Journal of Information Systems and Telecommunication
Vol.13, No.1, January-March 2025, 33-49
http://jist.acecr.org
ISSN 2322-1437 / EISSN:2345-2773

Review on Architecture and Challenges in Smart Cities

Mehdi Azadimotlagh [1*], Narges Jafari [2], Reza Sharafdini [3]

[1]. Department of Computer Engineering of Jam, Persian Gulf University, Jam, Iran
[2]. Department of Computer Engineering, Amirkabir University of Technology, Tehran, Iran
[3]. Department of Mathematics, Persian Gulf University, Bushehr, Iran

Received: 25 Oct 2024/ Revised: 04 Mar 2025/ Accepted: 05 Apr 2025

Abstract

Due to rapid urbanization, a balance between resources and urban growth is required. For the achievement of this equilibrium, the use of information technologies is essential. Smart cities are the answer to this requirement, as a result, they improve various aspects of urban life and address related challenges and/or mitigate them. Modern technologies, including a wide range of Internet of Things (IoT) sensors, are used in smart cities for collecting and analyzing data on different aspects of urban life to enhance their inhabitants' lives. Smart cities improve the sustainability and efficiency of urban dynamics. Today, smart cities can enhance services and citizens' lives in various fields such as governance, education, healthcare, transportation, and energy. Smart city applications require collaboration among individuals from various disciplines, including engineering, architecture, urban design, and economics, to plan, design, implement, and deploy a smart solution for a specific task. Therefore, a proper understanding of the applications and architecture of smart cities and the challenges they face is crucial. In this paper, we will provide background information about the applications of smart cities, describe the architecture of applications in smart cities, present security and privacy challenges to examine robustness and flexibility in smart city applications, and examine new trends in this field.

Keywords: Urban Growth; Internet of Things; Smart Utilities; Infrastructure Implementation; Security.

1- Introduction

A set of economic, environmental, and social factors has a significant impact on rapid urbanization. Therefore, economic, environmental, and social sustainability are essential to balance rapid urbanization with cities' resources. Modern technologies can improve the financial, environmental, and social aspects of urban life simultaneously, helping to overcome related challenges or mitigate them. As a result, rapid urbanization is one of the most important factors in the development of intelligent infrastructure, accelerating the need for smart cities and smart spaces [1-6].

Smart cities combine information, connectivity, and sophisticated sensors to manage municipal assets, allowing information to be sent in real time by using Internet of Things (IoT) sensors and network infrastructures. Smart city systems aim for a seamless and secure interconnection of sensors, actuators, and data processing resources to ensure efficient and reliable digital services [7-9].

Technological advances like cloud computing systems, digital devices, networks, sensor systems, and artificial intelligence (AI) capabilities are used by smart city architects to allow the elements of smart cities to coordinate and communicate with the routing protocol. In the coming years, smart cities will experience significant development, particularly in consumer, industry, and public services fields. The key goal of most of these fields is to focus on human comfort in smart homes and buildings, along with smart transportation, healthcare, education, etc. It is crucial to pay attention to security and privacy issues to achieve robustness and resilience in smart city infrastructures [5, 9-11].

This paper is organized as follows:

Section 2 provides background information on various applications of smart cities, offering in-depth insights into the technology's user-centric aspects.

Section 3 describes the architecture and implementation of smart city technology. The four-plane and five-plane

✉ **Mehdi Azadimotlagh**
m.azadim@pgu.ac.ir

architectures are introduced, followed by a detailed discussion of the latest architectural model: the six-plane architecture. Key implementation standards for each plane of this model are also outlined.
Section 4 explores the challenges of implementing smart city applications. These challenges are examined in detail across four categories: security, data management, infrastructure, and cyberattacks. At the end of this section, the role of artificial intelligence in addressing cyberattacks in smart cities is analyzed.
In the final section, an indicator for assessing the progress and comparison of smart cities is presented. An economic analysis of the necessity of transitioning toward smart cities is provided, and the section concludes by introducing the most important emerging trends for future research in the field..

2- Applications and Advantages

Intelligent cities improve the sustainability and efficiency of urban dynamics. Smart city services encompass a wide range of applications, from smart utilities to smart health, smart transportation, smart governance, and smart environment, utilizing real-time sensing, knowledge engineering, and presentation of analyzed data in an understandable format [2,7].
In the following, we review some key smart city applications like governance [12-16], home and building [8,17-20], public services [21-25], education [9,11,26-31], healthcare [32-38], business management [39-42], transportation [43-51], electricity and energy [8,17,33], clean and sustainable environment [52-55], surveillance [56-59], defense [60-63], agriculture [64-67], water management [68-69], crime tracking and detection [70-73], tourism [74-77], entertainment [1,78,79], etc.

2-1- Smart governance

For cities to become smart, we need standard frameworks and procedures for integrating technology, citizens, and governments. Smart governance, as the intelligent use of ICT to improve decision-making through better collaboration among different stakeholders, including government and citizens, can be strongly related to government approaches. Smart governance requires complex interactions between governments, citizens, and other stakeholders. Transparency, collaboration, participation, partnership, communication, and accountability are important smart governance factors that impact the quality of life in the context of smart cities. ICT-based tools, such as social media, and openness can be factors that increase citizen engagement and support smart government [14-16].

2-2- Smart Home and Smart Building

A smart environment can acquire and apply knowledge about its occupants and their surroundings for adaption to the occupants and meet comfort and efficiency goals. Smart homes and smart buildings are two representative applications within the smart environment that use an ensemble of sensors and actuators installed in homes to improve energy consumption, promote healthy lifestyles, ensure security, etc., which inevitably ties smart homes with other smart city applications such as smart grid and smart healthcare. Aside from their many advantages, smart homes are sometimes perceived by citizens as an invasion of their privacy and security [17-20,80].

2-3- Smart Public Services

The fundamental organizational framework of the intelligent city includes advances in communications, data analytics, IoT development, and a range of physical infrastructures for smart operations management. Smart cities provide many advantages to enhance the safety of the public, such as linked surveillance systems, smart roads and transportation, public safety monitoring, education, healthcare, crime tracking and detection, etc. [4,25].

2-4- Smart Education

Smart education utilizing AI has numerous potential applications, such as grading and evaluating students, predicting student retention and dropout rates, conducting sentiment analysis, providing intelligent tutoring, and monitoring and recommending systems for classrooms. Smart education in a smart city has education-hard problems and education-soft problems and ways to resolve them. The hard problems are the management of education with technology to optimize or monitor in real-time by the IoT technology the physical infrastructure, aspects related to the institutions of higher education as strategies for teaching and learning, high-tech services, the interaction between student-professor, and the design and development of multimedia contents for learning. The soft problems are the educational problems that handle information inaccurate or incomplete, with uncertainty and ambiguity, being ambiguous, volatile, poorly understood, and dynamic (education public policy, administration, decision-making, educational reforms) [11,26,29].

2-5- Smart Healthcare

In response to challenges such as population aging and the widespread outbreak of chronic diseases such as diabetes and obesity, a wide variety of smart healthcare applications employ sensing technologies with different characteristics

suitable to provide personalized and continuous monitoring. Recent technological advancements have made medical sensing possible for patients in their homes and offices. Smart healthcare systems can automatically monitor and track patients, personnel, and biomedical devices within hospitals and improve workflow efficiency in hospitals. Also, they can monitor the spread of diseases by healthcare institutions and people's reactions to environmental factors, such as pollution [9,33,34]. The conceptual system for real-time remote cardiac health monitoring proposed in [36] has reduced healthcare costs while increasing diagnostic accuracy.

2-6- Smart Business Management

Organizations across industries are increasingly utilizing AI systems to enhance their innovation processes, supply chains, marketing and sales, and other business functions. Through the implementation of AI, firms have reported efficiency gains from automation and improved decision-making due to more relevant, accurate, and timely predictions. Alibaba, one of the largest retail commerce companies in the world, provides the fundamental technology infrastructure and marketing reach to engage with its users, customers, and business partners [39-42].

2-7- Smart Transportation

By developing cities and increasing population, smart transportation has become an essential component of modern societies. Smart transportation establishes connectivity among vehicles, citizens, and infrastructure to improve road safety, reduce traffic, and increase fuel efficiency. The main motivation for developing smart transportation is to help improve the traffic flow of cities for people who want a shorter time for their daily trips. Also, smart transportation can protect pedestrians while walking in the streets or crossing the roads. For this purpose, traffic sensors are also used to detect and track pedestrian behavior [44-46, 49-51].

2-8- Smart Electricity and Energy

Given the urgent need for energy development in cities and the challenges of energy supply sources, it is crucial to address these issues. Monitoring and control programs, energy harvesting, and innovative measurement methods through smart devices are becoming increasingly important. Smart grids are revolutionizing existing electricity distribution systems due to the growing demand for energy and the expansion of new and innovative information and communication technologies (ICT), especially from an economic perspective [17] [81].

2-9- Clean and Sustainable Environment

Humanity is currently facing immense challenges related to Air pollution mitigating environmental impacts and also reduction of CO2 emissions. Traditional methods to monitor air quality are complex and costly. IoT-based pollution control systems are real-time and more precise, using faster, more cost-effective, and modern technology devices. The processing of images and AI-based systems of the IoT could lead to a major evolution in the clean energy production sector [53-55].

2-10- Smart Surveillance

The purpose of smart surveillance is to monitor people, homes, industries, offices, etc. in the absence of the user using IoT-based security surveillance systems. A great example of smart surveillance is the NATO big project namely WITNESS, which includes wide integration of sensor networks [56,57,59,82,83].

2-11- Smart Defense

Smart defense is all about creating security at a lower cost through collaboration and increased flexibility. In this approach, countries form smaller groups to pool their resources and develop capabilities that can benefit the entire alliance. Smart defense systems incorporate cutting-edge sensors, weapon systems, command and control elements, and decision-making tools to safeguard a nation against a wide range of threats. Additionally, smart cyber defense is centered on protecting against cyberattacks originating in cyberspace and enhancing defense strategies [60,62,84].

2-12- Smart Crime Tracking and Detection

Recently, information and communication technologies have been used to track and monitor crime and criminal activities in real-time online to reduce the crime rate. An IoT-based detection and tracking of criminals system aims to enable communication and collaboration between citizens and police forces in the criminal investigation process by using IoT technologies and local data computation; and distribution, along with information sharing. Using new sensors to detect criminal behavior and identify individual perpetrators; leads to deterrence and crime prevention [70,72,73].

2-13- Smart Water Management

Water quality management has gained utmost importance due to increasing pollution levels caused by industrial growth. Hence, it is essential to address the smart utilization of water resources, both from the quantity and quality perspectives [68,69].

2-14- Smart Agriculture

By utilizing the IoT and big data solutions, agricultural lands can be automatically managed, tracked, and improved in terms of operational efficiency and productivity with minimal human intervention. Generally, IoT applications for smart agriculture can be classified into seven categories; including smart monitoring, smart water management, agrochemical applications, disease management, smart harvesting, supply chain management, and smart agricultural practices [65-67].

2-15- Smart Tourism and Entertainment

Smart tourism involves the integration of innovation and information technology with tourism applications and urban infrastructure to provide solutions to tourists to meet specific travel-related needs. For example, Dubai has implemented a smart city and smart tourism platforms to interact with various stakeholders. Also, new technologies provide a framework for creating entertainment and augmented reality systems, using cloud-based technologies and real-time mobile technology interaction in various contexts [74,75,77,79].

2-16- AI-Based Smart City Applications

In a smart city application, AI techniques aim to process and identify patterns in data obtained from individual sensors or collective data generated by several sensors and provide useful insights on how to optimize underlying services. Explainable AI is particularly important in some key applications of smart cities, such as healthcare, transportation, banking, and other financial services. For instance, in transportation, AI could be used to analyze data collected from different parts of a city for future planning or deploying different transportation schemes in the city. The basic motivation of ML applications in healthcare lies in their ability to automatically analyze, identify hidden patterns, and extract meaningful clinical insights from large volumes of data, which is beyond the scope of human capabilities [85-88].

3- Smart City Applications Architecture and Implementation

The first architectural model for smart cities is a 4-layer framework comprising the sensor, transmission, data management, and application layers. In this model, security is not treated as a standalone layer but is instead integrated into each of the existing layers to ensure comprehensive protection [89]. To address the limitations of this approach, a more advanced and widely recognized architectural model has been developed. This model incorporates five key planes: sensing, communication, data, security, privacy, and the application plane, as illustrated in Figure 1. This framework builds upon the 4-layer model by introducing a dedicated security plane, enhancing the overall robustness of the architecture [9]. To improve interaction between different applications and create a unified smart city ecosystem, new definitions of smart city architecture have introduced a new abstraction layer called the business logic or management plane. This plane acts as an additional management layer placed above multiple applications within a smart city and provides support for functions like device management, local network topology management, and traffic and congestion management. Its main goal is to enhance communication between these applications and ensure efficient management of the smart city, which includes monitoring system performance and addressing any issues that may arise [90].

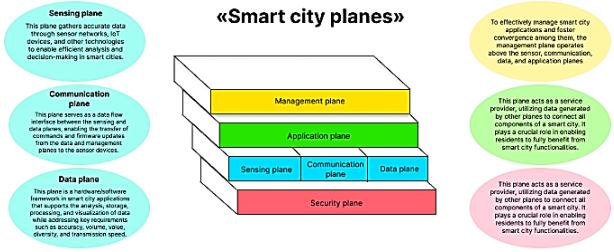

Fig 1. A High-Level Representation of the Smart City Six Planes Architecture

Although each plane has its standards for implementation in smart cities, the most crucial frameworks for developing and implementing smart cities are ITU-T Y.4000, ISO 37120, IEEE P1950.1, IEEE P2413.1, and the IES-City Framework from NIST.
The following subsections will delve into the architecture and significance of the sixth plane.

3-1- Sensing Plane

Collecting the correct data necessary for efficient analysis and decision-making in smart cities is a challenging and intricate task. This typically involves utilizing various components such as sensor networks, IoT devices, and more. Sensors can gather data from different smart city devices in various formats and can be applied in diverse scenarios. At the implementation level of this plane, sensors are generally divided into two categories. The first category includes dedicated sensors, such as humidity, temperature, and imaging sensors, which are designed to collect data for specific parameters. The second category comprises non-dedicated sensors, such as infrared, FID, and GPS sensors, which are capable of collecting and transmitting a variety of data types. In the field of sensors, we encounter three generations of these devices. The initial generation consisted of a limited number of sensor devices per application. The second generation was mainly influenced by the introduction of data fusion, enabling valuable insights to be derived by merging data from a wide array of sensors. The most recent (third) generation now integrates

information from external sources like databases, research, and external applications [9,89].
However, sensing in smart cities encounters several challenges, with the inadequate power supply being the primary cause of many of these obstacles. While energy harvesting techniques can alleviate this issue, their effectiveness in meeting other requirements such as cost, portability, and size is still limited. Additionally, the sensor plane is plagued by high fragmentation and heterogeneity, which complicates ensuring interoperability and scalability. The maturation of population sensing solutions can address many of these needs. Despite advancements in data processing and communication techniques contributing to this progress, the sensor plane itself has seen significant enhancements. Particularly, improvements in VLSI design have consistently decreased the power consumption and cost of sensors while enhancing their on-node computing capabilities [9].

3-2- Communication Plane

In the sensor plane, a network of connected devices collects data. After the data collection, it needs to be sent to the destination. Besides, the connected devices also need to communicate with others. The communication plane acts as a data flow interface between the sensing and data planes, facilitating the flow of commands and firmware updates from the data and management planes to the sensor devices. At the implementation level, the communication plane's functionality is divided into two components: the front-end and the back-end. The front-end establishes connections between sensor devices and focal points, such as access points or gateways. It encompasses local wireless networks, local wired networks, and backhaul networks. The back-end, on the other hand, provides communication links between these focal points and a centralized cloud-based or distributed edge-based data plane. This component handles the adoption, aggregation, and preprocessing of data.
The functionality of this plane can also be divided into three fields: (1) The first functional field is in-field communication, which involves resource-constrained sensor nodes to collect raw data and send it to in-field gateways or access points via wireless or wired connections. (2) The second functional field is the aggregation and adaptation capability, which involves cluster heads, gateways, and access points that have relatively more computational power than field sensors. The adaptation capability bridges the heterogeneous network technologies that exist in a typical smart city implementation. It ensures interoperability with the Internet, through which access to the cloud and its various services is provided. Finally, the third functional field is the network application component, which standardizes the message exchange between centralized or distributed cloud-based or edge-based servers and field devices, regardless of their vendor, topology, and functionality. The sending/receiving of data takes place at the transport layer, and the communication technology for communication can be divided into two primary modes. The first mode is short-range communication, which is suitable for various low-power sensor networks. The second mode is long-range communication, which is suitable for communication between ordinary smart devices such as mobile devices and various smart wired and wireless devices [9,89,91]. The most important IoT communication standards and protocols are MQTT, CoAP, LoRaWAN, Sigfox, Thread, Bluetooth, and BLE. Also, the most important IoT Networking Standards and protocols are 6LoWPAN, IPv6, and Thread.

3-3- Data Plane

Various smart city infrastructures continuously generate data. Data analysis is one of the most important features and functions of sustainable smart cities. The data plane is a hardware/software framework in smart city applications that enables the analysis, storage, processing, and visualization of data by observing data requirements such as accuracy, volume, value, diversity, and speed of transmission. Ultimately, it provides machine intelligence for smart city managers and residents, helping them make informed decisions in program implementation. Data collected from various sources must be cleaned and processed before use. Given the large volume of data generated in a smart city and the increasing amount of data, processing, storing, and maintaining them is a significant challenge; therefore, smart city infrastructures must be scalable. Data visualization can help smart city users and administrators understand the information extracted from the smart city. Machine learning and deep learning algorithms can be used to extract useful information from raw data. In an integrated smart city, effective and coherent visualization of data is crucial and challenging due to the wide range and differentiation of applications [9,92,93].
Two common approaches to data plane implementation are centralized cloud-based and distributed edge-based implementations. The former often offers superior management, usability, and reliability, while the latter usually excels in scalability and latency by reducing the physical distance between field devices and the data plane [89,94]. For example, the infrastructure monitoring system proposed in [95]. adopts a cloud-based architecture to meet core requirements such as large-scale data, real-time processing, and reliability, using replication techniques to enhance system robustness against occasional failures [96]. also proposes an edge-based platform with embedded scheduling techniques that reduce energy demand and provide quality service assurance. This solution allows participants to share their storage and processing resources through a Peer-to-Peer (P2P) network. The most important

IoT data and semantic standards and protocols are JSON, XML, RDF, and OWL.

3-4- Application Plane

The design of smart city services begins with defining applications. Other planes are then deployed to meet the needs of this application plane, from data collection to analysis. The application plane, as a service provider based on data generated by other planes, is crucial for users. This plane connects all components of a smart city so residents can enjoy the benefits of a smart city. The analyzed data from other planes is presented here as decisions. While people may not be aware of how applications work or the algorithms used for data collection and analysis, they can interact with the application plane to view final results and benefit from smart city services. These results include smart health services, smart energy, smart waste management, smart agriculture, smart education, and more. It's important to note that the efficiency of many smart city applications can be evaluated through this plane. If a program cannot effectively communicate with smart city users, even if it presents accurate results, it won't be utilized effectively. Therefore, a proper and user-friendly design of this plane is crucial [9,89]. Also, the most important IoT application layer standards and protocols are AMQP, LwM2M, XMPP, SSI, CoAP, MQTT, DDS, SMS/SMPP, USSD, and HTTP.

3-5- Management Plane

To optimally manage smart city applications and create convergence between different applications, the management plane sits on top of other sensor, communication, data, and application planes. In addition to device management, this plane also supports local network topology management, traffic, and congestion management. Its main goal is to increase communication between these applications and ensure efficient smart city management, including monitoring system performance and addressing any arising issues. The tasks of this plane are generally divided into two categories: Information Technology Service Management (ITSM) and Enterprise Business Service Management (ESM).

ITSM at three macro levels includes the strategy for delivering smart city services, reporting and dashboarding, and continuous service development. At a more granular level, tasks such as change management, service requests, project management, service asset management, asset management, service portfolio management, and service knowledge and catalog management constitute its components. ESM involves collaboration, follow-up, and improvement. Although at a more granular level, these components are similar to the IT service management level, issues are addressed from the perspective and framework of the organization and business rather than from an IT perspective [90,97]. The most important IoT device management standards and protocols are OMA-DM, OMA LWM2M, and AMQP.

3-6- Security Plane

The security plane of smart cities is situated alongside all the other smart city planes to ensure security. Each plane shown in Figure 1 requires mechanisms to guarantee security and privacy. The challenging task of meeting these requirements falls to the security plane. Many of these challenges stem from the security issues present in traditional information and communication systems used in other planes. Each smart city plane is made up of a variety of embedded cyber-physical systems, shared communication and computing infrastructures, and distributed systems. This diversity is a major factor contributing to the security challenges faced by smart cities. As a result, smart cities are increasingly vulnerable to cyber attacks, which can originate from both internal and external sources, underscoring the importance of security and privacy considerations. Designing an effective security plane necessitates comprehensive solutions that address the unique challenges faced by each plane. Some of these challenges include the susceptibility of the application plane to spoofing attacks due to its role in data collection and usage. The sensing plane is often vulnerable to attacks on the limited power capacity of sensors, given the challenges of power and energy provision. The communication plane requires security solutions that take into account the interoperability and coexistence of different communication technologies. The data plane manages a vast amount of heterogeneous, unstructured data stored in the cloud or at the mobile edge, inheriting security issues from cloud-based systems. Additionally, the management plane encounters authentication challenges [9,84,98-105]. In general, implementing services such as authentication, identification, access control, privacy, and data integrity are all related to this plane. The most important IoT Security Standards and protocols are TLS/SSL, DTLS, ECC, OAuth, and X.509.

4- Challenges

Smart city applications typically include a wide variety of sensing devices, leading to heterogeneity in sensing, communication, data, and security planes. Ensuring interoperability among these components and integrating them with existing infrastructure are major challenges in these applications [34]. Generally, challenges in the field of smart city applications can be classified into four categories:

1) Security challenges
2) Data-related challenges
3) Infrastructure challenges
4) Attacks

In the following section, these categories will be reviewed.

4-1- Security Challenges

Security challenges include integrity, availability, privacy, confidentiality, authentication, responsibility, and reliability which we must pay attention to in smart city applications [106-109]. In the following, the security challenges are reviewed.

4-1-1- Integrity

Data must be accurate and not easily accessible. This also includes protecting against external tampering [4].

4-1-2- Availability

Reliable real-time access is needed to monitor the different elements of the smart city infrastructure [4].

4-1-3- Privacy

The biggest challenge in human-centric smart city applications is ensuring the privacy of citizens, which is their fundamental right [1,107].

4-1-4- Confidentiality

Sensitive information must be kept private and secure against unauthorized access. This may include the deployment of firewalls or data anonymization [4].

4-1-5- Authentication

Continuous authentication and verification are essential for participating devices in smart city applications. Hybrid solutions combine behavioral pattern recognition with conventional biometrics-based hard authentication techniques to address this challenge [110].

4-1-6- Responsibility

System users must be responsible for their activities and interactions with sensitive data systems. User logs should document who accesses the information to provide accountability if issues arise [4].

4-1-7- Reliability

Reliability is defined as the probability that a product, system, or service will perform its intended function adequately for a specified period or operate in a defined environment without failure.

4-2- 4-2- Data-Related Challenges

Several challenges are associated with the collection, storage, sharing, ensuring, and maintaining the quality of data [1]. In the following, data-related challenges are reviewed.

4-2-1- Data ownership

people discuss data ownership, they really mean this key role in the data governance framework. They are not the only roles in a data governance framework, but they are the senior people who will make the data governance framework work.

4-2-2- Quality of Data

The quality of data in smart city applications largely depends on the accuracy of the IoT devices and sensors used for collecting data. Therefore, it should be ensured that the data infrastructure is accurate and error-free [111].

4-2-3- Diversity/Characteristics of the Data

In smart city applications, data is collected through several devices, making it challenging to understand the characteristics of the data for removing outliers [112].

4-2-4- Data Auditing

Data auditing involves assessing data to analyze whether the available data is suitable for a specific application, and the risks associated with poor data [1,113].

4-2-5- Informed Consent

Informed consent, which is the process of informing and obtaining participants's consent for data collection, is a key element of data ethics [1].

4-2-6- Data Biases

Datasets generally contain different types of hidden biases, either due to the collector or the respondent, in the collection phase, which are challenging to undo and have a direct impact on the analysis [106]. Various data biases can result in detrimental AI predictions in sensitive human-centric applications. For instance, algorithmic predictions may be biased against certain races and genders, as reported in [114,115]. Intentional and unintentional bias in AI decisions is even more dangerous, which might endanger citizens' lives in healthcare or law enforcement applications. For example, AI-based software used for future criminal predictions was found biased against blacks [1,115].

4-2-7- Interpretation

A key challenge to deploying AI in smart city applications is the lack of interpretability, which results in humans being unable to understand the causes of an AI model's decision [116]. Interpretability is a set of features fed to an AI algorithm, which learns from data by identifying hidden patterns and producing predictions. It is a key characteristic

of AI models deployed in smart city applications [116,117]. For better results, the data used for training an AI model should be interpretable [1].

4-2-8- Open Data

For transparency and developing trust, the data and insights obtained from the data should be openly accessible [1,118].

4-3- Infrastructure Challenges

Infrastructure challenges and security challenges include items such as a constrained environment, robustness to noise and interference, low-delay connectivity, and processing and battery efficiency of smart mobile devices. In the following, the security challenges are reviewed.

4-3-1- Constrained Environment:

Devices, in smart city applications, including data collection sensors and data transfer networks generally have limited resources (i.e., storage, bandwidth, and processing power) [111,119].

4-3-2- Robustness to Noise and Interference

Noise robustness is the capability of an application to maintain its performance despite noise and interference during activity.

4-3-3- Low-Delay Connectivity and Processing,

In user experience, delays of even a fraction of a second can determine success or failure, especially in the IoT as connected devices become more common. Users expect near-zero lag between user input and onscreen output. This requirement is more about humans than modern computers. While the device and its connection determine how quickly user input is reflected on the screen, humans are highly sensitive to response delays [120].

4-3-4- Battery Efficiency of Smart Mobile

Modern mobile devices that connect people consume a lot of battery for sensing and communication capabilities. Various sensors, high-resolution LCDs, wireless interfaces, GPS, and other advanced features drain batteries quickly, reducing operational time. Managing battery life in mobile devices is crucial and requires addressing ways to efficiently utilize battery life at hardware and software levels [121,122].

4-4- Attacks

The increased use of Smart Cities creates new attack opportunities for adversaries to gain access to or carry out disruptive attacks against local government and critical infrastructure networks. Security is one of the main concerns in smart city applications. AI has its unique security issues where a small modification in inputs or data consumed by AI algorithms might change the decision of AI models and cause serious consequences [1]. Intelligent city technology depends heavily on wireless IP networks that are increasingly susceptible to hackers [4]. AI models can be vulnerable to different kinds of attacks, such as adversarial examples, model extraction attacks, backdooring attacks, Trojan attacks, membership inference, and model inversion [123].

For instance, attackers can launch different types of adversarial attacks on AI models to affect their predictive capabilities and bias the decisions [124,125]. Attacks in sensitive application domains such as connected autonomous vehicles can lead to significant loss in terms of human lives and infrastructure [124]. For example, an adversarial attacker could potentially take control of an autonomous car on a highway and demand money to restart it. They could also halt a train on the platform just before the next train is scheduled to arrive [125]. In the following, some of the most important attacks are introduced:

1) Man-in-the-middle attacks
2) Data poisoning
3) Evasion attacks
4) Adversarial attacks
5) Trojan attacks
6) Model stealing (model extraction)
7) Membership inference attacks

4-4-1- Man-in-the-Middle Attacks

Manipulation of messages from a sender to a receiver, with the action being unnoticed by neither end, is termed a man-in-the-middle attack that has also been called manipulation attacks with the advent of the IoT concept. The most effective type of manipulation attack aims at manipulating the network layer immediately at the time when a new device is introduced to the network. As IoT is implemented in a distributed mobile environment, this makes IoT networks especially vulnerable [126-129].

In smart city applications, the session key establishment procedure is an open target for man-in-the-middle attacks. To address this vulnerability, a secure access control method with the objective of session key establishment based on a mutual authentication between a sender and a receiver and ECC encryption at the lower layer is proposed [130]. Network encryption, authentication and key management, identity verification, symmetric or asymmetric data encryption, and digest algorithms are the most effective solutions to answer smart city network layer security issues [131].

4-4-2- Data Poisoning Attack

In these attacks, adversaries intentionally manipulate training data, e.g., incorrect labels, to degrade model performance have control over the training data, or can contribute to it. They inject malicious perturbations into datasets, potentially leading to inaccurate results in offline learning and real-time decision-making processes. These attacks are an emerging threat as machine learning becomes widely deployed in AI applications [132-135].

4-4-3- Evasion Attacks

Compared to data poisoning, evasion attacks can take place after model training. In typical evasion attacks, an adversary perturbs a legitimate input to craft an adversarial sample that tricks a victim model into making an incorrect prediction. An evasion attack happens when the network is fed an “adversarial example” —a carefully perturbed input that looks and feels the same as its untampered copy to a human— but that completely throws off the classifier. Evasion attacks alter model behavior, usually to benefit the attacker [1,136].

4-4-4- Adversarial Attacks

This challenge has been recognized and discussed for crafting fake data that could belong to different domains: text [137], images [138], audio [139], and network signals [140], known as adversarial examples, or evaluating and developing solutions against this security threat [141]. Adversarial attacks are considered severe security threats in learner-based models due to their possible consequences. In smart cities and collaborations of data-driven applications and devices, the impact of misleading a model, e.g., a classifier, could result in harsh situations and a costly mess [1,142].

4-4-5- Trojan Attacks

Trojan attacks on AI algorithms are also very common in cloud and edge deployments of AI [143,144]. A Trojan Horse virus is a type of malware that downloads onto a computer disguised as a legitimate program. The delivery method typically sees an attacker use social engineering to hide malicious code within legitimate software to try and gain users' system access with their software. Unlike computer viruses, a Trojan horse cannot manifest by itself, so it needs a user to download the server side of the application for it to work. This means the executable file should be implemented and the program installed for the Trojan to attack a device’s system [145,146].

4-4-6- Model Stealing (Model Extraction)

The goal of model stealing (extraction) attacks is to steal the parameters or functionality of a confidential model. Model extraction is typically achieved by querying the confidential model and learning from its responses [147,148]. This occurs when an attacker gains access to the model's parameters. The ultimate objective of the adversary is to clone or reconstruct the target model, reverse engineer a black-box model, or compromise the nature and properties of the training data [149,150].

4-4-7- Membership Inference Attacks

In such attacks, the attackers do not necessarily need knowledge about the parameters of an AI model. Instead, knowledge of the type and architecture of the model and/or the service used for developing the model is used to launch an attack [1]. This attack allows an adversary to query a trained machine-learning model to predict whether or not a particular example was contained in the model’s training dataset. During this attack, an attacker tries to determine if you have used a particular person’s personal information to train a machine learning model, to access the person’s personal information [151-153].

4-5- Applications of AI in Responding to Cyber-Attacks in Smart Cities

Here are some ways AI can be used to defend against attacks in smart cities:

4-5-1- Improving the Efficiency of Intrusion Detection Systems (IDS)

Intrusion detection involves identifying and monitoring unauthorized access attempts to an information system. IDS, which can be hardware or software-based, continuously monitors network activity to identify unusual patterns and security risks to prevent cyberattacks. These systems consist of three main components: sensors for collecting data across the network, an analytics engine for processing the collected data, and a reporting system to alert administrators to potential threats and attacks. One challenge of IDS is reporting false positives of cyberattacks. False positives occur when traffic passing through the IDS is detected as a cyberattack when it is not, reducing their accuracy, efficiency, and reliability. By using AI and machine learning algorithms, it is possible to reduce false positives by improving the accuracy of intrusion detection systems and identifying unusual patterns and potential threats in real-time. These systems use machine learning to continuously learn and adapt to new threats, and AI-enhanced machine learning IDS algorithms to analyze network traffic patterns and detect anomalies that may indicate a cyberattack. AI-based IDS with intelligent

architectural frameworks can address security and privacy challenges in smart cities [154-156].

4-5-2- Attack Detection Frameworks

AI-based frameworks, such as the MDATA model, can enhance multi-stage attack detection capabilities by utilizing dynamic cognition based on spatio-temporal data. These models can identify attack patterns at various stages and gather events from different sources, allowing for a comprehensive understanding of security events. They can also assess the severity and impact of threats to prioritize and issue alerts [155].

4-5-3- Cybersecurity Defense Mechanisms

By integrating AI and cyber defense strategies such as software-defined networks (SDN) and fog computing, it is possible to overcome the challenges of resource limitations in smart city IoT equipment and create strong security. Fog computing, which complements cloud computing, utilizes end devices for data processing and storage. SDN is a network architecture approach that is intelligently and centrally controlled and programmed using software programs. In these networks, intelligence separates the network from the hardware, allowing for continuous and comprehensive management regardless of the network background technology. Therefore, by using AI at the edge of the network and relying on fog computing and SDN, it is possible to increase processing speed, enhance threat detection capabilities, and automatically respond to threats [157] [158,159].

4-5-4- Machine Learning Techniques

Techniques such as deep learning and support vector machines (SVM) are advanced methods for detecting cybersecurity attacks that can be effective in identifying and mitigating threats in IoT environments. Deep learning is used to identify complex patterns and detect sophisticated attacks, in which neural networks analyze large volumes of data. Given the power of SVM to classify data points into different categories, it is possible to distinguish between normal and malicious activities. Machine learning models can also identify potential threats by detecting deviations from normal behavior [154] [156].

5- Comparison of Smart Cities and New Trends

According to the 2023 report of the International Society for Urban Informatics on the ranking of smart cities, six indicators have been considered for comparing smart cities. These indicators include smart mobility, smart living, smart environment, smart people, smart government, and smart economy .

The goal of the smart mobility index is to benefit from a smart transportation system that is efficient, economical, safe, and environmentally friendly. The goal of the smart living index is to benefit from smart technologies to improve the living conditions of citizens and create a comfortable, safe, and healthy life. The smart environment reflects the creation of a balance between the city, nature, and residents based on smart technologies. The smart people index relies on creating a suitable environment for citizenship in a way that promotes favorable physical, mental, educational, and cultural states for citizens. The smart government index relies on the use of information technology-based services and systems to provide integrated services to the people by the government. The smart economy index refers to the use of new technologies to increase the efficiency of human resources, sustainability of economic development, and social welfare .

According to the above indicators, the top 10 smart cities in the world are, in order: Copenhagen, Stockholm, Helsinki, Berlin, New York, Toronto, Zurich, Oslo, Hong Kong, and London [97].

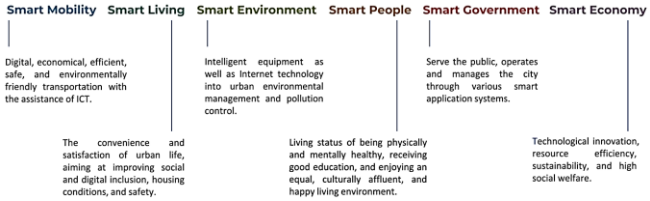

Fig. 2 Smart City Index Framework [97]

A review of the economic and industrial development strategies of industrialized, developed, and developing countries ssuch as the USA, Germany, France, Japan, China, South Korea, India, Indonesia, Turkey and the UAE highlights that smartization of industry has become one of the most critical components of competitive advantage and global market leadership. However, achieving this is impossible without prioritizing the development of smart city infrastructure. Studies indicate that companies and industries failing to take significant steps in this direction risk losing a substantial share of their market soon and may even face complete market exit.

To analyze future trends in the field of smart cities, we use analyses conducted by reputable institutions such as Gartner, Forbes, and Deloitte. In recent years, we have seen a growing use of AI for planning and service delivery in urban areas. This includes data analysis, more efficient resource allocation, predictive modeling, and providing critical real-time alerts to citizens. Given the increasing world population and water shortages in many regions of the world, the use of technological solutions to solve this challenge is of great interest in the coming years. Technologies that are used to manage water collection, storage, and use, consumption management, as well as

predicting availability, recycling, distribution, and desalination are of great interest. As cities become smarter, digital citizenship will become increasingly important, and governments will have programs to verify digital identities and use them to provide services such as applying for permits, receiving welfare payments, and paying taxes. Smart transportation infrastructure will gain momentum in the future to solve traffic problems, and air pollution, increase travel safety, and
move toward a healthier city. Digital twins are a virtual representation of physical assets using real-world data that can predict how components or systems will behave in the real world. The concept will have widespread application in predictive maintenance in industry and will develop rapidly. In the coming years, smart healthcare will grow rapidly, relying on digital technologies to enhance the quality of healthcare and expedite the prevention, diagnosis, and treatment of diseases. Advanced cities such as Singapore, Helsinki, and Dublin are also implementing digital twin projects on a city scale. Advanced smart cities like Rotterdam and New York will utilize IoT technologies to address instability, extreme changes, and weather events such as storms, floods, fires, and droughts. This will enable them to more effectively respond to and overcome these challenges [160] [161] [162]

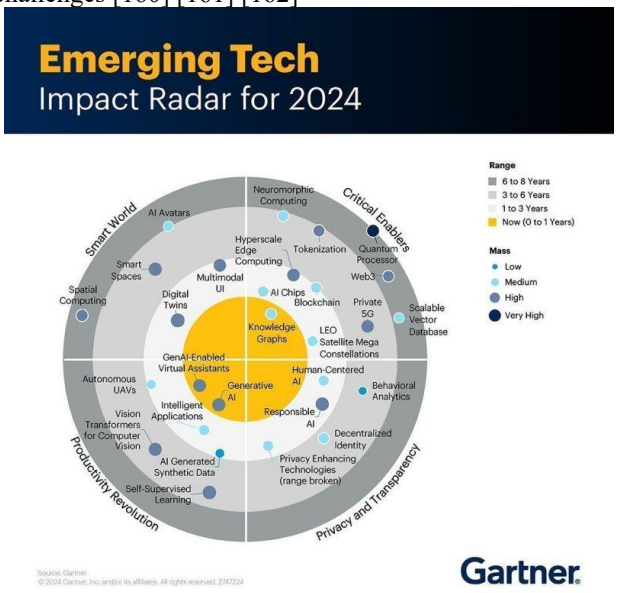

Fig 3. Gartner Emerging Tech Impact Radar for 2024 [159]

In its 2024 Technology Outlook report, Gartner ranks the smart world among the most popular emerging technologies that will experience high growth in the next 1 to 8 years and will create major changes in the use of new technology. Accordingly, figure 3, in the next 1 to 3 years, the use of digital twins in industry to improve the quality of products based on real customer data, as well as the use of multi-model user interfaces to increase human-computer interaction, will grow rapidly. In the next 3 to 6 years, integrated smart cities and AI avatars will also see significant development. In the next 6 to 8 years, [160]

6- Conclusion

Considering the lack of urban resources and the rapid growth of the population of cities, it is inevitable to move towards the increasing development of various services based on the IoT and the emergence of smart cities. Smart cities will have strong development in the coming years, but now in some related areas, great changes have taken place. In this paper, various applications of smart cities such as governance, healthcare, education, transportation, agriculture, energy, surveillance, etc. were reviewed, and it was shown that the scope of smart cities can encompass all aspects of life. To get a proper understanding of the implementation framework of smart city applications, their 5-plane architectures were reviewed. Various aspects of the security and privacy of smart city applications are requirements for their robustness and resilience, which were reviewed in the last part of this paper. New trends can motivate further studies in this area. The main point of this paper is that moving towards smart cities is not just an option, but a technological necessity. In the next decade, countries, cities, companies, and industries that make substantial progress towards becoming smarter will prosper, while those that fall behind risk being left out of competition.

References

[1] K. Ahmad, M. Maabreh, M. Ghaly, K. Khan, J. Qadir, and A. Al-Fuqaha, "Developing future human-centered smart cities: Critical analysis of smart city security, Data management, and Ethical challenges," Computer Science Review, vol. 43, p. 100452, 2022/02/01/ 2022, doi: https://doi.org/10.1016/j.cosrev.2021.100452.

[2] A. Gharaibeh et al., "Smart Cities: A Survey on Data Management, Security, and Enabling Technologies," IEEE Communications Surveys & Tutorials, vol. 19, no. 4, pp. 2456-2501, 2017, doi: 10.1109/COMST.2017.2736886.

[3] B. Green, The Smart Enough City: Putting Technology in Its Place to Reclaim Our Urban Future. The MIT Press, 2019.

[4] I. A. Mohammed, "Security, Privacy and Risks Within Smart Cities: Literature Review and Development of a Smart City Interaction Framework," SSRN Electronic Journal, vol. 8, pp. 55-59, 01/03 2020.

[5] A. AlDairi and L. a. Tawalbeh, "Cyber Security Attacks on Smart Cities and Associated Mobile Technologies," Procedia Computer Science, vol. 109, pp. 1086-1091, 2017/01/01/ 2017, doi: https://doi.org/10.1016/j.procs.2017.05.391.

[6] T. Guelzim, M. Obaidat, and B. Sadoun, "Introduction and overview of key enabling technologies for smart cities and homes," 2016, pp. 1-16.

[7] H. Habibzadeh, Z. Qin, T. Soyata, and B. Kantarci, "Large-Scale Distributed Dedicated- and Non-Dedicated Smart City Sensing Systems," IEEE Sensors Journal, vol. 17, no. 23, pp. 7649-7658, 2017, doi: 10.1109/JSEN.2017.2725638.

[8] B. Ali and A. I. Awad, "Cyber and Physical Security Vulnerability Assessment for IoT-Based Smart Homes," Sensors, vol. 18, no. 3, p. 817, 2018. [Online]. Available: https://www.mdpi.com/1424-8220/18/3/817.

[9] H. Habibzadeh, T. Soyata, B. Kantarci, A. Boukerche, and C. Kaptan, "Sensing, communication and security planes: A new challenge for a smart city system design," Computer Networks, vol. 144, pp. 163-200, 2018/10/24/ 2018, doi: https://doi.org/10.1016/j.comnet.2018.08.001.

[10] A. S. Elmaghraby and M. M. Losavio, "Cyber security challenges in Smart Cities: Safety, security and privacy," Journal of Advanced Research, vol. 5, no. 4, pp. 491-497, 2014/07/01/ 2014, doi: https://doi.org/10.1016/j.jare.2014.02.006.

[11] M. Caţă, "Smart university, a new concept in the Internet of Things," in 2015 14th RoEduNet International Conference - Networking in Education and Research (RoEduNet NER), 24-26 Sept. 2015 2015, pp. 195-197, doi: 10.1109/RoEduNet.2015.7311993.

[12] M. Razaghi and M. Finger, "Smart Governance for Smart Cities," Proceedings of the IEEE, vol. 106, no. 4, pp. 680-689, 2018, doi: 10.1109/JPROC.2018.2807784.

[13] S. Y. Tan and A. Taeihagh, "Smart City Governance in Developing Countries: A Systematic Literature Review," Sustainability, vol. 12, no. 3, p. 899, 2020. [Online]. Available: https://www.mdpi.com/2071-1050/12/3/899.

[14] G. Pereira, P. Parycek, E. Falco, and R. Kleinhans, "Smart governance in the context of smart cities: A literature review," Information Polity, vol. 23, pp. 1-20, 05/14 2018, doi: 10.3233/IP-170067.

[15] J. C. F. De Guimarães, E. A. Severo, L. A. Felix Júnior, W. P. L. B. Da Costa, and F. T. Salmoria, "Governance and quality of life in smart cities: Towards sustainable development goals," Journal of Cleaner Production, vol. 253, p. 119926, 2020/04/20/ 2020, doi: https://doi.org/10.1016/j.jclepro.2019.119926.

[16] A. Khanna et al., "Blockchain: Future of e-Governance in Smart Cities," Sustainability, vol. 13, no. 21, p. 11840, 2021. [Online]. Available: https://www.mdpi.com/2071-1050/13/21/11840.

[17] M. Collotta and G. Pau, "A Novel Energy Management Approach for Smart Homes Using Bluetooth Low Energy," IEEE Journal on Selected Areas in Communications, vol. 33, no. 12, pp. 2988-2996, 2015, doi: 10.1109/JSAC.2015.2481203.

[18] M. Daher, A. Diab, M. E. B. E. Najjar, M. A. Khalil, and F. Charpillet, "Elder Tracking and Fall Detection System Using Smart Tiles," IEEE Sensors Journal, vol. 17, no. 2, pp. 469-479, 2017, doi: 10.1109/JSEN.2016.2625099.

[19] J. Zhang, Y. Shan, and K. Huang, "ISEE Smart Home (ISH): Smart video analysis for home security," Neurocomputing, vol. 149, pp. 752-766, 2015/02/03/ 2015, doi: https://doi.org/10.1016/j.neucom.2014.08.002.

[20] E. Zeng, S. Mare, and F. Roesner, "End user security & privacy concerns with smart homes," presented at the Proceedings of the Thirteenth USENIX Conference on Usable Privacy and Security, Santa Clara, CA, USA, 2017.

[21] R. Batayneh, N. Taleb, R. Said, M. Alshurideh, T. Ghazal, and H. Alzoubi, IT Governance Framework and Smart Services Integration for Future Development of Dubai Infrastructure Utilizing AI and Big Data, Its Reflection on the Citizens Standard of Living. 2021, pp. 235-247.

[22] Q. Hu and Y. Zheng, "Smart city initiatives: A comparative study of American and Chinese cities," Journal of Urban Affairs, vol. 43, pp. 1-22, 01/08 2020, doi: 10.1080/07352166.2019.1694413.

[23] K. Löfgren and C. W. R. Webster, "The value of Big Data in government: The case of 'smart cities'," Big Data & Society, vol. 7, no. 1, p. 2053951720912775, 2020, doi: 10.1177/2053951720912775.

[24] F. T. Hartanti, J. H. Abawajy, M. Chowdhury, and W. Shalannanda, "Citizens' Trust Measurement in Smart Government Services," IEEE Access, vol. 9, pp. 150663-150676, 2021, doi: 10.1109/ACCESS.2021.3124206.

[25] j. zare and R. Hendijani, "E-Government Service Supply Chain: Identifying Performance Evaluation Indicators (Case Study of e-Customs System in Iran)," (in Fa), Journal of Information and Communication Technology, vol. 14, no. 53, pp. 111-139, 2023. [Online]. Available: https://www.magiran.com/paper/2551823.

[26] K. Ahmad et al., Artificial Intelligence in Education: A Panoramic Review. 2020.

[27] Y. Kim, T. Soyata, and R. F. Behnagh, "Towards Emotionally Aware AI Smart Classroom: Current Issues and Directions for Engineering and Education," IEEE Access, vol. 6, pp. 5308-5331, 2018, doi: 10.1109/ACCESS.2018.2791861.

[28] Z. Asadi, M. Abdekhoda, and H. Nadrian, "Understanding and predicting teachers' intention to use cloud computing in smart education," Interactive Technology and Smart Education, vol. ahead-of-print, 09/11 2019, doi: 10.1108/ITSE-05-2019-0019.

[29] O. Díaz-Parra et al., "Smart Education and future trends," International Journal of Combinatorial Optimization Problems and Informatics, vol. 13, no. 1, pp. 65-74, 01/27 2022. [Online]. Available: https://ijcopi.org/ojs/article/view/294.

[30] S. Ar, S. Panda, and S. Hanumanthakari, "Enabling Smart Education System Using Blockchain Technology," 2021, pp. 169-177.

[31] R. J. H. Vladimir L. Uskov, Lakhmi C. Jain, Smart Education and e-Learning - Smart Pedagogy Springer.

[32] A. Qayyum, J. Qadir, M. Bilal, and A. Al-Fuqaha, "Secure and Robust Machine Learning for Healthcare: A Survey," (in eng), IEEE Rev Biomed Eng, vol. 14, pp. 156-180, 2021, doi: 10.1109/rbme.2020.3013489.

[33] S. Alromaihi, W. Elmedany, and C. Balakrishna, "Cyber Security Challenges of Deploying IoT in Smart Cities for Healthcare Applications," in 2018 6th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW), 6-8 Aug. 2018 2018, pp. 140-145, doi: 10.1109/W-FiCloud.2018.00028.

[34] L. Catarinucci et al., "An IoT-Aware Architecture for Smart Healthcare Systems," IEEE Internet of Things Journal, vol. 2, no. 6, pp. 515-526, 2015, doi: 10.1109/JIOT.2015.2417684.

[35] Y. Ren, R. Werner, N. Pazzi, and A. Boukerche, "Monitoring patients via a secure and mobile healthcare system," IEEE Wireless Communications, vol. 17, no. 1, pp. 59-65, 2010, doi: 10.1109/MWC.2010.5416351.

[36] A. Page, M. Hassanalieragh, T. Soyata, M. K. Aktas, B. Kantarci, and S. Andreescu, "Conceptualizing a Real-Time Remote Cardiac Health Monitoring System," in Enabling Real-Time Mobile Cloud Computing through Emerging Technologies, T. Soyata Ed. Hershey, PA, USA: IGI Global, 2015, pp. 1-34.

[37] O. Kocabas, T. Soyata, J. P. Couderc, M. Aktas, J. Xia, and M. Huang, "Assessment of cloud-based health monitoring using Homomorphic Encryption," in 2013 IEEE 31st International Conference on Computer Design (ICCD), 6-9 Oct. 2013 2013, pp. 443-446, doi: 10.1109/ICCD.2013.6657078.

[38] A. Page, S. Hijazi, D. Askan, B. Kantarci, and T. Soyata, "Research Directions in Cloud-Based Decision Support Systems for Health Monitoring Using Internet-of-Things Driven Data Acquisition," International Journal of Services Computing, vol. 4, pp. 18-34, 04/01 2016.

[39] A. Leszkiewicz, T. Hormann, and M. Krafft, "Smart Business and the Social Value of AI," in Smart Industry – Better Management, vol. 28, T. Bondarouk and M. R. Olivas-Luján Eds., (Advanced Series in Management: Emerald Publishing Limited, 2022, pp. 19-34.

[40] J. Mendling, B. Baesens, A. Bernstein, and M. Fellmann, "Challenges of smart business process management: An introduction to the special issue," Decision Support Systems, vol. 100, pp. 1-5, 2017/08/01/ 2017, doi: https://doi.org/10.1016/j.dss.2017.06.009.

[41] B. Leavy, "Alibaba strategist Ming Zeng: “Smart business” in the era of business ecosystems," Strategy & Leadership, vol. 47, no. 2, pp. 11-18, 2019, doi: 10.1108/SL-01-2019-0006.

[42] K. Ćurko, T. Ćurić, and V. Vuksic, "Perspective of smart enterprises development in the Republic of Croatia," WSEAS Transactions on Business and Economics, vol. 14, pp. 378-390, 01/01 2017.

[43] M. Veres and M. Moussa, "Deep Learning for Intelligent Transportation Systems: A Survey of Emerging Trends," IEEE Transactions on Intelligent Transportation Systems, vol. 21, no. 8, pp. 3152-3168, 2020, doi: 10.1109/TITS.2019.2929020.

[44] C. Kaptan, B. Kantarci, T. Soyata, and A. Boukerche, "Emulating Smart City Sensors Using Soft Sensing and Machine Intelligence: A Case Study in Public Transportation," in 2018 IEEE International Conference on Communications (ICC), 20-24 May 2018 2018, pp. 1-7, doi: 10.1109/ICC.2018.8422969.

[45] S. Munder, C. Schnorr, and D. M. Gavrila, "Pedestrian Detection and Tracking Using a Mixture of View-Based Shape–Texture Models," IEEE Transactions on Intelligent Transportation Systems, vol. 9, no. 2, pp. 333-343, 2008, doi: 10.1109/TITS.2008.922943.

[46] Z. Karami and R. Kashef, "Smart transportation planning: Data, models, and algorithms," Transportation Engineering, vol. 2, p. 100013, 2020/12/01/ 2020, doi: https://doi.org/10.1016/j.treng.2020.100013.

[47] R. Sahal, S. H. Alsamhi, K. N. Brown, D. O’Shea, C. McCarthy, and M. Guizani, "Blockchain-Empowered Digital Twins Collaboration: Smart Transportation Use Case," Machines, vol. 9, no. 9, p. 193, 2021. [Online]. Available: https://www.mdpi.com/2075-1702/9/9/193.

[48] C. Zhao, K. Wang, X. Dong, and K. Dong, "Is smart transportation associated with reduced carbon emissions? The case of China," Energy Economics, vol. 105, p. 105715, 2022/01/01/ 2022, doi: https://doi.org/10.1016/j.eneco.2021.105715.

[49] R. A. Gonzalez, R. E. Ferro, and D. Liberona, "Government and governance in intelligent cities, smart transportation study case in Bogotá Colombia," Ain Shams Engineering Journal, vol. 11, no. 1, pp. 25-34, 2020/03/01/ 2020, doi: https://doi.org/10.1016/j.asej.2019.05.002.

[50] M. Ehteshami, M. Cheraghali, B. Tabrizian, and M. Teimourian, "Identifying and ranking factors affecting the digital transformation strategy in Iran's road freight transportation industry focusing on the Internet of Things and data analytics," Journal of Information and Communication Technology, vol. 15, pp. 1-20, 09/26 2022, doi: 10.61186/jict.42076.16.59.1.

[51] R. Bahri and s. zeynali, "Energy procurement of a cellular base station in independent microgrids with electric vehicles and renewable energy sources: Mixed-integer nonlinear programming model," (in Fa), Journal of Information and Communication Technology, vol. 15, no. 57, pp. 266-282, 2023. [Online]. Available: https://www.magiran.com/paper/2640169.

[52] S. L. Ullo and G. R. Sinha, "Advances in Smart Environment Monitoring Systems Using IoT and Sensors," Sensors, vol. 20, no. 11, p. 3113, 2020. [Online]. Available: https://www.mdpi.com/1424-8220/20/11/3113.

[53] H. Nandanwar and A. Chauhan, "IOT based Smart Environment Monitoring Systems: A Key To Smart and Clean Urban Living Spaces," in 2021 Asian Conference on Innovation in Technology (ASIANCON), 27-29 Aug. 2021 2021, pp. 1-9, doi: 10.1109/ASIANCON51346.2021.9544596.

[54] A. Razmjoo, A. Gandomi, M. Pazhoohesh, S. Mirjalili, and M. Rezaei, "The key role of clean energy and technology in smart cities development," Energy Strategy Reviews, vol. 44, 08/20 2022, doi: 10.1016/j.esr.2022.100943.

[55] K. Sujatha et al., "Smart Vision-Based Sensing and Monitoring of Power Plants for a Clean Environment," in Intelligent Manufacturing Management Systems, 2023, pp. 195-222.

[56] M. Vijarania, V. Jaglan, and A. Sanjay, "Security Surveillance and Home Automation System using IoT," EAI Endorsed Transactions on Smart Cities, vol. 5, p. 165963, 08/06 2020, doi: 10.4108/eai.21-7-2020.165963.

[57] "IBM Corp., IBM Db2 Database, Database Software, IBM Analytics,." https://www.ibm.com/analytics/us/en/db2/ (accessed 09 March 2018, 2018).

[58] A. Page, O. Kocabas, T. Soyata, M. Aktas, and J.-P. Couderc, "Cloud-Based Privacy-Preserving Remote ECG Monitoring and Surveillance," Annals of Noninvasive Electrocardiology, vol. 20, pp. 328-337, 12/01 2014, doi: 10.1111/anec.12204.

[59] a. dolatkhah, B. D. Yaghouti, and r. hashempour, "Face recognition and Liveness Detection Based on Speech Recognition for Electronical Authentication," (in Fa), Journal of Information and Communication Technology, vol. 15, no. 57, pp. 94-110, 2023. [Online]. Available: https://www.magiran.com/paper/2640158.

[60] J. Henius and J. L. McDonald, Smart Defense: A critical appraisal. NATO defense College, Research division= Collège de défense de l'Otan …, 2012.

[61] B. B. Gupta, P. Chaudhary, X. Chang, and N. Nedjah, "Smart defense against distributed Denial of service attack in

IoT networks using supervised learning classifiers," Computers & Electrical Engineering, vol. 98, 02/02 2022, doi: 10.1016/j.compeleceng.2022.107726.

[62] I. Karatas, "Cyber Warfare and NATO's New Security Concept: Smart Defense," 2021, pp. 273-285.

[63] T. FRUNZETI, "THE CONCEPT OF "SMART DEFENSE" IN THE CONTEXT OF AN EFFICIENT DEFENSE PLANNING," Journal of Defense Resources Management, vol. Vol. 3, no. 2, pp. pp. 3 – 18 2012.

[64] H. Azadi et al., "Rethinking resilient agriculture: From Climate-Smart Agriculture to Vulnerable-Smart Agriculture," Journal of Cleaner Production, vol. 319, p. 128602, 08/01 2021, doi: 10.1016/j.jclepro.2021.128602.

[65] O. Friha, M. A. Ferrag, L. Shu, L. Maglaras, and X. Wang, "Internet of Things for the Future of Smart Agriculture: A Comprehensive Survey of Emerging Technologies," IEEE/CAA Journal of Automatica Sinica, vol. 8, no. 4, pp. 718-752, 2021, doi: 10.1109/JAS.2021.1003925.

[66] B. Sinha and R. Dhanalakshmi, "Recent advancements and challenges of Internet of Things in smart agriculture: A survey," Future Generation Computer Systems, vol. 126, 08/14 2021, doi: 10.1016/j.future.2021.08.006.

[67] V. K. Quy et al., "IoT-Enabled Smart Agriculture: Architecture, Applications, and Challenges," Applied Sciences, vol. 12, no. 7, p. 3396, 2022. [Online]. Available: https://www.mdpi.com/2076-3417/12/7/3396.

[68] R. Stewart, R. Willis, D. Giurco, K. Panuwatwanich, and G. Capati, "Web-based knowledge management system: Linking smart metering to the future of urban water planning," Australian Planner, vol. 47, 06/01 2010, doi: 10.1080/07293681003767769.

[69] M. Phadke. "Smart Water Management – Need of the hour for utility sector." https://www.einfochips.com/blog/smart-water-management-need-of-the-hour-for-utility-sector/ (accessed.

[70] F. Adesola, S. Misra, N. Omoregbe, R. Damaševičius, and R. Maskeliunas, "An IOT-Based Architecture for Crime Management in Nigeria," 2019, pp. 245-254.

[71] S. Jain and N. Kesswani, "Smart Judiciary System: A Smart Dust Based IoT Application," 2019, pp. 128-140.

[72] J. Laufs, H. Borrion, and B. Bradford, "Security and the smart city: A systematic review," Sustainable Cities and Society, vol. 55, p. 102023, 2020/04/01/ 2020, doi: https://doi.org/10.1016/j.scs.2020.102023.

[73] A. Tundis, H. Kaleem, and M. Mühlhäuser, "Detecting and Tracking Criminals in the Real World through an IoT-Based System," Sensors, vol. 20, p. 3795, 07/07 2020, doi: 10.3390/s20133795.

[74] M. S. Khan, M. Woo, K. Nam, and P. K. Chathoth, "Smart City and Smart Tourism: A Case of Dubai," Sustainability, vol. 9, no. 12, p. 2279, 2017. [Online]. Available: https://www.mdpi.com/2071-1050/9/12/2279.

[75] P. Lee, W. C. Hunter, and N. Chung, "Smart Tourism City: Developments and Transformations," Sustainability, vol. 12, no. 10, p. 3958, 2020. [Online]. Available: https://www.mdpi.com/2071-1050/12/10/3958.

[76] N. Habeeb and S. Talib, "HighTech and Innovation Journal Relationship of Smart Cities and Smart Tourism: An Overview," HighTech and Innovation Journal, vol. 1, 12/01 2020, doi: 10.28991/HIJ-2020-01-04-07.

[77] N. Chung, H. Lee, J. Ham, and C. Koo, "Smart Tourism Cities' Competitiveness Index: A Conceptual Model," 2021, pp. 433-438.

[78] A. Gohar and G. Nencioni, "The Role of 5G Technologies in a Smart City: The Case for Intelligent Transportation System," Sustainability, vol. 13, no. 9, p. 5188, 2021. [Online]. Available: https://www.mdpi.com/2071-1050/13/9/5188.

[79] A. Garcia Crespo, I. Gonzalez-Carrasco, J. Cuadrado, D. Villanueva, and Á. González, "CESARSC: Framework for creating Cultural Entertainment Systems with Augmented Reality in Smart Cities," Computer Science and Information Systems, vol. 13, pp. 6-6, 06/01 2016, doi: 10.2298/CSIS150620006G.

[80] D. Cook, G. Youngblood, and S. Das, A Multi-agent Approach to Controlling a Smart Environment. 2006, pp. 165-182.

[81] P. Pitchai, S. Subramani, K. Usa, K. Raju, M. Alsharif, and M. K. Kim, "Technological Advancements Toward Smart Energy Management in Smart Cities," Energy Reports, vol. 10, pp. 648-677, 06/24 2023, doi: 10.1016/j.egyr.2023.07.021.

[82] A. Braicov et al., "Smart Surveillance Systems and Their Applications," 2020, pp. 179-187.

[83] A. Medjdoubi, M. Meddeber, and K. Yahyaoui, "Smart City Surveillance: Edge Technology Face Recognition Robot Deep Learning Based," International Journal of Engineering, vol. 37, no. 1, pp. 25-36, 2024, doi: 10.5829/ije.2024.37.01a.03.

[84] K. Liao, Z. Zhao, A. Doupe, and G. J. Ahn, "Behind closed doors: measurement and analysis of CryptoLocker ransoms in Bitcoin," in 2016 APWG Symposium on Electronic Crime Research (eCrime), 1-3 June 2016 2016, pp. 1-13, doi: 10.1109/ECRIME.2016.7487938.

[85] J. M. Alonso and C. Mencar, "Building cognitive cities with explainable artificial intelligent systems," in CEx@ AI* IA, 2017.

[86] A. Adadi and M. Berrada, "Peeking Inside the Black-Box: A Survey on Explainable Artificial Intelligence (XAI)," IEEE Access, vol. 6, pp. 52138-52160, 2018, doi: 10.1109/ACCESS.2018.2870052.

[87] R. K. E. Bellamy et al., "AI Fairness 360: An Extensible Toolkit for Detecting, Understanding, and Mitigating Unwanted Algorithmic Bias," ArXiv, vol. abs/1810.01943, 2018.

[88] M. Roy, "Cathy O'Neil. Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy . New York: Crown Publishers, 2016. 272p. Hardcover, $26 (ISBN 978-0553418811)," College & Research Libraries, vol. 78, pp. 403-404, 03/01 2017, doi: 10.5860/crl.78.3.403.

[89] A. K. M. B. Haque, B. Bhushan, and G. Dhiman, "Conceptualizing smart city applications: Requirements, architecture, security issues, and emerging trends," Expert Systems, vol. 39, 2021.

[90] B. Tekinerdogan, Ö. Köksal, and T. Çelik, "System Architecture Design of IoT-Based Smart Cities," Applied Sciences, vol. 13, no. 7, p. 4173, 2023. [Online]. Available: https://www.mdpi.com/2076-3417/13/7/4173.

[91] W. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "An Application-Specific Protocol Architecture for Wireless Micro-Sensor Networks," Wireless Communications, IEEE Transactions on, vol. 1, pp. 660-670, 11/01 2002, doi: 10.1109/TWC.2002.804190.

[92] W. Shi, J. Cao, Q. Zhang, Y. Li, and L. Xu, "Edge Computing: Vision and Challenges," IEEE Internet of Things Journal, vol. 3, no. 5, pp. 637-646, 2016, doi: 10.1109/JIOT.2016.2579198.

[93]"Google Science Journal." https://makingscience.withgoogle.com/science-journal (accessed.

[94] Y. Geng, J. Chen, R. Fu, G. Bao, and K. Pahlavan, "Enlighten Wearable Physiological Monitoring Systems: On-Body RF Characteristics Based Human Motion Classification Using a Support Vector Machine," IEEE Transactions on Mobile Computing, vol. 15, pp. 1-1, 01/01 2015, doi: 10.1109/TMC.2015.2416186.

[95] J. Yin, I. Gorton, and S. Poorva, Toward Real Time Data Analysis for Smart Grids. 2012, pp. 827-832.

[96] D. Neumann, C. Bodenstein, O. Rana, and R. Krishnaswamy, "STACEE: Enhancing storage clouds using edge devices," 06/14 2011, doi: 10.1145/1998561.1998567.

[97]"the International Society for Urban Informatics, The ISUI Smart City " https://www.isocui.org/smart_city_index (accessed.

[98] A. Elmaghraby and M. Losavio, "Cyber Security Challenges in Smart Cities: Safety, security and privacy," Journal of Advanced Research, vol. 5, 07/01 2014, doi: 10.1016/j.jare.2014.02.006.

[99] Y. Zhao, "Research on Data Security Technology in Internet of Things," Applied Mechanics and Materials, vol. 433-435, pp. 1752-1755, 10/01 2013, doi: 10.4028/www.scientific.net/AMM.433-435.1752.

[100] A. Page, M. Hassanalieragh, T. Soyata, M. Aktas, B. Kantarci, and S. Andreescu, "Conceptualizing a Real-Time Remote Cardiac Health Monitoring System," 2015, pp. 1-34.

[101] T. Soyata, Enabling Real-Time Mobile Cloud Computing through Emerging Technologies. 2015.

[102] G. Honan, A. Page, O. Kocabas, T. Soyata, and B. Kantarci, Internet-of-everything oriented implementation of secure Digital Health (D-Health) systems. 2016, pp. 718-725.

[103] A. Page, S. Hijazi, D. Askan, B. Kantarci, and T. Soyata, "SUPPORT SYSTEMS FOR HEALTH MONITORING USING INTERNET-OF-THINGS DRIVEN DATA ACQUISITION," Services Transactions on Services Computing, vol. 4, pp. 18-34, 10/01 2016, doi: 10.29268/stsc.2016.4.4.2.

[104] K. Cabaj and W. Mazurczyk, "Using Software-Defined Networking for Ransomware Mitigation: The Case of CryptoWall," IEEE Network, vol. 30, 08/23 2016, doi: 10.1109/MNET.2016.1600110NM.

[105] S. Mohurle and M. Patil, "A brief study of Wannacry Threat: Ransomware Attack 2017," INTERNATIONAL JOURNAL OF ADVANCED RESEARCH IN ENGINEERING & TECHNOLOGY, vol. 8, 06/11 2022.

[106] S. Latif, A. Qayyum, M. Usama, J. Qadir, A. Zwitter, and M. Shahzad, "Caveat Emptor: The Risks of Using Big Data for Human Development," IEEE Technology and Society Magazine, vol. 38, no. 3, pp. 82-90, 2019, doi: 10.1109/MTS.2019.2930273.

[107] K. Zhang, J. Ni, K. Yang, X. Liang, J. Ren, and X. S. Shen, "Security and Privacy in Smart City Applications: Challenges and Solutions," IEEE Communications Magazine, vol. 55, no. 1, pp. 122-129, 2017, doi: 10.1109/MCOM.2017.1600267CM.

[108] H. Ekbia et al., "Big Data, Bigger Dilemmas: A Critical Review," Journal of the Association for Information Science and Technology, vol. 66, 08/01 2015, doi: 10.1002/asi.23294.

[109] K. Crawford and R. Calo, "There is a blind spot in AI research," Nature, vol. 538, pp. 311-313, 10/13 2016, doi: 10.1038/538311a.

[110] L. Holmquist, F. Mattern, B. Schiele, P. Alahuhta, M. Beigl, and H. Gellersen, Smart-Its Friends: A Technique for Users to Easily Establish Connections between Smart Artefacts. 2001, pp. 116-122.

[111] S. Mallapuram, N. Ngwum, F. Yuan, C. Lu, and W. Yu, Smart City: The State of the Art, Datasets, and Evaluation Platforms. 2017.

[112] A. Ali, J. Qadir, R. Rasool, A. Sathiaseelan, and A. Zwitter, "Big Data For Development: Applications and Techniques," Big Data Analytics, vol. 1, 07/01 2016, doi: 10.1186/s41044-016-0002-4.

[113] H. Yu, Z. Yang, and R. Sinnott, "Decentralized Big Data Auditing for Smart City Environments Leveraging Blockchain Technology," IEEE Access, vol. PP, pp. 1-1, 12/20 2018, doi: 10.1109/ACCESS.2018.2888940.

[114] A. W Flores, K. Bechtel, and C. Lowenkamp, "False Positives, False Negatives, and False Analyses: A Rejoinder to "Machine Bias: There's Software Used Across the Country to Predict Future Criminals. And it's Biased Against Blacks."," Federal probation, vol. 80, 09/30 2016.

[115] K. Crawford, "Artificial Intelligence's White Guy Problem," 2016.

[116] S. M. Lundberg et al., "Explainable machine-learning predictions for the prevention of hypoxaemia during surgery," (in eng), Nat Biomed Eng, vol. 2, no. 10, pp. 749-760, Oct 2018, doi: 10.1038/s41551-018-0304-0.

[117] R. R. Selvaraju, M. Cogswell, A. Das, R. Vedantam, D. Parikh, and D. Batra, "Grad-CAM: Visual Explanations from Deep Networks via Gradient-Based Localization," in 2017 IEEE International Conference on Computer Vision (ICCV), 22-29 Oct. 2017 2017, pp. 618-626, doi: 10.1109/ICCV.2017.74.

[118] C. Drew, "Data science ethics in government," Philosophical Transactions of The Royal Society A Mathematical Physical and Engineering Sciences, vol. 374, p. 20160119, 12/28 2016, doi: 10.1098/rsta.2016.0119.

[119] F. Samie, L. Bauer, and J. Henkel, "Hierarchical Classification for Constrained IoT Devices: A Case Study on Human Activity Recognition," IEEE Internet of Things Journal, vol. 7, no. 9, pp. 8287-8295, 2020, doi: 10.1109/JIOT.2020.2989053.

[120] C. R. Gregersen. "3 IoT Latency Issues and How to Fix Them." https://builtin.com/articles/how-to-fix-iot-latency (accessed.

[121] R. S. Rajeshwari Adrakatti "Approaches for Managing the Smart Phone Battery Efficiently," International Journal of Engineering Research & Technology (IJERT), vol. 3, no. 27, 2018, doi: 10.17577/IJERTCONV3IS27006.

[122] M. Ali, J. M. Zain, M. F. Zolkipli, and G. Badshah, "Battery efficiency of mobile devices through computational offloading: A review," in 2015 IEEE Student Conference on Research and Development (SCOReD), 13-14 Dec. 2015 2015, pp. 317-322, doi: 10.1109/SCORED.2015.7449347.

[123] A. Qayyum et al., "Securing Machine Learning in the Cloud: A Systematic Review of Cloud Machine Learning Security," Frontiers in Big Data, vol. 3, 12/02 2020, doi: 10.3389/fdata.2020.587139.

[124] A. Qayyum, M. Usama, J. Qadir, and A. Al-Fuqaha, "Securing Connected & Autonomous Vehicles: Challenges

Posed by Adversarial Machine Learning and the Way Forward," IEEE Communications Surveys & Tutorials, vol. 22, no. 2, pp. 998-1026, 2020, doi: 10.1109/COMST.2020.2975048.

[125] "a guide to anticipating the future impact of today's technology." https://mediaethics.ca/wp-content/uploads/2019/11/Ethical-OS-Toolkit-2.pdf (accessed.

[126] J. Krimmling and S. Peter, "Integration and evaluation of intrusion detection for CoAP in smart city applications," in 2014 IEEE Conference on Communications and Network Security, 29-31 Oct. 2014 2014, pp. 73-78, doi: 10.1109/CNS.2014.6997468.

[127] H. Suo, J. Wan, C. Zou, and J. Liu, "Security in the Internet of Things: A Review," Proceedings - 2012 International Conference on Computer Science and Electronics Engineering, ICCSEE 2012, vol. 3, 03/01 2012, doi: 10.1109/ICCSEE.2012.373.

[128] M. J. Covington and R. Carskadden, Threat implications of the Internet of Things. 2013, pp. 1-12.

[129] A. Barua, M. A. A. Alamin, M. Hossain, and E. Hossain, "Security and Privacy Threats for Bluetooth Low Energy in IoT and Wearable Devices: A Comprehensive Survey," IEEE Open Journal of the Communications Society, vol. 3, pp. 1-1, 01/01 2022, doi: 10.1109/OJCOMS.2022.3149732.

[130] N. Ye, Y. Zhu, R.-c. Wang, R. Malekian, and L. Qiao-min, "An Efficient Authentication and Access Control Scheme for Perception Layer of Internet of Things," Applied Mathematics & Information Sciences, vol. 8, 07/01 2014, doi: 10.12785/amis/080416.

[131] D. Puthal, S. Nepal, R. Ranjan, and J. Chen, "Threats to Networking Cloud and Edge Datacenters in the Internet of Things," IEEE Cloud Computing, vol. 3, pp. 64-71, 05/01 2016, doi: 10.1109/MCC.2016.63.

[132] M. Aljanabi et al., Data poisoning: issues, challenges, and needs. 2024, pp. 359-363.

[133] W. Li, R. Zhao, T. Xiao, and X. Wang, "DeepReID: Deep Filter Pairing Neural Network for Person Re-identification," in 2014 IEEE Conference on Computer Vision and Pattern Recognition, 23-28 June 2014 2014, pp. 152-159, doi: 10.1109/CVPR.2014.27.

[134] F. Wang, X. Wang, and X. Ban, "Data poisoning attacks in intelligent transportation systems: A survey," Transportation Research Part C Emerging Technologies, vol. 165, p. 104750, 08/01 2024, doi: 10.1016/j.trc.2024.104750.

[135] M. Billah, A. Anwar, Z. Rahman, and S. M. Galib, "Bi-Level Poisoning Attack Model and Countermeasure for Appliance Consumption Data of Smart Homes," Energies, vol. 14, no. 13, p. 3887, 2021. [Online]. Available: https://www.mdpi.com/1996-1073/14/13/3887.

[136] M. A. Ayub, W. A. Johnson, D. A. Talbert, and A. Siraj, "Model Evasion Attack on Intrusion Detection Systems using Adversarial Machine Learning," in 2020 54th Annual Conference on Information Sciences and Systems (CISS), 18-20 March 2020 2020, pp. 1-6, doi: 10.1109/CISS48834.2020.1570617116.

[137] M. Sato, J. Suzuki, H. Shindo, and Y. Matsumoto, Interpretable Adversarial Perturbation in Input Embedding Space for Text. 2018.

[138]N. Papernot, P. McDaniel, S. Jha, M. Fredrikson, Z. B. Celik, and A. Swami, The Limitations of Deep Learning in Adversarial Settings. 2016, pp. 372-387.

[139] N. Carlini and D. Wagner, Audio Adversarial Examples: Targeted Attacks on Speech-to-Text. 2018, pp. 1-7.

[140] I. Corona, G. Giacinto, and F. Roli, "Adversarial attacks against intrusion detection systems: Taxonomy, solutions and open issues," Information Sciences, vol. 239, pp. 201–225, 08/01 2013, doi: 10.1016/j.ins.2013.03.022.

[141] N. Carlini et al., On Evaluating Adversarial Robustness. 2019.

[142] S. Utomo, A. Rouniyar, H.-C. Hsu, and P.-A. Hsiung, "Federated Adversarial Training Strategies for Achieving Privacy and Security in Sustainable Smart City Applications," Future Internet, vol. 15, p. 371, 11/20 2023, doi: 10.3390/fi15110371.

[143] Y. Liu et al., A Survey on Neural Trojans. 2020, pp. 33-39.

[144] Y. Gao, C. Xu, D. Wang, S. Chen, D. Ranasinghe, and S. Nepal, STRIP: a defence against trojan attacks on deep neural networks. 2019, pp. 113-125.

[145] "Trojan Horse Virus." https://www.fortinet.com/resources/cyberglossary/trojan-horse-virus (accessed.

[146] C. Dong, Y. Xu, X. Liu, F. Zhang, G. He, and Y. Chen, "Hardware Trojans in Chips: A Survey for Detection and Prevention," Sensors, vol. 20, no. 18, p. 5165, 2020. [Online]. Available: https://www.mdpi.com/1424-8220/20/18/5165.

[147] M. Juuti, S. Szyller, S. Marchal, and N. Asokan, PRADA: Protecting Against DNN Model Stealing Attacks. 2019, pp. 512-527.

[148] X. W. Minxue Tang, Yitu Wang. "Model Stealing Attacks." https://people.duke.edu/~zg70/courses/AML/Lecture14.pdf (accessed.

[149] https://owasp.org/www-project-machine-learning-security-top-10/docs/ML05_2023-Model_Theft (accessed.

[150] P. Irolla. "What is model stealing and why it matters." https://www.mlsecurity.ai/post/what-is-model-stealing-and-why-it-matters (accessed.

[151] N. Carlini, S. Chien, M. Nasr, S. Song, A. Terzis, and F. Tramèr, "Membership Inference Attacks From First Principles," in 2022 IEEE Symposium on Security and Privacy (SP), 22-26 May 2022 2022, pp. 1897-1914, doi: 10.1109/SP46214.2022.9833649.

[152] "Membership inference attacks | A new AI security risk." https://www.michalsons.com/blog/membership-inference-attacks-a-new-ai-security-risk/64440 (accessed.

[153] A. Famili and Y. Lao, "Deep Neural Network Quantization Framework for Effective Defense against Membership Inference Attacks," Sensors, vol. 23, no. 18, p. 7722, 2023. [Online]. Available: https://www.mdpi.com/1424-8220/23/18/7722.

[154] M. Abdullahi et al., "Detecting Cybersecurity Attacks in Internet of Things Using Artificial Intelligence Methods: A Systematic Literature Review," Electronics, vol. 11, no. 2, p. 198, 2022. [Online]. Available: https://www.mdpi.com/2079-9292/11/2/198.

[155] Y. Jia et al., "Artificial intelligence enabled cyber security defense for smart cities: A novel attack detection framework based on the MDATA model," Knowledge-Based Systems, vol. 276, p. 110781, 07/01 2023, doi: 10.1016/j.knosys.2023.110781.

[156] M. Chohan, U. Haider, M. Y. Ayub, H. Shoukat, T. Bhatia, and M. Hassan, "Detection of Cyber Attacks using Machine Learning based Intrusion Detection System for IoT Based

Smart Cities," EAI Endorsed Transactions on Smart Cities, vol. 7, 06/28 2023, doi: 10.4108/eetsc.3222.

[157] A. Nunn and P. W. C. Prasad, "Using Artificial Intelligence to Defend Internet of Things for Smart City Networks," in Innovative Technologies in Intelligent Systems and Industrial Applications, Cham, S. C. Mukhopadhyay, S. M. N. A. Senanayake, and P. W. C. Prasad, Eds., 2024// 2024: Springer Nature Switzerland, pp. 345-367.

[158] B. J. Ospina Cifuentes, Á. Suárez, V. García Pineda, R. Alvarado Jaimes, A. O. Montoya Benitez, and J. D. Grajales Bustamante, "Analysis of the Use of Artificial Intelligence in Software-Defined Intelligent Networks: A Survey," Technologies, vol. 12, no. 7, p. 99, 2024. [Online]. Available: https://www.mdpi.com/2227-7080/12/7/99.

[159] M. Songhorabadi, M. Rahimi, A. M. Moghadam Farid, and M. Haghi Kashani, "Fog computing approaches in IoT-enabled smart cities," Journal of Network and Computer Applications, vol. 211, p. 103557, 12/01 2022, doi: 10.1016/j.jnca.2022.103557.

[160] "Introduction to "Discover Emerging Technologies in Trends in 2024"." [Online]. Available: https://www.linkedin.com/pulse/part-1-navigating-future-technology-smart-worlds-lennart-kalwa-qh68e/

[161] C. Bernard Marr. "8 Critical Smart City Trends Reshaping Urban Life In 2025." https://www.forbes.com/sites/bernardmarr/2025/01/09/8-critical-smart-city-trends-reshaping-urban-life-in-2 (accessed.

[162] J. G. B. Miguel Eiras Antunes, Daniela Guerreiro de Oliveira. "Urban Future With a Purpose 12 trends shaping the future of cities by 2030." https://www.deloitte.com/global/en/Industries/government-public/perspectives/urban-future-with-a-purpose.html (accessed.