y. (2020). Secure software-defined networking communication systems for smart cities: Current status, challenges, and trends. IEEE Access, 9, 12083-12113.
[13]. Li, S., Da Xu, L., & Zhao, S. (2018). 5G Internet of Things: A survey. Journal of Industrial Information Integration, 10, 1-9.
[14]. Voas, J., Kuhn, R., Kolias, C., Stavrou, A., & Kambourakis, G. (2018). Cybertrust in the IoT age. Computer, 51(7), 12-15.
[15]. Rahman, M. S., Basu, A., Nakamura, T., Takasaki, H., & Kiyomoto, S. (2018). PPM: Privacy Policy Manager for Home Energy Management System. J. Wirel. Mob. Networks Ubiquitous Comput. Dependable Appl., 9(2), 42-56.
[16]. Chifor, B. C., Bica, I., Patriciu, V. V., & Pop, F. (2018). A security authorization scheme for smart home Internet of Things devices. Future Generation Computer Systems, 86, 740-749.
[17]. H. Yang and Y. Kim, (2016), Routing Optimization with SDN, document, IETF Internet-Draft. [Online]. Available: https://tools.ietf.org/html/draftyang-dmm-sdn-dmm-05
[18]. Shin, D., Sharma, V., Kim, J., Kwon, S., & You, I. (2017). Secure and efficient protocol for route optimization in PMIPv6-based smart home IoT networks. IEEE Access, 5, 11100-11117.
[19]. Törngren, M., Asplund, F., Bensalem, S., McDermid, J., Passerone, R., Pfeifer, H., ... & Schätz, B. (2017). Characterization, analysis, and recommendations for exploiting the opportunities of cyber-physical systems. In Cyber-physical systems (pp. 3-14). Academic Press.
[20]. Hou, R., Jeong, S., Lynch, J. P., & Law, K. H. (2020). Cyber-physical system architecture for automating the mapping of truck loads to bridge behavior using computer vision in connected highway corridors. Transportation research part c: emerging technologies, 111, 547-571.
[21]. Gifty, R., Bharathi, R., & Krishnakumar, P. (2019). Privacy and security of big data in cyber physical systems using Weibull distribution-based intrusion detection. Neural Computing and Applications, 31(Suppl 1), 23-34.
[22]. Yaqoob, I., Ahmed, E., Hashem, I. A. T., Ahmed, A. I. A., Gani, A., Imran, M., & Guizani, M. (2017). Internet of things architecture: Recent advances, taxonomy, requirements, and open challenges. IEEE wireless communications, 24(3), 10-16.

[23]. Nguyen, T. H., & Yoo, M. (2017, January). Analysis of link discovery service attacks in SDN controller. In 2017 International Conference on Information Networking (ICOIN) (pp. 259-261). IEEE.
[24]. Askar, S. (2017). SDN-Based Load Balancing Scheme for Fat-Tree Data Center Networks. Al-Nahrain Journal for Engineering Sciences (NJES), Vol.20, No.5, pp.1047-1056.
[25]. S. Gundavelli, K. Leung, V. Devarapalli, K. Chowdhury, and B. Patil,Proxy Mobile IPv6, document IETF RFC 5213, 2008. [Online]. Available: https://tools.ietf.org/html/rfc5213.
[26]. Elshenawy, M., Abdulhai, B., & El-Darieby, M. (2018). Towards a service-oriented cyber–physical systems of systems for smart city mobility applications. Future Generation Computer Systems, 79, 575-587.
[27]. Mahmood, Z., Ning, H., & Ghafoor, A. (2016, December). Lightweight two-level session key management for end user authentication in Internet of Things. In 2016 IEEE international conference on internet of things (iThings) and IEEE Green computing and communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData) (pp. 323-327). IEEE.
[28]. Cui, L., Xie, G., Qu, Y., Gao, L., & Yang, Y. (2018). Security and privacy in smart cities: Challenges and opportunities. IEEE access, 6, 46134-46145.
[29]. Dousti, M. S., & Jalili, R. (2016). An efficient statistical zero-knowledge authentication protocol for smart cards. International Journal of Computer Mathematics, 93(3), 453-481.
[30]. Biswas, K., & Muthukkumarasamy, V. (2016, December). Securing smart cities using blockchain technology. In 2016 IEEE 18th international conference on high performance computing and communications; IEEE 14th international conference on smart city; IEEE 2nd international conference on data science and systems (HPCC/SmartCity/DSS) (pp. 1392-1393). IEEE.
[31]. Dorri, A., Kanhere, S. S., Jurdak, R., & Gauravaram, P. (2017, March). Blockchain for IoT security and privacy: The case study of a smart home. In 2017 IEEE international conference on pervasive computing and communications workshops (PerCom workshops) (pp. 618-623). IEEE.
[32]. I.S. Abdulkhaleq and S. Askar, 2021, "Evaluating the impact of network latency on the safety of blockchain transactions," Int. J. Sci. Bus., vol. 5, no. 3, pp. 71–82, doi: 10.5281/zenodo.4497512.
[33]. Natgunanathan, I., Mehmood, A., Xiang, Y., Beliakov, G., & Yearwood, J. (2016). Protection of privacy in biometric data. IEEE access, 4, 880-892.
[34]. Torres, D., Dias, J. P., Restivo, A., & Ferreira, H. S. (2020, September). Real-time feedback in node-red for iot development: An empirical study. In 2020 IEEE/ACM 24th International Symposium on Distributed Simulation and Real Time Applications (DS-RT) (pp. 1-8). IEEE.
[35]. Ali, K., & Askar, S. (2021). Security Issues and vulnerability of IoT devices. International Journal of Science and Business, 5(3), 101-115.
[36]. Hamad, Z. J., & Askar, S. (2021). Machine Learning Powered IoT for Smart Applications. International Journal of Science and Business, 5(3), 92-100.
[37]. Qadir, G. A., & Askar, S. (2021). Software defined network based vanet. International Journal of Science and Business, 5(3), 83-91.

[38]. Majumder, A. J. A., Veilleux, C. B., & Miller, J. D. (2020). A cyber-physical system to detect IoT security threats of a smart home heterogeneous wireless sensor node. IEEE Access, 8, 205989-206002.
[39]. Hu, X., Wan, J., Wang, T., & Zhang, Y. (2020). An IoT-based cyber-physical framework for turbine assembly systems. IEEE Access, 8, 59732-59740.
[40]. Noguchi, H., & Sugano, S. (2020). Ephemeral-cyber-physical system: a cloud-like CPS using shared devices in open IoT. IEEE Systems Journal, 14(4), 5176-5186.
[41]. Amin, F., & Choi, G. S. (2020). Hotspots analysis using cyber-physical-social system for a smart city. IEEE access, 8, 122197-122209.
[42]. Abbas, A. W., & Marwat, S. N. K. (2020). Scalable emulated framework for IoT devices in smart logistics based cyber-physical systems: bonded coverage and connectivity analysis. IEEE Access, 8, 138350-138372.
[43]. Peng, H., Liu, C., Zhao, D., Ye, H., Fang, Z., & Wang, W. (2020). Security analysis of CPS systems under different swapping strategies in IoT environments. IEEE Access, 8, 63567-63576.
[44]. Siboni, S., Sachidananda, V., Meidan, Y., Bohadana, M., Mathov, Y., Bhairav, S., ... & Elovici, Y. (2018). Security testbed for Internet-of-Things devices. IEEE transactions on reliability, 68(1), 23-44.
[45]. Jaigirdar, F. T., Tan, B., Rudolph, C., & Bain, C. (2023). Security-aware Provenance for Transparency in IoT Data Propagation. IEEE Access.
[46]. Mohamed, N., Al-Jaroodi, J., Jawhar, I., & Kesserwan, N. (2020). Data-driven security for smart city systems: Carving a trail. IEEE Access, 8, 147211-147230.
[47]. Aldahmani, A., Ouni, B., Lestable, T., & Debbah, M. (2023). Cyber-security of embedded IoTs in smart homes: challenges, requirements, countermeasures, and trends. IEEE Open Journal of Vehicular Technology, 4, 281-292.
[48]. Wei, D., Ning, H., Shi, F., Wan, Y., Xu, J., Yang, S., & Zhu, L. (2021). Dataflow management in the internet of things: Sensing, control, and security. Tsinghua Science and Technology, 26(6), 918-930.
[49] Nafees Zaman; Ahmad Abu Saiid; Md Arafatur Rahman; Shavan Askar; Jasni Mohamad Zain , “A Data-Intelligent Scheme Toward Smart Rescue and Micro-Services”, IEEE Access Volume 11, 2023.
[50] Omar Shirko; Shavan Askar , “A Novel Security Survival Model for Quantum Key Distribution Networks Enabled by Software-Defined Networking” IEEE Access, Volume 11, 2023.
[51] Baydaa Hassan Husain & Shavan Askar, 2021. "Survey on Edge Computing Security," International Journal of Science and Business, IJSAB International, vol. 5(3), pages 52-60.
[52] Chnar Mustaf Mohammed & Shavan Askar, 2021. "Machine Learning for IoT HealthCare Applications: A Review," International Journal of Science and Business, IJSAB International, vol. 5(3), pages 42-51.
[53] Shavan Askar & Chnar Mustaf Mohammed & Shahab Wahhab Kareem, 2021. "Deep Learning in IoT systems: A Review," International Journal of Science and Business, IJSAB International, vol. 5(6), pages 131-147.