International Journal of Artificial Intelligence and Machine Learning
Volume 10 • Issue 2 • July-December 2020

Internet of Things in E-Government:
Applications and Challenges

Panagiota Papadopoulou, National and Kapodistrian University of Athens, Greece
Kostas Kolomvatsos, National and Kapodistrian University of Athens, Greece
Stathes Hadjiefthymiades, National and Kapodistrian University of Athens, Greece

ABSTRACT

E-government can greatly benefit by the use of IoT, enabling the creation of new innovative services or the transformation and enhancement of current ones, which are informed by smart devices and real-time data. The adoption of IoT in e-government encompasses several challenges of technical as well as organizational, political and legal nature which should be addressed for developing efficient government-to-citizen and government-to-society applications. This article examines IoT adoption in e-government in a holistic approach. It provides an overview of the IoT potential in e-government across several application domains, highlighting the specific issues that seek attention in each of them. The article also investigates the challenges that should be considered and managed for IoT in e-government to reach its full potential. With the application of IoT in e-government being at an early stage, the article contributes to the theoretical and practical understanding of how IoT can be leveraged for e-government purposes.

KEYWORDS

E-Government, Internet Of Things, IoT, Smart Government

INTRODUCTION

IoT is a very promising technology and is predicted to flourish within the next years, as 127 new devices connect to the Internet every second (McKinsey, 2018), with the number of IoT devices being expected to exceed 64 billion by 2025 (Business Insider, 2019). With the advent of the Internet of Things (IoT) machines and objects constitute dynamic intelligent actors of networked environments providing novel services. The ubiquitous nature of IoT brings dramatic changes to the way we work and live, with an increasing adoption in various domains of personal and organizational activity. IoT can bring unprecedented benefits in the public sector, making a shift from e-government to smart government, transforming G2C, G2B, and G2G transactions and processes. According to industry forecasts, the smart government market is estimated to reach USD 52.19 billion by 2026 (Reports and Data, 2019). IoT-enabled government information systems and applications can offer innovative services or extend the type and the quality of existing ones with smart provisions across a wide spectrum of domains, such as health, transportation, environment, communications, security/safety, energy, defense and smart cities. In each of these sectors IoT can be used to provide a variety of sophisticated e-government services that can be valuable and helpful to citizens, the society and the environment. In all these cases, IoT systems and applications enable the provision of advanced services to people and the society in general, that can enhance their security and safety against a

DOI: 10.4018/IJAIML.2020070106

number of threats and risks and in diverse contexts, allowing for the protection of the public, the prevention of disasters and the immediate and effective response to emergency situations. In addition to the critical safety provisions, thanks to the use of IoT, these electronic government-to-citizen (G2C) and government-to-society (G2S) services allow for a better quality of life by protecting the environment and by facilitating everyday activities. Despite the increasing progress and interest in both areas of IoT and e-government, research on their combined use is limited (e.g. Wirtz et al., 2019; AlEnezi et al., 2018; Brous and Janssen, 2015a, 2015b). Literature focus is largely on technology or governance aspects or a specific application area such as smart cities. How e-government can benefit and grow from IoT has not been fully addressed yet. In order to gain a better understanding about how e-government can successfully leverage the IoT potential, a comprehensive, holistic approach of applying IoT in e-government is needed, covering challenges of both technical and non-technical nature, associated with the combined use of e-government and IoT systems. In this paper an attempt is made towards setting a framework for designing and implementing smart citizen and society-oriented government services with IoT-based systems. In this direction, after an overview of the research literature related to the topic, we describe several application domains of IoT in e-government, with a particular focus on critical services provision, in areas of public security/safety, healthcare, environment, transportation, energy, waste management and smart city. Then, we identify the challenges, technical and non-technical, that can be encountered in the development of successful IoT egovernment systems and we propose solutions that can be used to tackle these challenges. The paper proceeds to showcase the potential of IoT-based e-government as well as the challenges and how they should be addressed through an example case. Finally, the paper summarizes our findings and provides conclusions and guidelines. The paper aims to contribute to a better understanding of how the IoT promise in government can be realized and to provide insights that can be of value for both researchers and practitioners active in the growing field of IoT and e-government.

BACKGROUND

IoT and e-government as a joint topic has recently received research attention in a number of research works. AlEnezi et al. (2018) study smart government as the technological union of e-government and smart cities. Smart cities could incorporate an ICT infrastructure on top of the physical infrastructure that can involve sensors, actuators, network hardware, end users devices and so on. The authors, in their recent work, discuss three IoT-based smart government challenges, namely, mindscaping, investment and security and privacy, which are considered as of primary concern to the overall implementation success or failure of smart government. Tang and Ho (2018) provide an empirical analysis of smart sensor adoption by US local governments. They examine two specific questions regarding sensor adoption: what factors affect the scope of sensor adoption by municipal governments and what factors affect the level of integration among sensors across different urban domains. Their results show that the change in smart sensor adoption in e-government is incremental. The study gives evidence that local governments' early adoption of smart sensors is likely to stem from their needs in specific policy domains. The authors also find that a local government's historical paths on urban sustainability and data-driven decision-making practices can predict its trajectory of sensor deployment, in terms of the scope and the integration of smart sensors across different urban domains. On the other hand, a local government's e-government progressiveness is not found to be a significant predictor of smart sensor adoption. Brous and Janssen's (2015a) work was on the identification of the potential benefits of IoT in egovernment applications. Drawing from a review of the research literature and using data from two case studies they found that e-government can be benefited from IoT at political, strategic, tactical and operational level. Their findings show that IoT enables effective knowledge management, sharing and collaboration between domains and divisions at all levels of the organisation, as well as between government and citizens. Specifically, according to the study, the IoT benefits for e-government include improved efficiency, effectiveness and flexibility of services, reduction of costs, improved

citizen empowerment, improved government transparency, more efficient enforcement of regulations, improved planning and forecasting and improved health and safety measures.

The previous authors have also studied the impediments that block IoT adoption by governments in Brous and Janssen (2015b). Based on a literature review and two case studies they identify the main barriers of adopting IoT for government purposes, which are classified at the strategic, tactical and operational level. Specifically, impediments of IoT for e-government can be attributed to data privacy issues, data security issues, weak or uncoordinated data policies, weak or uncoordinated data governance, and conflicting market forces, costs, interoperability and integration issues, acceptance of IoT and trust related issues, a lack of sufficient knowledge regarding IoT, IT infrastructural limitations, and data management issues. Sideridis et al. (2015) provide an overview of Smart Cross Border e-Government Systems (SCBeG) making full use of ICT innovations in cloud computing, big data and IoT, based on the results of the EU project STORK 2.0. The authors propose the development of SCBeG systems in combination with e-identification platforms and their utilization in various application areas. Sideridis and Protopappas (2015) have studied IoT in e-government focusing in life sciences. They discuss smart e-government systems as they are enabled by IoT and cloud computing technologies and they specifically examine the application of such systems in the domain of agriculture. In a similar vein, the work of Kumar (2017) investigates the use of IoT in e-governance, focusing on IoT services in the field of agriculture. The author presents the benefits of IoT for economy and sustainable development through a case study of agricultural production in India. The study suggests that IoT in agriculture can lead to better productivity and higher revenue which in turn can enhance the country's economy and lead to prosperity. Schwertner et al. (2018) examine IoT as one of the technology components that are essential in Industry 4.0 and suggest an approach for its use in the context of natural disaster and crisis management, targeting data acquisition, management and analysis. The use of IoT-based systems for natural disaster detection and warning has also been the topic of several studies such as Alphonsa et Ravi, (2016), Amjath Ali et al., (2017) and Babu et al., (2018). Haddadeh et al. (2018) propose an acceptance model for IoT smart devices in the context of public sector services.

They present an empirically tested model on the perceived value and continuous use intention of public services enabled by IoT. Their findings show that citizens' perceived value of IoT can be influenced by empowerment, perceived use and privacy, resulting in affecting their continuous use intentions. Perceived value and continuous use intention of IoT in the context of public services were not found to be predicted by informational social support. Thibaud et al. (2018) provide a comprehensive overview of publications on IoT-based applications in high-risk Environment, Health, and Safety (EHS) industries. They focus specifically on healthcare services, food supply chain (FSC), mining and energy industries (oil & gas and nuclear), intelligent transportation, and building and infrastructure management with emphasis on emergency response operations until 2016. They identify the main general characteristics of IoT applications by industry, specifically system architecture, sensor level, communication, back-end system and business/market aspects. They also provide a review of the challenges that IoT-based application need to deal with. These are grouped in technical and social and economic challenges. Technical challenges include energy efficiency, communication and data-related challenges (connectivity, latency, throughput, standardization), scalability (network size, interoperability), security and safety (reliability, privacy protection). Social and economic challenges that are identified comprise business model, standardization, compliance with regulatory and industry standards, community support and staff training, affordability vs. high cost of implementation, absence of global or national standards and regulation and time-to-market for IoT-based applications. For these challenges the authors present the main solutions proposed per industry in the reviewed literature, which are mostly focused on tackling the technical issues. The authors review also covers the future research trends and challenges in each EHS industry, which seem to concentrate mostly on technical challenges and trends, especially in communication and processing capabilities. Wirtz et al. (2019) propose an integrative public IoT framework for smart

government. Based on a literature analysis of twelve IoT frameworks, the study identifies four layers integrating the technology and business model dimensions of IoT frameworks, namely, the public strategic layer, the public value creation layer, the public demand layer and the technology transfer layer. These layers are described along their components to provide the proposed framework.

APPLICATION OF IoT IN E-GOVERNMENT

IoT adoption in e-government can be harnessed across a wide variety of sectors. Various e-government applications could be developed to make use of the data that can be collected by IoT devices. Each of them could aim to provide extended analytics services to support fast and informed decision making, which could be of great value, particularly to citizens and the society and especially for cases requiring emergency response. In this section, indicative G2C and G2S applications of IoT in e-government are described, focusing on areas that are related to public security and safety, transportation, health, smart city, waste management, energy and the environment. The latter is analyzed into environment pollution and natural phenomena, which are related to fire, earthquakes and the weather. Table 1 provides a comprehensive categorization of IoT application domains, with example applications for each domain.

Health

A major opportunity of adopting IoT technology is the health domain. IoT can be of high value to the healthcare sector, facilitating a continuous, cost-effective and error-free monitoring of patients without the need for the physical presence of a doctor. IoT services can be used for remote health monitoring and tele-health systems, enabling medical staff to remotely examine patients, make diagnoses and provide medical care. IoT health systems can also be used for helping people monitor their health problem themselves, for example, by measuring their blood pressure or insulin levels, and enabling a remote communication with medical personnel for receiving treatment. In this way, the use of sensors and other IoT devices allows for patients to be monitored constantly, generating notifications and alerts, thus enabling the prevention or the on-time intervention and treatment of problems or even life-threatening events. Tracking patients at real time can save lives, particularly in case of an emergency, as it allows for instant check and appropriate reaction, irrespective of time and place, that would not be possible otherwise. Apart from all these medical benefits, the application of IoT in the health sector can thus offer valuable benefits of economic nature to both people and governments, as it can reduce various costs of health systems related to physical doctor appointments, medical examinations, diagnosis, treatment and hospitalization. A possible impediment to using IoT in healthcare is that it is very sensitive to personal data which are collected and used at real time. However, the use of IoT systems could help improve the quality of life for patients, especially patients with chronic illnesses, patients who live in rural areas away from urban medical facilities and patients with moving difficulties such as elderly people or people with disabilities.

Security/Safety

Security and safety are of major importance for citizens and the society. IoT can provide support for addressing various security and safety requirements. The autonomous nature of IoT nodes and the sensing and advanced onboard processing capabilities allow for tasks such as object detection and sensor information fusion.

IoT could be used to provide effective and efficient surveillance and control of critical security and safety areas. IoT nodes can be used to monitor country borders, land, maritime or aerial, or other sensitive areas in regard to public security and safety, such as airports, ports and train, metro or bus stations. IoT systems can also be employed for the control of other public places which are highly populated and receive large concentrations of people, especially in particular events or periods, such as popular squares and roads during Christmas holidays and various festivals, or venues and places

Table 1. IoT domains and applications in e-government

IoT Application Domain	IoT Applications
Health	Remote health monitoring
	Remote medical diagnosis and treatment
	Constant Tracking of patients
Environment (Incidents, Natural phenomena)	Pollution (air, water, sea, soil)
	Weather monitoring
	Noise pollution
	Forest fire detection
	River flood detection
	Earthquake alert
Transportation	Connected vehicles
	Driverless vehicles
	Traffic control
	Dynamic routing
	Emergency management
Security/Safety	Border Surveillance
	Critical security and safety areas control
	Surveillance of popular public areas
	Protection of critical infrastructure
Smart City	Structure conditions of buildings/bridges
	Lightning for buildings, roads, parks
	Road traffic and driving conditions
	Surveillance
	Emergency alert and response
	Parking
Waste Management	Waste collection
	Waste transport
	Waste recycling
Energy	Smart grid
	Renewable energy systems
	Prognostics for power grids

like stadiums during concerts or games and other sports or art events. In addition, IoT capabilities can be valuable for the security and safety protection of critical infrastructure, such as energy plants for electrical power or water supply.

In each of these contexts, IoT nodes can work, both separately and in collaboration, to provide enhanced security and safety control and protection, and allow for detection and prevention of illegal trespassing, invasion or crimes. IoT nodes can collect data with the use of acoustic and motion sensors and cameras, which can be processed to provide information about the current status of the monitored area. Such information can be of great value to stakeholders to assess potential vulnerabilities and

threats, handle dangerous incidents that may occur and facilitate their decision-making process regarding operations management and the course of action that should be taken. Public authorities, the police, command and control centers can be significantly benefited from the functional features and facilities of IoT systems and the amount and richness of the information they can provide.

Using IoT systems, the surveillance and control of critical areas can be done remotely and constantly, at any time, in ways that could be difficult if not impossible otherwise. Border control can be significantly improved and become more effective. Critical areas can easily be monitored and controlled, without putting humans in risk, as IoT nodes can be used anywhere, particularly mobile IoT devices and unmanned vehicles. Thus, IoT systems can allow for surpassing human limitations and enable immediate response to critical events to offer increased security and safety to countries and their citizens.

Transportation

IoT technology has already been adopted in transportation systems either in the available infrastructure (e.g., roads) or in the vehicles. Intelligent transportation systems such as in-car IoT systems, smart highways or route planning can assist users to deal with all the constraints associated with traffic, time, and cost. IoT can be used in cars, trucks, buses or other vehicles, enabling them to collect ambient information and communicate with other vehicles in order to avoid accidents or find optimal routing. E-government services can be built on top of the collected data and provide functionalities related to traffic or emergency management. Traffic congestion is a growing problem in most urban areas across the world (Hounsell et al., 2009). Traffic management services can collect data from IoT sources, process and manage these data and use the delivered information to implement various measures to manage traffic. This will lead to a better flow of vehicles reducing the observed traffic jams and consequently eliminating the risk of accidents or facilitating the fast move of people or the police, ambulances and fire brigade in case of emergency. IoT devices can report data related not only to vehicles but also to drivers. In any case, the in-vehicle devices can monitor drivers' status or the status of the vehicles in close distance and relay this data to the centralized infrastructure. The central system can have a view on the status of each vehicle being immediately informed about the presence of any emergency. In addition, the central system can have the overview of any area in the city and support services for long-term traffic management. Such emergency situations can be also identified by the in-vehicle devices forming a huge infrastructure of autonomous vehicles that can assist in emergency management.

Smart City

IoT offers new opportunities for technology solutions that improve existing services and the living experience of citizens, with smart cities (SCs) infrastructures and numerous services built on top of them. SCs are complex cities and are based on the physical infrastructure where IoT devices could be embedded. With the technical support from IoT, smart cities need to have three features of being instrumented, interconnected and intelligent (Kim et al., 2017) to gain benefits from the IoT infrastructure. New, efficient, scalable, and reliable applications for smart cities are proposed based on the IoT infrastructure. Due to the low cost of IoT, it is now possible to monitor and manage activities that were previously unreachable. Currently, cities create the conditions for continuous development: digital technologies are becoming increasingly important, urban infrastructures and buildings are planned more efficiently and sustainably. As with IoT deployments in all market segments, the key for smart cities is real-time data, how they are processed and stored, how they are analyzed and how the processing outcomes are adopted to drive actions. Smart cities use intelligent technologies to achieve an energy-efficient and environmentally friendly infrastructure. For instance, smart lighting will only give light when someone actually walks past them like setting brightness levels and tracking daily use to reduce the need of electrical power. Integrated sensors can send real-time updates of various phenomena to a centralized system, then, an analysis over the collected data could assist in

the automated adjustment of various parts of smart city infrastructure. For instance, sensors in the ground can report via smartphone the driver, where they can find a free parking space while others can use vehicle feedback to tell precisely where the openings are and nudge waiting cars towards the path of least resistance. Numerous sensors are placed in various places in SCs forming a 'grid' that generates huge volumes of data. However, the generation of huge volumes of data makes their management very difficult. Public authorities, local companies and citizens need efficient mechanisms that will manage the data. Large scale system integrators could provide knowledge and products on top of the discussed data, usually, through efficient aggregation processes and transformation tools. The heterogeneity of the data sources makes this task very difficult and requires the appropriate tools according to the application domain. Citizens could also gain knowledge from these data. For instance, the provided services could be adapted not only to personal needs but also to the needs of groups of people (e.g., drivers, neighborhoods, workers). This means that the knowledge extracted from the huge volumes of data should be transformed in different forms according to the needs of each group. Public authorities could also adopt such an approach to gain insights on the needs of citizens. This way, authorities could reduce the citizens cost-to-serve and offer services fully adapted on their needs, keeping the social sustainability at high levels.

Waste Management

Waste management is another domain where IoT technologies can support innovative applications. Such solutions can be based on a wireless sensor network (WSN) infrastructure where sensors are used to collect and process ambient information and, thus, upgrade 'legacy' waste management mechanisms. This allows for a smart environment approach which can be adopted for environmental pollution and the improvement of people's lives. Various types of sensors can be incorporated into waste bins or garbage containers. Smart bins or other waste disposal units can monitor the fill level and waste type in real time, thus enabling efficient garbage collection and recycling, based on the actual disposal activity. In this vein, waste management can be modelled as a set of services on top of the IoT infrastructure in a Smart City. These services cover the following parts of a waste management scheme: (i) waste collection planning and implementation (e.g., scheduling and routing solutions for collection trucks, dynamic adaptation of routes); (ii) waste transport to specific locations (e.g., routing according to the type of waste); (iii) recycling and preparation for re-use. IoT can be the key enabling technology applying dynamic models on contemporary waste collection with the use of sensors, actuators and digital tagging such as Radio Frequency Identification (RFID), NFC and QR codes. In this context, static waste collection models could be transformed to Waste Collection as a Service (WCaaS) which enables online dynamic scheduling and routing of the collection trucks (Lingling et al., 2011). The dynamic waste collection could be described as an online decision process for defining: (i) when to collect waste from bins (i.e., scheduling), and (ii) which routes the collection trucks should follow (i.e., routing). Many technologies and hardware are already used in waste management adopting different approaches in the management of the physical infrastructure as well as the data collected in the field. For instance, the IoT hardware and technology could identify real objects and transform them to 'smart things' (Lopez et al., 2012).

Energy

With IoT, the electricity industry has entered a new era that revolutionizes the legacy electrical grids, transforming them to the smart grid (SG). SG offers more efficient and effective power management, better reliability, reduced production costs, and more environmentally friendly energy generation (Coppolino et al., 2014). As the next generation power system, the SG is increasingly attracting the attention of governments, industry, and academia. The SG is an upgraded electricity network that depends on two-way digital communications between suppliers and consumers that in turn give support to intelligent metering and monitoring systems (Fan and Gong, 2013). The SG offers significant performance benefits to the electricity industry and facilitates consumers in managing

and optimizing their power consumption. The SG basis is the intelligence built on top of the data reported by end devices i.e., smart meters. Hence, the SG transforms legacy electricity networks to a software-driven infrastructure with numerous possibilities. A variety of applications and software components could provide specific functionalities over the data reported by smart meters. The SG heavily relies on the communication networks and the secured delivery and management of smart meters data. Various applications can be proposed over the huge infrastructure of SG. Smart meters installed in the consumer premises can be the critical part of these applications acting as a point of processing for the efficient energy management. The energy sector can be further benefited with the future management of the hierarchy of nano and micro SG. Nano grids are related to the production of energy in single users or a building adopting renewable resources while microgrids are related to several buildings. Smart microgrids can communicate with their parents and peers on ongoing basis forming a complete energy ecosystem. Hence, the use of IoT for energy can be cornerstone for an efficient e-government.

Environment

Environmental monitoring is considered one of the top areas IoT can deliver the most value for (Columbus, 2018). IoT, due to its autonomous nature, can provide support for environment monitoring and control where elaborate sensing, processing and possibly reacting are needed. IoT devices can be adopted for providing smart e-government services, by monitoring specific phenomena and, when needed, generating alerts or taking action. Such phenomena can be related to various facets of the environment covering a wide spectrum of incidents. The phenomena for which IoT could be used for e-government purposes can be grouped into two broad categories, environment pollution and natural phenomena. Natural phenomena include fire in forests and rural areas, earthquakes and weather phenomena.

Environment Pollution

IoT e-government systems can be used for the protection from environment pollution. They can involve applications such as monitoring of air quality, water quality, sea quality and soil quality. Environmental IoT systems can allow for activities such as air pollution detection, quality control of water for drinking and agriculture, soil quality control for agricultural purposes and sea quality control for swimming and fishing. E-government services for environment protection can also involve IoT devices for the monitoring of waste management and pollution coming from industrial or residential activity. Energy production plants and management can also be supported by IoT systems, allowing for the continuous risk-free provision of general public goods such as electricity or gas or water supply. The critical issue in such e-government services is the efficient management of the collected data. Such management can assist in making long- or short-term decisions. For instance, short-term decisions could be related with taking immediate actions to avoid environmental pollution with negative consequences in people's lives. Long-term decisions can be related with the delivery of strategies to proactively avoid environmental pollution. The proactive decision making should be based on historical data but also on the estimation of the future trends in the observed information. In any case, the timely processing of the collected data should lead to a set of analytics designed by experts in order to support further decision making. Hence, the discussed e-government services should be designed having ICT experts cooperating with experts in other domains (e.g., environmental scientists) in order to conclude the best possible result.

Fire Detection in Forests and Rural Areas

IoT could be used for fire detection in forests and rural areas. For instance, a set of sensors could be adopted to monitor a forest for identifying fire events. Mobile IoT devices, particularly unmanned vehicles, could also be extremely valuable tools for fire protection. Such devices can be deployed for forest and rural areas monitoring, which can be used to contribute in fire prevention as well as in

fire extinguishing. Hence, such services can assist in the proactive decision making together with the efficient situational awareness when an event is triggered. In particular, the autonomous functionality of IoT devices can be leveraged to allow for remote management of fire events. Beneficiaries of such a system could be the fire brigade, local authorities, municipalities, public authorities or citizens. In case of detecting a suspicious event, the IoT-based system would be capable of generating fire alerts, informing the interested parties and also be connected with command and control systems of emergency management authorities. In particular, mobile IoT devices such as unmanned vehicles could serve as valuable actors for fire protection. For example, unmanned aerial vehicles (UAVs) can conduct regular flights above the area of interest to provide an aerial view allowing for complete and wide coverage of the area. UAVs can also serve as part of the operation for extinguishing a fire, providing valuable information that can be used for several purposes. Similarly, unmanned ground vehicles (UGVs) can assist in the better monitoring of land surfaces, especially those that are not easily accessible by humans and regular vehicles, contributing with the data that they can collect on the spot, to the prevention of fire incidents as well as to their management in case of occurrence. Thus, IoT devices can greatly facilitate the difficult work of the fire brigade, at operational level, in locating areas that are in need and in planning their fighting against fire. IoT information can also be useful in informing citizens about fire events and also help the police, civil protection and local authorities in their decision-making about actions that need to be taken, for example the evacuation of an area.

Earthquake Alert

IoT capabilities can be particularly useful for the protection from earthquakes, a natural phenomenon to which it is still extremely difficult to react promptly and effectively and it is still debatable within the scientific community if it can be predicted and how reliable such predictions can be. Autonomous, distributed sensor systems can be used in order to monitor earth conditions for seismic activity. Examples of IoT systems for earthquake detection can be found in the works of Alphonsa et Ravi (2016), Amjath Ali et al. (2017) and Babu et al. (2018). Such IoT systems can send warnings in the occurrence of an earthquake so as to inform people and government systems faster and allow for efficient response actions. These alerts can be generated and received by smart phones or other devices and systems early enough to prevent damages or human loss. In such cases, it is important is to enhance the situational awareness of possible damages or affected areas in order to assist public authorities in their first response. A challenge in this domain is to manage the heterogeneity of the external systems that should be informed when an event occurs. This kind of e-government services will act as the intermediary between the sensory infrastructure and systems of public authorities. Hopefully, IoT systems can also be used to contribute in the prediction of earthquakes and, consequently, help governments and the public in the timely reaction and protection from them.

Weather Monitoring and Forecasting for Intense or Dangerous Phenomena

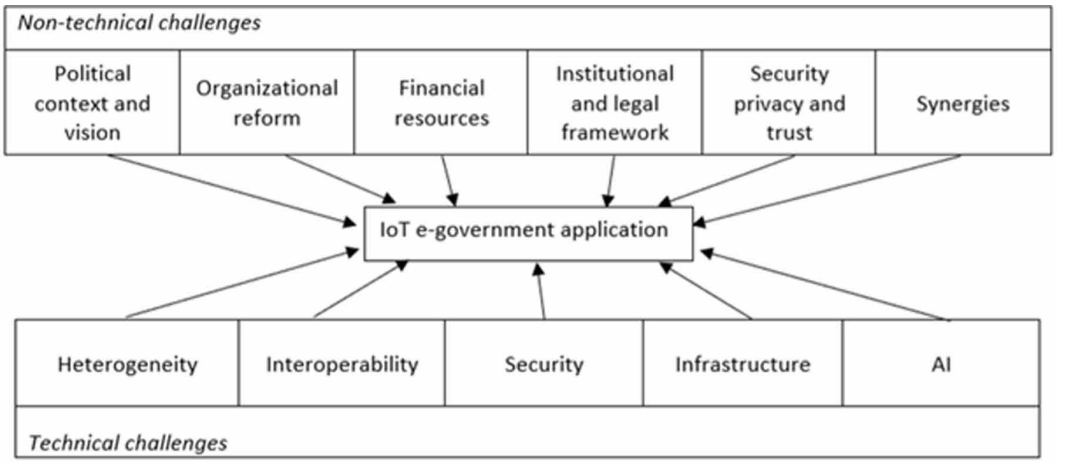
IoT devices and systems can be used to monitor weather conditions for intense or dangerous phenomena, allowing for effective reaction against them. Such phenomena include storms, strong winds, floods, tsunamis and high rain or snowfall levels. Leveraging IoT capabilities can support the early detection of such phenomena, enabling disaster prevention or mitigation through provision of timely warnings and facilitation of immediate response (e.g. Amjath Ali et al., 2017). E-government services from meteorology offices can be greatly informed using the data that can be collected with IoT devices. The analysis of these meteorological data can enhance the accuracy and timeliness of weather forecasts and monitoring. In this way, IoT-based meteorological systems enable the provision of frequent and highly precise weather updates as well as the generation of alerts in case intense or dangerous weather phenomena are estimated to appear, providing rich information regarding their location, duration and intensity. IoT devices can be used for monitoring the water level in rivers, lakes or the sea, creating alerts when a rise is detected and notifying for evacuation plan of inhabited areas in case of flood possibility. IoT can also be valuable for e-government services in case of extreme

weather phenomena such as hurricanes and tornados. Intense weather phenomena forecasting, and the timely estimation of their consequences may positively affect various industries in addition to general populace safety. For instance, agriculture depends on precise up-to-date readings on soil, temperature and moisture while the identification of any dangerous situation seems to be imperative (Burkhalter, 2018).

CHALLENGES OF IoT E-GOVERNMENT

The adoption of IoT in e-government can be very promising as well as challenging at the same time. In this section, we focus on the challenges of the use of IoT in e-government which can be divided into technical and non-technical. These are depicted in Figure 1.

Figure 1. Challenges of IoT e-government



Technical Challenges

The central concept of the IoT era is that 'things interact with each other'. Such interactions refer to peer to peer communication and data exchange as well as communication with back end systems usually found in the Cloud. The autonomous nature of IoT devices allows us to gain from the automation of various functionalities, the integration of data and services and the analysis of the behavior of autonomous entities and the collected data. It should be noted that IoT devices are characterized by two parameters, i.e., the type of the hardware they use and the type of the software they adopt. In the following paragraphs we provide our view on the technical challenges in the adoption of the IoT vision in e-government services.

Heterogeneity

Initially, the heterogeneity of the devices plays a crucial role in the provision of services that can be supported by the entire set of the available nodes. This way, we can have the opportunity to create universal services for 'injecting' smart government functionalities into the devices. The diversity of IoT devices poses difficulties in their connection and communication. Difficulties are further created by the lack of common standards for data exchange, which can refer to communication among devices and information systems, among information systems and end-users – citizens or organizational

entities, and among different government entities and organizations. The key aspect in addressing these communication problems is the adoption of high-quality protocols, metadata and algorithms to handle the discussed heterogeneity. The research community has already devoted attention on this challenge through the development of applications for heterogeneous devices. Middleware is significant to solve the aforementioned problem and facilitate the collection of data from homogeneous or heterogeneous IoT devices. The burden mainly lies in the collection of data from sensors and subsequently their transformation into a unified representation for further processing. On top of the unified data, efficient interfaces can be provided to facilitate the access to the collected data, thus, to generate knowledge over them. This way, end users can attach their devices to Cloud interfaces and 'upload' sensors measurements through lightweight APIs. It should be noted that in such cases, the management of large-scale data is significant for further processing and delivering results that can be useful in e-government applications.

Interoperability

Interoperability facilitates the exchange of information between communicating entities, citizens or public and private bodies. In particular, data interoperability enables different bodies share information and increase the efficiency through the mitigation of the data inconsistencies. In addition, data interoperability can help in avoiding duplications of data, thus allowing for saving storage and resources. To support the 'connection' of heterogeneous data, different data models can be combined into a single model that covers the desired application domain. The delivered model should meet requirements like reliability, performance, scalability, heterogeneity coverage and interoperability. This way, we can deliver e-government services in the minimum time with high quality incorporating a low cost. As described in Cenci et al., (2017), the European Interoperability Reference Architecture (EIRA) (Chou et al., 2015) uses a service-oriented architecture and the Open Group's ArchiMate ontology and tools as its reference model. EIRA interoperability is defined through a set of architecture building blocks, i.e. technical, semantic, organizational and legal. Technical Interoperability involves the planning for technical issues involved in linking computer systems and services. Semantic Interoperability is related to giving precise meaning to the exchanged information while organizational interoperability refers to coordinated processes between different entities. Finally, legal interoperability refers to the aligned legislation so that exchanged data is accorded proper legal weight.

Security

Security is another challenge for the adoption of the IoT in e-government. Numerous devices can have access to e-government services present in the Cloud, thus, it is imperative to secure the authorized access to data collected, generated or inserted. This aspect of the problem is more intense for sensitive personal data. Cloud architectures already provide security mechanisms for accessing their services, however, the autonomous nature of the IoT nodes imposes additional challenges. A lot of discussion can be done about the danger of the hacking of devices and systems to obtain information and data. Another danger is potential cyber-attacks against the devices themselves; attacks which take over control of the device and cause them to operate in dangerous and insecure ways. Due to the complexity of the architecture of the IoT e-government services, a solution for the security of the applications could be the adoption of multi-layered security services. Firewalls, security protocols, authentication, encryption and intrusion detection mechanisms can be employed to e-government IoT systems to provide the necessary level of security.

Infrastructure

The use of IoT in e-government also poses a challenge related to the technical resources that are needed for data collection, transfer, processing and storage. A physical infrastructure should be in place including sensors, actuators, digital tags and their addition to devices as well as their network connection allowing them to generate and share data. The plethora of data collected by IoT systems

create a need for storage and processing infrastructure with high capacity to accommodate the volume of data as well as the speed with which they are generated. Access to IoT e-government data should be controlled and at the same time be fast and facilitate queries and response for efficient service provision. IoT e-government systems should support efficient data analytics capabilities for informed decision making in real time and at large scale. E-government cloud infrastructures can be created and used to satisfy storage and processing requirements of IoT data and services in conjunction with their security requirements. The advent of advanced network technology, such as 5G, LPWAN and IPv6, is also required to provide the connectivity for transferring the high volume of IoT data fast and reliably and for offering timely services to end users.

IoT smart government is enabled by technologies that help transform objects into smart things. RFID can be used for tagging an object thus giving a unique identifier to each smart thing (Jin et al., 2014). Sensors and WSNs enable the measurement of physical quantities and the transformation to digital signals, which are processed wirelessly by an ad-hoc network infrastructure (Ma, 2014). Low-power radio communications and low-cost embedded devices enable sensors to incorporate RFID tags (Vakali et al., 2014). Actuators are adopted to stimulate and give feedback to digital systems by interacting, in the physical layer, with the infrastructure (Jara et al., 2014). Future Internet provides interconnection to smart things with IPv6 over Low Power Wireless Personal Area Networks (6LoWPAN) protocol, a modified version of IPv6 for low-power embedded devices (Theodoridis et al., 2013). In addition, many IoT system architectures are built on Cloud Infrastructure (i.e., OpenIoT) (Suciu et al., 2013), enabling the concept of Infrastructure as a Service (IaaS) (Fortino et al., 2014). Energy requirements and limitations of IoT infrastructure also have to be taken into account for smart government as the autonomy of IoT devices, particularly of mobile unmanned vehicles (UAV, UGV, USV), is a critical success factor of any endeavor that involves them.

Artificial Intelligence

Another challenge for adopting IoT in e-government lies in the incorporation of Artificial Intelligence (AI) in e-government applications. AI can provide the means for building intelligent applications over the collected data from diverse sources. With the adoption of AI, the provided e-government applications will be capable of supporting human-like reasoning and activities. Machine learning may empower devices and systems with the ability to detect patterns, take decisions autonomously or learn from the adopted models and adjust any decision based on the status of the environment. The benefit of using such technology is that systems need not be fully 'programmed' in advance, but they can learn the correct line of actions during their functioning. This ability to embed learning capabilities within the IoT device itself, and in addition, marry device-centric insights with aggregated intelligence in the Cloud, is expected to dramatically improve outcomes (Cooke, 2018).

Non-Technical Challenges

IoT in e-government goes beyond technical challenges and comprises non-technical ones, which are of equal, if not greater importance. These challenges comprise a wide range of organizational, political, financial, institutional and legal issues. They can greatly influence the effectiveness of any endeavour in leveraging IoT technological possibilities in e-government systems. They should be carefully be taken into account and handled, particularly because of their inherent complexities as well as their multilateral interdependencies which render them hard to manage. The rest of this section presents our perspective of the non-technical challenges associated with the successful use of IoT in e-government systems and services.

Political Context and Vision

Several issues can affect the decisions that need to be made and the actions that will follow them regarding the utilization of IoT technology for e-government purposes at strategic, tactical and operational level. Decisions and actions can concern the extension of current e-government systems

and services or the development of new ones for utilizing IoT. Such decisions about plans and actions for pursuing smart government projects with IoT need not necessarily be driven by top government but they can rather start at local authority level. In any case, IoT-based information systems and services should be designed so as to be aligned with government or local administration strategy and objectives. Setting and applying such initiatives is a hard political and social task. Any IoT-based e-government application implies approval and acceptance by government administration, of local or greater level, depending on the aim and scope of the e-government system and the community or the society to which it is addressed. This requires changes in the mentality of the authorities and citizens that the IoT-oriented system serves and affects, in their mode of operation and work and even in individual lifestyle and behavior. As with any new technology introduced, resistance to change in organizations and citizens is hardly inevitable and should be taken into consideration in IoT e-government initiatives. Such changes and anticipated reactions can be managed effectively if they are driven by strong support from the respective government authorities.

Organizational Reform

The introduction of IoT in e-government calls for organizational reform and process redesign, in order to allow for the adaptation of current government services or the introduction of new ones, based on IoT. This may entail the need for the creation of new government bodies and institutions or organizations as well as the formation of co-operations and coalitions that will facilitate the effective development and use of IoT-oriented e-government services. Such services can be deployed at either organizational or interorganizational level, involving the connection of different entities that should cooperate and depend on each other in a seamless and integrated mode of operation. The provision of interorganizational services implies the need for interoperability, not only of the data exchanged among involved entities but also of the organizations themselves, sharing processes and policies that enable their communication.

Financial Resources

As mentioned, the transition to IoT-enabled e-government requires the existence and availability of the appropriate infrastructure and resources, such as 5G telecommunication networks. These, in turn, require strategic investments for their implementation and use. Financial support for IoT e-government services, including sufficient funding as well as appropriate billing schemes, is essential for their feasibility and sustainability. As e-government services are largely non-profit and aim to serve the public interest, revenue models have to take into account the social, commonwealth purpose of IoT applications, especially in sectors such as healthcare. Revenue can be generated either directly by efficient pricing policies that are affordable and adaptable to end users or indirectly by the cost reduction resulting from the IoT solution. Financial schemes can involve various stakeholders and bodies coming from the public or the private sector and being part of the academia or the industry.

Institutional and Legal Framework

IoT-based information systems and services need to be formally acceptable by institutional structures, fulfil legal requirements and comply with regulations. Therefore, the effective adoption of IoT in e-government requires strong institutional support. At the same time, institutions and legislation itself can drive IoT adoption by governments, enforcing technological evolution and its application in its operation. For example, Estonia as part of its program for 2020 plans to implement the “no legacy principle” which will be introduced by law, meaning that the public sector should not adopt any kind of Information Communication Technology solution that is older than 13 years (e-Estonia, 2018). In a similar vein, institutional support is needed to overcome bureaucracy and other typical burdens faced in the public sector.

Security, Privacy and Trust

Security and privacy of data are aspects that cross horizontally almost every IoT e-government application. Apart from their technical characteristics, security and privacy are prominent issues of IoT e-government with aspects that also request a non-technical approach. Security is imperative for high risk services such as energy power production and management plants or environment protection. In addition to technical mechanisms, non-technical measures such as access control, management processes and security policies are also needed for risk mitigation. Similarly, the protection and control of personal data is also required in practically all sectors of IoT-based e-government, especially in highly sensitive applications such as healthcare. IoT government applications need to be trusted by citizens in order to be accepted and used. Ensuring security and privacy, as well the quality of the information and services of are fundamental for IoT e-government to gain the trust of individuals, organisations and the society in general. Regulations and procedures should be in place to guarantee the availability, high quality and safe use of the provided IoT-oriented e-government services without jeopardizing security and data privacy. At the same time, imposing security and privacy rules and policies should not be in the expense of IoT-based systems usability.

Synergies

The effectiveness of IoT adoption in e-government should be facilitated by being realized in cooperation with academic and research institutions and with synergies between the public and private sector. This will enable the development of IoT systems and services, and the infrastructure needed for their effective support. Public-private sector partnerships are identified as an important factor for the successful use of IoT in e-government as shown in the World Bank Group (2017) report by lessons learnt during the actual implementation of IoT-oriented projects in several countries. Such partnerships can also help towards the development of IoT-based business models that allow for sustainability and affordability. This is highlighted in the previously mentioned report, which denotes a lack of IoT-specific government-to-business models and policies. The same report also reveals that there is a lack of understanding of IoT and its data value and management needs. This implies a need for raising awareness and improving knowledge on IoT and the role it can have in government contexts. This can be addressed towards all potentially involved parties through education and partnerships among academic, government and business entities, constituting a vital component of governments strategic planning along with IoT-based project design and implementation.

IoT-BASED E-GOVERNMENT: AN APPLICATION CASE AND CHALLENGES

Having discussed the application domains as well as the challenges associated with the adoption of IoT in e-government, we proceed to examine them through a specific example case. This section describes the application of an IoT-based e-government system in providing alerts for weather phenomena showing the challenges associated with it and the response to them for their solution. Assume a number of smart devices placed on a set of road vehicles with routing functionalities. End users may use these devices to calculate the optimal path for their activities. In this setting, they may use a smart government service which is capable of monitoring and processing device location data and meteorological data to derive decisions and issue alerts in relation to intense meteorological events. The service is delivered by the Civil Protection department of the Ministry of Internal affairs, in cooperation with the National Meteorological Service and the Ministry of Transportation. The service is placed in the central, cloud infrastructure to increase efficiency and benefit from the increased computational capabilities while IoT nodes change their location as citizens move. IoT devices are subscribed in the aforementioned service and are ready to receive data related to alerts for emergency weather phenomena. As IoT devices are mobile, they should update their location in the central service. This is automatically performed through the exchange of lightweight messages,

so that the central system is capable of knowing the location of the end users. Suppose the discussed service identifies intense meteorological events in a specific area. This area is continuously updated as the events are realized. The central system can perform a simple reasoning process and group the end users in a set of clusters according to the risk of being affected by the phenomenon. The groups are continuously updated during the realization of the phenomenon to keep up with the changes in its intensity and location. Spatio-temporal clustering is employed to continuously generate clusters of IoT nodes, avoiding network flooding and enabling location-based and targeted information push. Specific warning messages are delivered to users belonging to groups that are affected or will be affected by the phenomenon. IoT nodes after the reception of the aforementioned messages can easily update their operation, e.g., update their routing and follow a different route. In this way, the IoT e-government service can monitor and inform citizens in order to avoid intense weather phenomena and move safely without traffic congestion problems. The challenges, technical and non-technical, associated with the described case and the proposed solutions to address them are presented in Table 2.

As it can be seen, this e-government service can easily be combined with systems that track the activity of end users as they are moving around and utilize it not only to update their location but also to update the IoT node operation. This location-based service can be easily incorporated in the IoT e-government systems; however, it should be enhanced by techniques for handling the heterogeneity of the devices and their interoperability for the functions they perform. Security measures and AI mechanisms should also be employed. IoT nodes can be grouped for offering targeted services as well as network load balance. In this way, the e-government service can target specific groups of users and support multiple roles. The modular, role-based approach can increase the efficiency in the delivery of data creating the basis for a personalized e-government service. However, the required monitoring of citizens and IoT devices, with the activity tracking and location-based data exchange for the targeted service, can only be enabled given that the security and privacy of citizen data are respected, and after user consent. In addition, the service is the result of the synergy of the involved government authorities and entities, which should undergo several changes in their procedures to cooperate effectively. This is preceded by a political decision and action in favor of the provision of the service, endorsed with the appropriate legal coverage and financial support.

CONCLUSION

The use of IoT in e-government can be extremely valuable as it offers the possibility for a wide range of applications and services that can be available and beneficial to the public. IoT-based systems can enable the provision of new, innovative e-government services or ameliorate and complement the existing ones. This paper seeks to contribute to a better understanding of the potential of IoT in e-government and how such potential could be reached. The aim is to examine IoT use highlighting the benefits as well as the challenges that come with introducing it in e-government. The analysis of IoT in e-government with regards to the application domains, the technical and non-technical challenges and the example case presented can offer useful insights that can be of interest for both researchers and practitioners. As shown in our analysis, IoT enables advanced e-government services that can be sustainable and efficient and which could not be previously affordable or even possible. IoT can allow for the effective treatment of security and safety needs of the public sector through the sensing, processing and communication capabilities of autonomous devices. Critical areas, in aerial, maritime and ground contexts, can be greatly benefited by being monitored with the use of IoT technology to facilitate appropriate and timely action. In particular, the use of mobile IoT devices can enable a wide range of activities related to security and safety, such as the surveillance and monitoring of areas, the detection of threats, the effective management of events, the fast response to emergency situations, the alerts about security/safety risks and the communication of current status to people. Such IoT empowered activities can be applied to a number of contexts such as border surveillance and control for trespassing, healthcare, transportation, weather monitoring and forecasting for intense

Table 2. IoT challenges and responses

Challenge		Response
Technical	Heterogeneity	A publish-subscribe model can enable the interaction with different devices. The use of an end point where end users' devices can be 'hooked' and receive information. The end point will be controlled by the appropriate software while supported by a model for data exchange.
	Interoperability	The use of a data model and software that will align the heterogeneous data in an automatic manner, preventing the system from having to deal with different data formats and semantics
	Security	The back-end system should be secured against unauthorized access through access control techniques. This is very important due to the criticality of the application. In addition, the security mechanisms should also be applied on the end users devices to avoid the generation and spread of fake messages.
	Infrastructure	Mobile IoT nodes are needed, grouped with spatiotemporal clustering, and also a central cloud infrastructure where the service resides, capable of meteorological data processing and location-based and role-based decisionmaking and message exchange. The service also presupposes the existence of mobile network connectivity to cover the communication needs of mobile IoT nodes.
	AI	AI can be included in the reasoning process for events identification as well as in the clustering of end users. Complex event processing, pattern identification, classification and prediction can assist in events detection that will fire the creation of messages for end users. In addition, clustering can be performed on top of multivariate data to depict not only the current position of users but personalized aspects like their ability to respond in emergency scenarios. For instance, the instructions to end users can differ based on their personal characteristics and their initial route.
Non-Technical	Political context and IoT vision	Political decisions and actions by government administration are needed for setting and applying a policy for using IoT for the provision of e-government services and particularly for the provision of the specific service for warning against weather phenomena. The envisioned endeavour should take involve all relevant parties and be planned to be realised within a feasible timeframe and cost
	Organizational reform	The provision of such interorganizational services implies the need for interoperability not only of the data exchanged among the involved entities but also of the organizations themselves, sharing processes and policies that enable their communication. This entails changes in the structure and operation of the involved Ministries and bodies
	Financial resources	Funding is needed for the development of the government cloud infrastructure and the provided service. Funding might also be needed to citizens for encouraging the addition of IoT nodes to vehicles. If charges apply for the use of the service a pricing policy is also needed.
	Institutional and legal framework	A legal framework with the appropriate laws and regulations should be in place to allow the use of the service, including coverage for data collection and use, in real-time, particularly for data related to user location and movement tracking
	Security, privacy and trust	Providing a trustworthy to use service by enabling the collection and use of real-time geo-positioning data and activity tracking whilst protecting citizens security and privacy and after user consent in the intended data collection and use
	Synergies	The implementation of the service requires the collaboration of government bodies such as the Civil Protection department of the Ministry of Internal affairs with the National Meteorological Service and also with the Ministries of Transportation and Communication

or dangerous phenomena, environmental pollution detection, earthquake monitoring and alerts, fire detection in forests and rural areas, monitoring of water level in rivers, lakes and the sea for avoiding floods or quality control of water for drinking and agriculture. We believe that these critical public services are where IoT can bring most value to e-government. Furthermore, our work suggests that the successful implementation of IoT-based e-government systems can be deemed as primarily technology-driven. It is the enabling infrastructure, technologies and solutions overcoming issues such as the heterogeneity of devices, interoperability and security that are required for making IoT government services feasible and available to the citizen and the society. However, the introduction and adoption of IoT e-government is also driven by political decisions and actions. In addition, planning and implementation of IoT applications implies requirements and changes of organizational and economic nature, regarding processes, policies and investments, whilst setting the need for an appropriate legal and regulatory framework that enables the IoT e-government and the changes implied. Cooperation of different entities is essential for the provision of IoT e-government services, in ways that protect citizen security and privacy. All of these aspects, jointly and each of them separately, are important contributors to the success of IoT-oriented e-government. This might request the cooperation of all involved parties from the public sector or the industry in a specific domain of interest for defining IoT vision and policies for e-government. This holistic approach of IoT e-government can serve as a starting point for further study and work in this promising field.

REFERENCES

AlEnezi, A., AlMeraj, Z., & Manuel, P. (2018). Challenges of IoT based Smart-government Development. In Proceedings of the 2018 IEEE Green Technologies Conference (GreenTech) (pp. 155-160). IEEE Press. doi:10.1109/GreenTech.2018.00036

Alphonsa, A., & Ravi, G. (2016). Earthquake early warning system by IOT using Wireless sensor networks. In *Proceedings of 2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET)*. Academic Press. doi:10.1109/WiSPNET.2016.7566327

Amjath Ali, J., Thangalakshmi, B., & Vincy Beaulah, A. (2017). IoT Based Disaster Detection and Early Warning Device. *International Journal of MC Square Scientific Research*, *9*(3), 20–25. doi:10.20894/IJMSR.117.009.003.003

Babu, A. S., Naidu, G. T., & Meenakshi, U. (2018). Earth Quake Detection And Alerting Using IoT. *International Journal of Engineering Science Invention*, *07*(05), 14–18.

Brous, P., & Janssen, M. (2015a). Advancing e-Government Using the Internet of Things: A Systematic Review of Benefits. In E. Tambouris et al. (Eds.), *Electronic Government EGOV 2015*. Cham: Springer. doi:10.1007/978-3-319-22479-4_12

Brous, P., & Janssen, M. (2015b). A Systematic Review of Impediments Blocking Internet of Things Adoption by Governments. In M. Janssen et al. (Eds.), *Open and Big Data Management and Innovation I3E 2015*. Cham: Springer. doi:10.1007/978-3-319-25013-7_7

Burkhalter, M. (2018). How IoT infrastructure allows for more accurate weather forecasting. Perle. Retrieved from https://www.perle.com/articles/how-iot-infrastructure-allows-for-more-accurate-weatherforecasting-40169629.shtml

Business Insider Intelligence. (2019). The Internet of Things Report. Retrieved from https://store.businessinsider.com/products/the-internet-of-things-report

Cenci, K., Fillottrani, P., & Ardenghi, J. (2017). Government Data Interoperability: A Case Study from Academia. In Proc. of the ICEGOV. Academic Press. doi:10.1145/3047273.3047382

Chou, B. C. C. H., Chou, B. C. C. H., Archive, F. D., Archive, F. D., Goethals, A., & Goethals, A. (2015). *An introduction to the European Interoperability Reference Architecture v0.9.0*. EIRA.

Columbus, L. (2018). Where IoT can deliver the most value in 2018. Forbes. Retrieved from https://www.forbes.com/sites/louiscolumbus/2018/03/18/where-iot-can-deliver-the-most-value-in-2018/

Cooke, A. (2018). Realising the future and full potential of connected IoT devices with AI. Silicon Republic. Retrieved from https://www.siliconrepublic.com/enterprise/ai-iot-automation-ibm

Coppolino, L., D' Antonio, S., & Romano, L. (2014). Exposing Vulnerabilities in Electric Power Grids: An experimental approach. *International Journal of Critical Infrastructure Protection*, *7*, 51–60. doi:10.1016/j.ijcip.2014.01.003

e-Estonia. (2018). Internet of Things paves the way for smart B2G solutions. Retrieved from https://eestonia.com/internet-of-things-way-for-b2g-solutions/

El-Haddadeh, R., Weerakkody, V., Osmani, M., Thakker, D., & Kapoor, K. K. (2018). Examining citizens' perceived value of internet of things technologies in facilitating public sector services engagement. *Government Information Quarterly*. doi:10.1016/j.giq.2018.09.009

Fan, X., & Gong, G. (2013). Security Challenges in Smart-Grid Metering and Control Systems. *Technology Innovation Management Review*, *3*(7), 42–49. doi:10.22215/timreview/702

Fortino, G., Guerrieri, A., Russo, W., & Savaglio, C. (2014). Integration of agent-based and Cloud Computing for the smart objects-oriented IoT. In *Proceedings of the IEEE 18th International Conference on Computer Supported Cooperative Work in Design (CSCWD)* (pp. 493-498). IEEE Press. doi:10.1109/CSCWD.2014.6846894

Hounsell, N. B., Shrestha, B. P., Piao, J., & McDonald, M. (2009). Review of urban traffic management and the impacts of new vehicle technologies. *IET Intelligent Transport Systems*, *3*(4), 419–428. doi:10.1049/iet-its.2009.0046

Jara, A. J., Lopez, P., Fernandez, D., Castillo, J. F., Zamora, M. A., & Skarmeta, A. F. (2014). Mobile discovery: Discovering and interacting with the world through the Internet of Things. *Personal and Ubiquitous Computing*, *18*(2), 323–338. doi:10.1007/s00779-013-0648-0

Jin, J., Gubbi, J., Marusic, S., & Palaniswami, M. (2014). An Information Framework for Creating a Smart City Through Internet of Things. *Internet of Things Journal*, *1*(2), 112–121. doi:10.1109/JIOT.2013.2296516

Kim, T.-H., Ramos, C., & Mohamed, S. (2017). Smart City and IoT. *Future Generation Computer Systems*, *76*, 159–162. doi:10.1016/j.future.2017.03.034

Kumar, S. P. (2017). Internet of Things for sophisticated e-governance: A special focus on agricultural sector. *International Journal of Trend in Research and Development*.

Lingling, H., Haifeng, L., Xu, X., & Jian, L. (2011). An Intelligent Vehicle Monitoring System Based on Internet of Things. In *Proceedings of the IEEE 7th International Conference on Computational Intelligence and Security* (pp. 231-233). IEEE Press.

Lopez, T. S., Ranasinghe, D. C., Harrison, M., & Mcfarlane, D. (2012). Adding sense to the Internet of Things. *Personal and Ubiquitous Computing*, *16*(3), 291–308. doi:10.1007/s00779-011-0399-8

Ma, J. (2014). Internet-of-Things: Technology evolution and challenges. In *Proceedings of the IEEE MTT-S International Microwave Symposium (IMS)* (pp. 1-4). IEEE Press.

McKinsey. (2018). The Internet of Things: How to capture the value of IoT. McKinsey & Company. Retrieved from https://www.mckinsey.com/featured-insights/internet-of-things/our-insights

Reports and Data. (2019). Smart Governments Market By Deployment (Cloud And On-Premises). Retrieved from https://www.reportsanddata.com/report-detail/smart-governments-market

Schwertner, K., Zlateva, P., & Velev, D. (2018). Digital technologies of industry 4.0 in management of natural disasters. In *Proceedings of the 2nd International Conference on E-commerce, E-Business and EGovernment*. Academic Press.

Sideridis, A., & Protopappas, L. (2015). Recent ICT Advances Applied to Smart e-Government Systems in Life Sciences. In *Proceedings of the 7th International Conference on Information and Communication Technologies in Agriculture, Food and Environment (HAICTA 2015)*. Academic Press.

Sideridis, A. B., Protopappas, L., Tsiafoulis, S., & Pimenidis, E. (2015). Smart Cross-Border e-Gov Systems and Applications. In S. Katsikas & A. Sideridis (Eds.), *E-Democracy – Citizen Rights in the World of the New Computing Paradigms. e-Democracy 2015*. Cham: Springer.

Suciu, G., Vulpe, A., Halunga, S., Fratu, O., Todoran, G., & Suciu, V. (2013). Smart Cities Built on Resilient Cloud Computing and Secure Internet of Things. In *Proceedings of the IEEE 19th International Conference on Control Systems and Computer Science (CSCS)* (pp. 513-518). IEEE Press. doi:10.1109/CSCS.2013.58

Tang, T., & Ho, A. T.-K. (2018). A path-dependence perspective on the adoption of Internet of Things: Evidence from early adopters of smart and connected sensors in the United States. *Government Information Quarterly*. doi:10.1016/j.giq.2018.09.010

Theodoridis, E., Mylonas, G., & Chatzigiannakis, I. (2013). Developing an IoT Smart City Framework. In *Urban Computing & Modern Cities Workshop, IEEE 4th International Conference on Information, Intelligence, Systems and Applications (IISA)* (pp. 1-6). IEEE Press. doi:10.1109/IISA.2013.6623710

Thibaud, M., Chi, H., Zhou, W., & Piramuthu, S. (2018). Internet of Things (IoT) in high-risk environment, health and safety (EHS) industries: A comprehensive review. *Decision Support Systems*, *108*, 79–95. doi:10.1016/j.dss.2018.02.005

Vakali, A., Anthopoulos, L., & Krco, S. (2014). Smart Cities Data Streams Integration: experimenting with Internet of Things and social data flows. In *Proceedings of the 4th ACM International Conference on Web Intelligence, Mining and Semantics (WIMS'14)*. ACM. doi:10.1145/2611040.2611094

Wirtz, B. W., Weyerer, J. G., & Schichtel, F. T. (2019). An integrative public IoT framework for smart government. *Government Information Quarterly*, *36*(2), 333–345. doi:10.1016/j.giq.2018.07.001

World Bank Group. (2017). Internet of Things: The New Government to Business Platform. Retrieved from http://documents.worldbank.org/curated/en/610081509689089303/pdf/120876-REVISED-WP-PUBLICInternet-of-Things-Report.pdf