Integration of IoT into e-government

Shao, Deo; Ishengoma, Fredrick R.; Alexopoulos, Charalampos; Saxena, Stuti; Nikiforova, Anastasija; Matheus, Ricardo

DOI
10.1108/FS-04-2022-0048

Publication date
2023

Document Version
Final published version

Published in
Foresight

Citation (APA)
Shao, D., Ishengoma, F. R., Alexopoulos, C., Saxena, S., Nikiforova, A., & Matheus, R. (2023). Integration of IoT into e-government. *Foresight*, *25*(5), 734-750. https://doi.org/10.1108/FS-04-2022-0048

Integration of IoT into e-government

Deo Shao, Fredrick R. Ishengoma, Charalampos Alexopoulos, Stuti Saxena, Anastasija Nikiforova and Ricardo Matheus

(Information about the authors can be found at the end of this article.)

Abstract

Purpose – *The purpose of this paper is to highlight the drivers, barriers, benefits and risks affecting the integration of Internet of Things (IoT) into the e-government and to provide a future research agenda.*

Design/methodology/approach – *Existing literature examining the relationships between e-government and IoT is scanned and evaluated by conceptualizing the IoT concept in the e-government perspective.*

Findings – *The study shows that there are drivers to integrate IoT in e-government, such as ensuring the economy, efficiency and effectiveness of government operations, which would largely establish a relationship between the government and the citizens. Furthermore, there are barriers to such integration, given the lack of political will, the appropriate information technology infrastructure, the training of the stakeholders with a focus on the employee and the like.*

Originality/value – *The integration of IoT in e-government is a novel and weakly explored concept, particularly in the light of new advances such as blockchain in the e-government, which requires further exploration and conceptualization, thereby achieving a shared/common vision and body of knowledge for its further successful and sustainable adoption – to the best of the authors' knowledge, the current study is one of these initial attempts.*

Keywords *IoT, Internet of things, E-government, E-governance, Electronic government, Barrier, Driver, Integration, Digital transformation, Sustainability*

Paper type *Research paper*

1. Introduction

With the development of information technology (IT) and information and communications technology (ICT), as well as the increasingly diverse needs of citizens, governments sought to provide public services through the internet, which became known as e-government. The objective of the adoption of IT in the provision of public services was to establish a connection with users and to provide public services in an economic, efficient and effective manner. In this respect, the Internet of Things (IoT) seen as an emerging as one of the major trends shaping the development of technologies in the ICT sector (Miorandi *et al.*, 2012), which transformation potential has been a topic of interest both in literature and practice for decades, has been an important breakthrough in the field of intelligent and smart technologies.

It is also tend to be characterized as "the most revolutionary and attractive technology of today without which it is nearly impossible to imagine the future due to its application in numerous fields such as smart cities, home automation, wearable devices, etc., and its ability to make human life much easier via integration with other technologies such as cloud "computing and artificial intelligence" (Bansal *et al.*, 2022). This paradigm shift (an internet used for interconnecting end-user devices to IoT) leads to rethink some of the traditional approaches commonly used in networking, computing and service management (Miorandi *et al.*, 2012; Pinochet *et. al.*, 2018). As a result, it is capable of transforming government into smart government.

Received 28 April 2022
Revised 8 November 2022
20 December 2022
Accepted 29 January 2023

This paper addresses the call by Oke and his colleagues (Oke *et al.*, 2023) that "Government is also encouraged to adopt the principles of IoT [. . .] to improve the economy of the nation". By lending credence to the assertion that disruptive technologies ought to be integrated in the administrative systems (Ronzhyn *et al.*, 2019), the current study argues that the integration of IoT into e-government could lead to a revolution in the provision of public service. Two research questions are raised and expected to be answered:

RQ1. What are the drivers and barriers to the integration of IoT into e-government?

RQ1. What are the benefits and risks to the integration of IoT in e-government?

To answer the above-defined research questions, the study provides a background building a common knowledge base based on previous literature (Section 2), provides a brief on the methodology adopted for the present purpose (Section 3), identifies potential drivers to IoT integration into e-government (Section 4), identifies potential barriers to IoT integration into e-government (Section 5), outlines the benefits of integrating IoT into e-government (Section 6) and determines the risks of integrating IoT into e-government (Section 7). Section 8 concludes the study and Section 9 provides a brief on the practitioner implications.

2. Background

Firstly, given the variety of definitions of both concepts, i.e. IoT and e-government, let us briefly discuss these concepts and provide coherent definitions.

2.1 Internet of Things

In general, the IoT has been defined as "everyday objects that can sense the environment around them and communicate that data to other objects and services via the Internet" (Hoy, 2015, p. 353). According to Hoy (2015), it is important to note that this term refers to a combination of several distinct ideas: a large number of heterogeneous "smart objects", which refers to "things" in the "Internet of Things" term, all connected to the internet, with applications and services that use data from these objects to create interactions. Miorandi *et al.* (2012) described it with the three major pillars, according to which the above-mentioned "smart objects" should be identifiable, be able to communicate, be able to interact with each other and build networks of interconnected objects or with end-users or other network entities.

The question, which could arise here, is what the term "smart object" stands for? Miorandi *et al.* define them as entities that have a physical embodiment and a set of associated physical characteristics such as size and shape; have a minimal set of communication functions, such as the ability to be discovered and to accept incoming messages and respond to them; have a unique identifier; are associated with at least one name and one address, where the name is a human-readable description of the object and can be used for reasoning purposes, while the address refer to a machine-readable string that can be used to communicate with the object; have some basic computing capabilities, which can range from the ability to match an incoming message with a specific footprint and ending with the ability to perform complex computations, including discovery of services and network management tasks; may be means to sense physical phenomena such as temperature, light, electromagnetic radiation level or to trigger actions that affect on physical reality/actuators.

Today, IoT has an increasing number of applications, including production and manufacturing, where it promotes the inspection, instrumentation and information factories to improve quality and productivity, logistics, where this means a unique identifier for individual items, so that supply chains can become more robust and "smart", development of new products and services, where it supports the development of smart, connected

products that provide information about their state so that information can be used to improve the operations the products support, disaster management, retail sector, smart cities and other areas (De Franca *et al.*, 2021; Pawar *et al.*, 2021; Wahyudi *et al.*, 2017). All in all, IoT-based technologies aim at enabling organizations and individuals to make better informed decisions, to be more productive and to improve health and quality of life.

The IoT uses devices to exchange data and act based on that data. It is also possible that a group of devices cooperate to achieve a common goal and communicate via the internet. There may be a variety of scenarios in which developing applications to harness the data collected by these devices will provide e-government with strategic, tactical and operational advantages. The IoT collects a large amount of big data has the potential of increasing transparency and openness. Citizens and businesses can use the data to improve self-service, ensure proper oversight, reduce labour and fraud costs, automate security and improve process efficiency.

2.2 E-government

E-government is a paradigm that aims to support, improve and change government activities to modern ways through digital technologies. The development of e-government has had a big impact on government-citizen interaction because it makes it easier for citizens to exercise their democratic rights and help run the state (Engin and Treleaven, 2019) besides furthering accountability and transparency (Saxena, 2017). E-government can be defined as a digital traditional government model built using a variety of ICT, including but not limited to IoT, cloud computing and machine learning (ML). Its aims are to enhance the access to and delivery of government/public services to benefit citizens, business partners and employees, as well as to increase the participation of citizens in the governmental activities electronically (e.g. IoT-based online voting) and thereby remotely (Bansal *et al.*, 2022; Silcock, 2001). It also gained an increased popularity and demonstrated benefits in sectors such as health, education and agriculture, gaining popularity for unmanned aerial vehicles. However, other sectors also serve as positive examples and include but are not limited to the environment (water and air pollution, disaster prediction, etc.), where the IoT and ML are combined with the active use of social network analysis.

E-government is considered to be an indispensable part of a smart city that uses ICT to transform relationships between public authorities/government bodies and citizens, businesses and other government departments to improve government services, improve interactions and increase the efficiency of governmental operation.

The e-government paradigm has evolved due to the increase in the degree of adoption of digital technologies. Its first-generation, called “e-government 1.0”, used ICT to support and transform government agencies’ complicated internal processes to make them more efficient. Later, with the widespread use of the internet, it shifted its focus to providing transactional services to citizens and businesses through electronic channels like the internet and, later, the mobile phone. Next, the “e-government 2.0” generation of e-government came about because of the widespread use of social media and the widespread ideas about open and participatory government that people shared. It was all about how to use the internet, especially social media, to make it easier for people to be involved, be more transparent and work together. A new type of e-government called e-government 3.0 has come out in the past few years. The e-government 3.0 focuses on leveraging digital technology to help government people make smart decisions and policies about how to solve problems in the world is one of its main goals. The e-government 3.0 uses digital technology to support evidence-based decisions about solving problems in the world like big data, AI, data mining and the IoT (Kim, 2013).

2.3 Summing up

Integration of theoretical concepts in significant in research involving integration of phenomena based on identification, observation and appreciation of the commonalities and even the differences between them (Gigerenzer, 2017). In the present study, the selection of theoretical concepts of IoT and e-government was not arbitrary but reflective of the observations, and the necessity for contribution towards the body of knowledge (Lysaght, 2011) also provides a rationale for application in the actual governmental settings. Given that multiple theories lend diverse perspectives on a specific theme, the present study sought to align the theoretical concepts to the overarching research objectives (Grant and Osanloo, 2014).

Bansal *et al.* (2022) referred to the concept of "smart" government and its realization by mean of fog computing with IoT, which resulted in the Fog-of-Things architecture. The authors divide it in "extensions smart government", which is described as a admin-centric and not transparent combination of an e-government and smart cities; and "next generation smart government" described as a people-centric and transparent form of smart government, which takes features of government 2.0 and smart cities. The authors, however, acknowledge the set of challenges or barriers to be overcome. The issue of the IoT adoption by government and identification of the impediments blocking it was originally addressed by Brous and Janssen (2015) emphasizing limited literature on the IoT in the e-government domain, and lack of determination of barriers affecting its adoption in general, particularly pointing on the lack of a systematic analysis. They find that these impediments are interrelated and occur on the strategic, tactical and operational level, which should be resolved jointly rather than independently/one-by-one. They have identified and classified possible impediments into:

- strategic/political barriers associated with data privacy issues, data security issues, weak or uncoordinated data policies, weak or uncoordinated data governance and conflicting market forces;
- tactical barriers, referring to costs, interoperability and integration issues, acceptance of IoT and trust-related issues; and
- operational referred to a lack of sufficient knowledge regarding IoT, IT infrastructural limitations and data management issues.

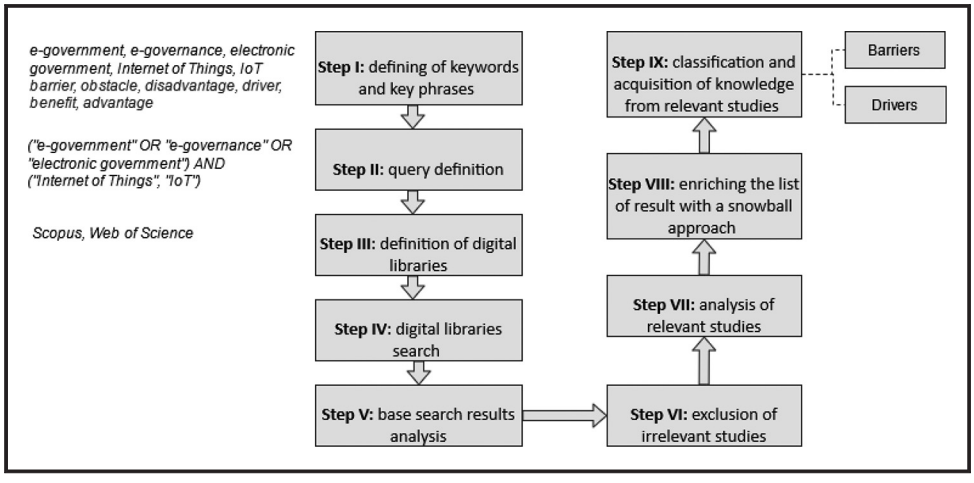
Their further analysis of two IoT case studies has proved the compliance of this classification with the real world, although some of the above-mentioned impediments were less expressed, i.e. data security, costs, IT infrastructural limitations and data management issues.

In general, both concepts have common objectives in some sense, i.e. to improve the quality of services and quality of life as a whole through technology. This makes the combination of both logical and almost self-evident "must have", yet they have some potential barriers, which governments face. It is therefore important to be aware of them to be able to deal with them, preferably in a preventive manner, i.e. before they actually intervened. The IoT paradigm is deemed to make e-government 3.0 a reality while also ensuring that the new technology has the intended effect, thanks to new ubiquitous, integrated, intelligent and universal devices. Indeed, IoT is considered the backbone of smart governments. IoT may be defined as internet-connected sensors that, among other capabilities, enable companies to monitor individuals. However, there is not a lot of research on IoT in the field of e-government to help find the nexus between the two (Brous and Janssen, 2015; Kankanhalli *et al.*, 2019) – the present research seeks to underline this nexus.

3. Methodology

For the purpose of this study, we performed a systematic literature review based on keyword search (Figure 1). Looking for all articles related to the topic of the question, we

Figure 1 Methodology adopted in the study



searched for all the articles falling in the IoT and e-government. As for the sources, while there are high-quality journals devoted to topics similar to the inspected, we looked broader and addressed two major digital libraries/databases, more precisely Scopus and Web of Science.

An in-depth analysis of the relevant studies was then carried out. Although, in view of the nature of this study, it may be appropriate to add more keywords as exclusion criteria to limit the number of studies further dedicated to the topic by addressing the barriers and drivers of the adoption and integration of the IoT in e-government, and the benefits and challenges arising from this, we have decided not to do so. The reasons for this are twofold: firstly, this could affect the completeness of the results, if the authors dealing with the above-mentioned issues had used other terminology (e.g. benefits, advantages, pros, positive outcome, positive results, etc.) that would exclude the relevant studies from our resulting set. Secondly, to obtain as full overall picture as possible, we examined all the studies and derived the above-mentioned points from the results obtained by the authors, if the identification of the above-mentioned was not the primary aim of these studies. This should enrich our study and make our outputs more reliable and relevant to the real world as the search for studies on barriers (["iot" OR "internet of things"] AND ["e-government" OR "e-governance" OR "electronic government"] AND ["barrier" OR "obstacle" OR "impediment"]) resulted in 210 studies in Scopus and 59 in Web of Science, 44 and 12 of which, respectively, were available in an open access. Given relatively low number of studies available in an open access, we looked for pre-prints and/or archived versions of the results obtained from these two searches. Specifically, the coding rules included aspects such as discipline and sub-discipline (information management, public policy and government, humanities and social sciences, engineering), type of study (theoretical, quantitative, qualitative or mixed methods), year of publication (2010–2022), language (only English), methods used (if applicable), authors, title, journal, volume, issue number, pages and digital object identifier. Using snowballing approach, the resultant research articles are back-tracked and forward-tracked, and then the abstracts were filtered followed by a close double-review of the remaining 58 studies by three of the authors, and finally, these studies were compiled in the categories of "barriers" and "drivers" for the integration of IoT in e-government.

4. Potential drivers to effect integration of internet of things in e-government

One of the most popular fears of e-government as a new digitized form of government complemented with the emerging technologies is e-government, and each component

consists of (e.g. artificial intelligence) security and safety (Young *et al.*, 2019). According to Young *et al.* (2019), to meet this requirement, the implementation of a secure and safe e-government ecosystem uses many cutting-edge technologies underpinning theoretical breakthrough in the fields of AI, telecommunication, cryptography and authentication. Interestingly, that AI serves here as both the threat and the treatment as AI and ML are widely used in the emulating of abnormal network traffic, including such widely occurred threats as intrusion, Denial of Service (DoS), fishing email and consequent development of the respective detection systems, thereby improving the state of the security at various levels.

Another technology to mention is blockchains – a peer to peer distributed ledger, which is shared among participating parties on the network and is used to record transactions that are verified by a consensus mechanism that creates trust in the network (Peck *et al.*, 2017; Batubara *et al.*, 2018) and secured using public key cryptography applied to blocks of these records (Young *et al.*, 2019). As regards the security, to break the security of the blockchain, most peers/parties should be violated by the attacker simultaneously, which make it a difficult task seen as almost unrealistic at this point. The blockchain has the potential to improve the efficiency of government operation by improving public service delivery and increasing trust and confidence in the public sectors (Konashevych, 2017). Batubara *et al.* (2018) considered this, and trust and transparency in particularly, to be particularly beneficial for developing countries as they are found to be more vulnerable to corruption, fraud and lack of trust compared to the developed countries. However, it also means that even developed countries, which governments can be characterized with the above-mentioned (corruption, lack of trust, etc.), can be a source of resistance to the adoption of this technology and put it at risk, thus also putting e-government at risk.

The use of IoT in the government sector can ensure the smooth operation of routine activities. IoT opens up new possibilities for technology solutions that improve existing e-government services and digital infrastructures in general (Gil-Garcia *et al.*, 2020; Velsberg *et al.*, 2020).

It is evident that a significant amount of research has reported the potential of e-government in transforming relations among government institutions, businesses and citizens through the use of ICT. Many are limited in scope and are not comprehensive in identifying and analysing the role of emerging technologies. Although the benefits of e-government are overwhelming, understanding of the feasibility of emerging technologies such as IoT remains under-explored, to say the least. To reap the benefits of the IoT infrastructure, e-government 3.0 must possess three characteristics: instrumentation, interconnection and intelligence (Ølnes *et al.*, 2017). There are several factors that can drive IoT integration in the e-government.

4.1 Political and bureaucratic support

It is a key driver of IoT and e-government integration, without which relevant policies are unlikely to succeed. Scholars regard IoT as an archetype of e-government reform with the potential to significantly improve traditional e-government practices (Brous and Janssen, 2015). Many governments, for example, want to improve public services, ensure proper oversight, cut labor and fraud costs, automate security and improve process efficiency. All of these lofty goals necessitate the strategic application of new technologies such as IoT which has the potential to combine and analyse disparate data to assist governments in developing and improving services that isolated systems cannot provide. Legislative and regulatory frameworks are important considerations in IoT integration in e-government (Guler and Demir, 2020). Many existing legal and regulatory frameworks did not cover the aspects of IoT because IoT adoption in e-government initiatives is still in its infancy. As a result, new frameworks are attempting to incorporate IoT as a fundamental component that promotes the advancement of e-government (Gil-Garcia *et al.*, 2020). Enhanced connected

devices should be in place such that the smart phones' manufacturers ensure that strong authentication and encryption platforms are ensured. Likewise, biometric security and surveillance may be ensured. Regular and automatic software update is mandatory to tackle the risks of being attacked by threats such as worms, backdoors, rooters and Trojans. Before data transmission, mutual authentication is must such that the sensors can only accept connections and commands from authorized systems. Finally, a comprehensive e-government information security maturity model should be in place to ensure security in e-government systems.

4.2 e-Readiness

This is another driver of IoT integration in e-government. The advancement of existing e-services will be aided by basic technological infrastructure. Stable and fast broadband infrastructure, collaboration among actors, stable information systems and data security and privacy laws will not only drive the growth of IoT integration in e-Government but also increase citizens' adoption of IoT-mediated e-government services. To achieve success in integrating IoT in e-government, public agencies must recognize the significance of integration and transformation in all e-government building blocks – IT strategy, processes, technology and people (Botchway and Yeboah-Boateng, 2019).

4.3 Citizens' trust and the usability of e-services

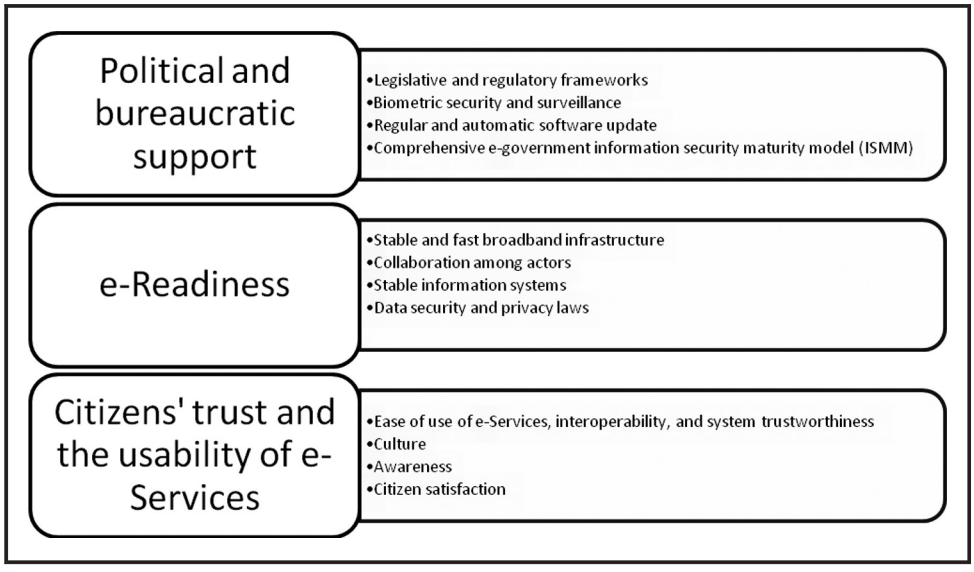
In fact, successful e-government initiatives must be citizen-centric; otherwise, they will fail. This is especially evident in IoT-integrated e-government initiatives, which appear to collect more data sets that could jeopardize privacy. Furthermore, unlike traditional e-government services, IoT-based e-government services may necessitate a slightly higher level of IT literacy for adoption; thus, aspects of ease of use are critical to promoting trust and acceptance (El-Haddadeh *et al.*, 2019). According to Rai *et al.* (2020), perceived ease of use of e-services, interoperability and system trustworthiness are significant predictors of acceptance and use of an e-government service. Similarly, Zhao and Khan (2013) argue that there is compelling evidence of a link between culture, awareness, trust and adoption of any e-government service. As a result, for planning or integrating IoT in public services, ensuring citizen satisfaction is crucial.

The aforementioned drivers towards integration of IoT in e-government have been enumerated in Figure 2. While the public sector across the world is undergoing a profound digital transformation, the central pillar of this transformation is the realization of a data-driven government. Datafication of public sector and governmental institutions requires control over their physical assets (Broomfield and Reutter, 2021). The hassle and inconveniences of the usual approaches motivate governments to think of ways such as IoT to optimize the control over data to improve services and make them more accessible to all citizens. As government agencies face challenges in maximizing the value of their data resources, IoT integration in e-government systems can assist them in gleaning useful insights from data sets usually presented in different formats that do not connect to each other (Brous and Janssen, 2015).

5. Potential barriers to effect an integration of internet of things in e-government

In the previous section, we have already mentioned the blockchain and its potential in the context of e-government. However, as with other technologies, resistance and low acceptance of the technology are sometimes noticed. Therefore, Batubara *et al.* (2018) have explored the adoption and use in the e-government. They found that the main challenges faced in adopting blockchain are mostly technological aspects such as security, scalability and flexibility. However, there are also organizational challenges, such as the issues of acceptability and the need for new governance models identified as key barriers

Figure 2 Potential drivers for integration of IoT in e-government



to adoption, and the lack of legislation and regulatory support identified as a major environmental barrier to adoption.

Despite several significant benefits of IoT and e-government integration, overall integration has received little attention from the governments due to several barriers. These barriers include security, device heterogeneity, interoperability, privacy, ethical issues, legal issues and IoT policy, as discussed in the following sub-sections.

Security threats linked with IoT may relate to physical security, computing security and data security (Ahmid and Kazar, In Press). This calls for authentication for securing information which may be made possible by using biometric authentication with iris recognition (Meena and Choudhary, 2019). Furthermore, conceding that diverse data (identification, positional, environmental, historical and descriptive) would be a part of the integrated IoT–e-government ecosystem, it is important that aspects such as querying, indexing, process modeling, transaction handling and integration of data across heterogenous systems be done in a deft manner (Cooper and James, 2009). Another barrier is linked with the need to clearly outline the legislative framework (Chatterjee and Kar, 2018) pertaining to IoT's application in e-government, in particular, apart from other areas.

5.1 Security

One of the major barriers towards integrating IoT in e-government is the security. The sheer magnitude of the IoT network creates an "attack surface" that traditional firewalls and solutions cannot handle comprehensively (Sniatala *et al.*, 2021). The capacity to safeguard each layer of the IoT ecosystem from intrusions and security vulnerabilities becomes challenging as the ecosystem expands into multiple levels. Furthermore, some of the devices connected to the IoT typically lack basic security measures, which makes them vulnerable to cyber-attacks (Tchagna *et al.*, 2022). This becomes challenging as e-government systems contain sensitive government data, documents and citizens' particulars which needs adequate security measures (Cho *et al.*, 2021).

Most governments (as a norm) use technologies that have already been matured, evaluated and standardized and as security in the IoT environment is not yet satisfactory, the security

issue remains one of the major barriers of IoT and e-government integration. Security threats linked with IoT encompasses physical security, software security and data security.

5.2 Device heterogeneity

The growing number of linked IoT devices necessitates many sophisticated solutions to support the heterogeneous connectivity of devices and the connection scale, where all devices must have standardized protocols and algorithms for seamless communication. The variety of IoT devices makes it challenging to connect and communicate between devices. This has resulted in disjointed, splintered smart systems, with each device vendor offering unique/proprietary protocols. The lack of standardized data exchange standards, which might refer to communication between devices and e-government systems, between e-government systems and citizens, adds to the difficulty of integrating IoT and e-government. Thus, governments, researchers and IoT stakeholders need to develop interoperability standards to manage the heterogeneity of IoT devices. Without standardization, the heterogeneity factor would remain a barrier not only to IoT and e-government integration but also to other domain.

5.3 Interoperability

Most traditional communication protocols lacked the foresight to include the IoT and as a result, their coverage is insufficient to support the interoperability of overgrowing IoT settings. Moreover, most of the IoT architecture, application cases, devices and other aspects of the industry are designed as vertical silos, with each one using its data format, storage design and proprietary protocols (Noura *et al.*, 2019). This makes it harder for interoperability among IoT devices. From the perspective of IoT devices, lack of interoperability means that e-government systems would be tied to a single hardware or IoT vendor and must continue with it, potentially limiting scalability and plethora of services to support. Lack of interoperability across IoT platforms forces e-government software developers to conform their applications to platform-specific application programming interfaces and information models, preventing cross-platform and cross-domain software development. Nevertheless, academics and innovators are currently researching effective approaches to solve the IoT interoperability barrier.

Standardization is one way the industry attempts to overcome IoT interoperability issues (Palau *et al*, 2021). Several initiatives to define standards for interoperability across IoT devices, systems, applications and data formats introduced by various vendors are emerging. Researchers, industry giants and standardization bodies are currently promoting IoT interoperability standardization. The European Union, for instance, has also lately financed research projects focusing on the unification of IoT platforms through the H2020 initiative (Noura *et al.*, 2019).

5.4 Privacy

IoT sensors capture a wide range of data from various sources, such as citizens, physical surroundings, buildings and machinery. However, IoT devices can expose people to various new privacy issues (Alfandi *et al.*, 2021). Sensor data generated from IoT devices can indirectly expose a plethora of sensitive private information. Traffic light cameras, for instance, capture photos of automobiles running red lights, which can be swiftly analysed by algorithms trained to watch changes in street lighting and car positioning (Hewei *et al.*, 2022).

According to researchers (Baldini *et al.*, 2018), the issue of privacy under IoT needs special attention since the volume of data from IoT devices is increasing, and soon, it will be too complex to control. Moreover, the complication will increase when determining which data

is private and which is not. This has recently captured the researchers' and government's attention to address citizens' privacy rights under IoT and e-government integration. For instance, consider an IoT reception system installed in a government agency building to automatically authenticate visitors' identities and issue an access card (with some personal collecting information). This has led to the privacy dilemma on the management and authority of the collected data. For instance, what percentage of this data should be collected and maintained and for how long should it be retained? What data classification scheme should the IoT-based e-government system use for each data category? Is it possible to sell or publish part (or all) of the data? Without carefully considering privacy, the government risks being accused of invading the privacy of the general population, leading to mistrust and citizens' disapproval of IoT-based e-government systems.

5.5 Legal issues

Another barrier is the lack of a legislative framework that governs IoT's integration in e-government (Chatterjee and Kar, 2018). With the potential for IoT devices to enhance e-government systems and services, the legal implication when IoT devices fail or lead to data breach is still a dilemma. Numerous problems can occur with network-enabled devices, such data interception (man-in-the-middle attacks) and distributed denial of service (DDoS) attacks when the IoT-based e-government system is hacked and used as part of a network. Due to the interconnected nature of IoT devices, identifying liability is more challenging than ever. This can make legal battles exceedingly difficult and costly.

5.6 Internet of things policy

Lack of IoT policies is another barrier to integrating IoT and e-government in most countries. IoT policies and regulations are being established at a far slower pace than IoT, e-government services and the two's integration. With a lack of clear IoT policy, e-government practitioners, users and providers of IoT services are experiencing confusion and dilemma on the how to operate seamlessly in the integration context. This is a barrier, as without the IoT policy, there remain many predicaments surrounding IoT's working environment in e-government. As an emerging technology, the IoT requires a suitable policy framework that supports future innovation and ethically protects against abuse without limiting its ability to bring societal and economic advantages. Moreover, the IoT policies should go hand in hand with establishing countries' strategic roadmap to lead the IoT implementation and adoption. Government agencies active in particular industries can produce specialized action plans for specific domains, such as e-government, in addition to a holistic roadmap.

5.7 Ethical issues

Ethical concerns about integrating IoT technology with e-government are also a barrier that needs to be addressed (Mittelstadt, 2017). Due to the massive volume of data collected and processed in IoT and the sensitivity of the e-government data, the ethical issues become more complicated than those of simple internet. Lack of transparency of IoT firms regarding how data are obtained from vast numbers of IoT devices and e-government users and how the data are handled and used is a key current ethical issue. Governments are responsible for regulating this issue and should establish appropriate ethical guidelines. Currently, several ethical concerns are debatable by researchers. For instance, what happens if an IoT device operates in unanticipated ways on e-government data? What would happen to e-government data if an IoT product/service provider goes out of business and the integration is no longer supported? Is the integration of IoT and e-government likely to widen the digital gap for citizens who lack smart devices or the skills to use them? These, along with other ethical concerns, need to be addressed and resolved for the effective integration of IoT and e-government.

Figure 3 summarizes the potential barriers to integrating IoT in e-government.

6. Potential benefits of integrating internet of things in e-government

While it is crystal clear that IoT will have a major impact to bolster e-government services. However, IoT adoption in the public sector is still at the earlier stages (Brous and Janssen, 2015). Precisely, IoT can bolster efficiency in various facets of e-government including health care, transport, environment, emergency services and security and surveillance.

6.1 Public health-care services

IoT promises affordable and accessible health-care services. Precisely, IoT can benefit the delivery of health-care services by enabling remote monitoring, timely care, sensor-based equipment, ingestible sensors, smart beds in the hospital and real-time tracking. Citizens can benefit from increased access to services, and there are opportunities for rural and remote areas to receive public services (Javaid and Khan, 2021).

6.2 Public transport services

IoT can also help the government improve their services through the collection and use of real-time data using sensors. These data sets are useful to manage public transportation from monitor traffic conditions to route planning and improving service experience (Bharambe and Shaikh, 2017; Gil-Garcia *et al.*, 2020).

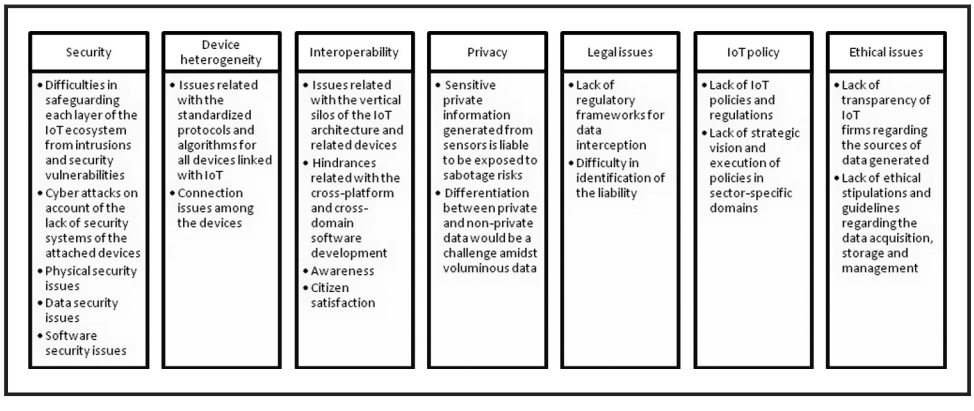
6.3 Environmental monitoring

Environmental sustainability is one of the major responsibilities of governments. IoT can help governments to monitor and control pollution levels in the air and signpost the necessary action at the right time.

6.4 Security services

Security is a primary concern of the governments. IoT can bolster government security and surveillance services by supporting real-time coordination and instant detection of unusual scene. Through real-time monitoring, governments can use IoT to monitor and optimize the performance of physical assets (Bello and Zeadally, 2019). Additionally, it can be used to identify vulnerabilities and mitigate cybersecurity risks. IoT can be used to collect data on the use and maintenance of public infrastructure. Moreover, IoT-based systems in

Figure 3 Potential barriers of integrating IoT in e-government



governance can be used to monitor state, land, air, sea borders and other sensitive locations from a public safety standpoint. Furthermore, IoT capabilities can safeguard critical infrastructures, such as electricity and water generation plants (Panchatcharam and Vivekanandan, 1AD).

6.5 Emergency response services

IoT can help the government to deal with natural disaster and emergency management (Dugdale *et al.*, 2021). Real-time capture of data sets about pressure, fog, smoke, temperature and fire, government can analyse and draw insights to deal with current and future emergencies.

In general, using IoT can support governments getting control of physical assets. Given the fact that almost all governments worldwide have a visible presence on the internet, they can expand their reach with the use of IoT. Governments can provide better services to their citizens by leveraging the IoT to extend the soft infrastructure have control of over distributed infrastructure (Wirtz *et al.*, 2019). IoT can help the government achieve its goals, such as increased economic growth and improvements in environmental sustainability, public safety and security, service delivery and productivity, in the same way that the internet has helped economies develop and flourish.

7. Potential risks of integrating internet of things in e-government

Integrating IoT into e-government is not without risks. The IoT systems pose unique risks when integrated with e-government, given the complex nature and heterogeneity of the devices. In the following sub-sections, we discussed several potential risks.

7.1 Physical attack

Integrating IoT into e-government has potential risks to physical attacks that need to be considered. Physical attacks may be possible depending on where the government agencies set the IoT devices. As physical parts of the devices can give the point of entry onto a network, IT administrators should consider the risks of IoT physical security. Cybercriminals can physically dismantle an IoT device to obtain access to the device's internal parts, terminals, pins and circuitry, then hook up to the entire network, potentially exposing critical government data and citizen records. Physical vulnerability can be classified into two categories: invasive and non-invasive attacks.

1. Invasive attacks require the chip's surface to be exposed, allowing it to be physically modified. For instance, an attacker can physically tamper with the integrated circuit (IC) to collect sensitive information from the metal wires using tiny probes. An attacker may even attempt to change the circuit's functionality by overdriving the IC's state (Balogh *et al.*, 2021).
2. Non-invasive attacks necessitate the attacker being proximate enough to target the chip and electrical properties in IoT device, allowing the attackers to alter device behaviour or obtain sensitive data. For instance, an attacker can analyse the power signature or electromagnetic radiation emitted by an IC to obtain sensitive data (Batina *et al.*, 2021).

7.2 Software vulnerabilities

Millions of IoT devices feature security flaws in their software that might allow cybercriminals to compromise e-government systems. Network services that run on insecure IoT devices, especially those accessible to the internet, can compromise the availability of confidentiality, integrity and authenticity of government data. The flaws might aid cybercriminals in gaining access to government systems and stealing sensitive data, tampering with – or deactivating – operational technologies.

7.3 Data breach

As IoT devices are connected with e-government, failure to maintain the proper security of IoT devices poses a severe risk of data breaches. Many IoT components contain sensors connected to communicators, which is the root of the data breach problem. A webcam, speaker or other sensing devices, for instance, can gather up government data from the environment and communicate it to a remote location, such as the internet or a proprietary server (Lipford *et al.*, 2022). There have previously been several examples in which smart electronics (such as televisions) have transferred data collected from people's homes and offices back to the company's servers without the users' consent. Moreover, not only may IoT operators use IoT devices to spy on government agencies and their operations, but inadequate device security can also lead to IoT-connected devices being used as a source of distributed denial of service (DDoS) attacks and, ultimately, government data breaches.

8. Conclusion

IoT is a network connection of people, processes, data and things. Its integration into e-government would result in efficacious public service delivery. The paper sought to underline the drivers, barriers, benefits and risks resulting from such integration. A systematic literature review was conducted to arrive at the finalized research articles. Having appreciated the drivers and barriers for bringing about the integration of IoT in e-government, the study looks into the potential caveats as well. It may be deduced that the integration of IoT in e-government would result in realizing the over-arching vision of the Society 5.0 and Industry 5.0. The government's increasing use of and investment in digital technologies necessitates extensive research in this area, on the one hand, to improve e-government efficiency, effectiveness and innovation. Because IoT application in e-government is still in its early stages, this study contributes to both practical and theoretical understanding of how it can be leveraged in the e-government context. It is without a doubt that IoT has a significant impact on e-government services in the future, bringing a range of benefits to e-government at all levels, but more understanding is needed to explore the seamless integration between the two in multiple perspectives by mitigating the potential challenges. By integrating two concepts, the present study advances the IT governance research domain (Peterson *et al.*, 2000) as well as providing a sounding board for the practitioners for effecting the integration of IoT in e-government.

While most of the current studies have focused on the design of IoT frameworks, applications, architectures and their potential impact, there is little evaluation of these concepts in the context of e-government. As a result, future research should move beyond the conceptual level and focus on practical models for evaluating and putting such ideas into real e-government systems. Moreover, some uncertainties need to be addressed in future research:

- *Q1.* How should access control and authentication be handled in IoT-based e-government systems?
- *Q2.* How can new cryptographic algorithms be used efficiently in IoT-based e-government environments?
- *Q3.* How to effectively address the ethical and legal dilemmas resulting from the integration of IoT and e-government?

Future studies should also explore the citizen adoption of IoT-based e-government systems in different social-economic and cultural settings. Another aspect is the advancement of IoT security for e-government from the design point of view. As e-government deals with sensitive data, researchers should advance the security standards. Thus, security must be from the design and functionality of IoT devices, and standards should be developed with input from the government and industry based on empirical research and thorough cost-benefit

analysis. Lastly, it would be valuable to make a call for unified theory of acceptance and use of technology, technology acceptance model, technology organization environment, item response theory studies on their perceived benefits, behavioural intention, etc., to appreciate how the integration of IoT in e-government is being embraced by the concerned stakeholders.

9. Practitioner implications

New technologies are assisting governments in improving e-service delivery and adapting to changing needs, but their full potential has yet to be realized in many parts of the world. Increased adoption of frontier technologies like the IoT has seemingly limitless potential; such technologies can be used to address needs in a variety of areas, including agriculture, health care, education and social protection. Governments, in fact, are an excellent testbed for real-world, practical and effective IoT applications. They have a vested interest in boosting efficiency by leveraging massive amounts of data collected from connected devices, as well as the infrastructure and budget to support it. Governments, on the other hand, have been slower to respond to the IoT than the private sector.

In the public sector, bringing about change or introducing new technology is a difficult task. IoT has been slow to gain traction in the public sector. The importance of IoT in government cannot be overstated. The IoT generates an infinite amount of data, but governments can only benefit if they have the right solution in place to manage and leverage it. Using the right platform will ensure that the information gathered is put to good use. To regain control over data, governments must implement a highly secure and adaptable platform. Centralized master data management, for example, uses an agile approach to govern data flow and standardizes IoT adoption. The present study showed that while there are several drivers, barriers and risks towards integration of IoT in e-government, there is no gainsaying the fact that each of these components might have differential significance for the practitioners in line with the organizational strategic vision, resource availability and external environmental factors, namely, technological infrastructure, macroeconomic indices and digital divide, thereby making a step forward towards organizational learning (Schilling and Kluge, 2009).

References

Alfandi, O., Khanji, S., Ahmad, L. and Khattak, A. (2020), "A survey on boosting IoT security and privacy through blockchain", *Cluster Computing*, Vol. 24, pp. 37-55, doi: 10.1007/s10586-020-03137-8.

Baldini, G., Botterman, M., Neisse, R. and Tallacchini, M. (2018), "Ethical design in the internet of things", *Science and Engineering Ethics*, Vol. 24 No. 3, pp. 905-925.

Balogh, S., Gallo, O., Ploszek, R., Špaček, P. and Zajac, P. (2021), "IoT security challenges: cloud and blockchain, postquantum cryptography, and evolutionary techniques", *Electronics*, Vol. 10 No. 21, p. 2647.

Bansal, M., Sirpal, V. and Choudhary, M.K. (2022), "Advancing e-government using internet of things", In *Mobile Computing and Sustainable Informatics*, Springer, Singapore, pp. 123-137.

Batina, L., Djukanovic, M., Heuser, A. and Picek, S. (2021), "It started with templates: the future of profiling in side-channel analysis", in Avoine, G. and Hernandez-Castro, J. (Eds), *Security of Ubiquitous Computing Systems*, Springer, Cham.

Batubara, F.R., Ubacht, J. and Janssen, M. (2018), "Challenges of blockchain technology adoption for e-government: a systematic literature review", *19th Annual International Conference on Digital Government Research: Governance in the Data Age*, pp. 1-9, doi: 10.1145/3209281.3209317.

Bello, O. and Zeadally, S. (2019), "Toward efficient smartification of the internet of things (IoT) services", *Future Generation Computer Systems*, Vol. 92, pp. 663-673.

Bharambe, M.S.M. and Shaikh, M.Z. (2017), "Integration of IoT in public transport", *International Research Journal of Engineering and Technology (IRJET)*, Vol. 4 No. 6, pp. 1468-1472, available at: https://irjet.net/archives/V4/i6/IRJET-V4I6273.pdf

Botchway, E.A. and Yeboah-Boateng, E.O. (2019), "IoT readiness of project management teams within local government organizations in Ghana", *International Journal of Civil Engineering and Technology*, Vol. 10 No. 7, pp. 308-332.

Broomfield, H. and Reutter, L. (2021), "Towards a data-driven public administration: an empirical analysis of nascent phased implementation", *Scandinavian Journal of Public Administration*, Vol. 25 No. 2, pp. 73-97.

Brous, P. and Janssen, M. (2015), "Advancing e-government using the internet of things: a systematic review of benefits", *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, pp. 156-169.

Chatterjee, S. and Kar, A.K. (2018), "Regulation and governance of the internet of things in India", *Digital Policy, Regulation and Governance*, Vol. 20 No. 5, pp. 399-412.

Cho, S., Oh, S., Rou, H. and Gim, G. (2021), "Study on security and privacy of e-government service", in Kim, J. and Lee, R. (Eds), *Data Science and Digital Transformation in the Fourth Industrial Revolution, Studies in Computational Intelligence*, Springer, Cham, Vol 929.

Cooper, J. and James, A. (2009), "Challenges for database management in the internet of things", *IETE Technical Review*, Vol. 26 No. 5, pp. 320-329, doi: 10.4103/0256-4602.55275.

De Franca, B.R., Kovaleski, J.L., da Silva, V.L., Pagani, R.N. and de Genaro Chiroli, D.M. (2021), "Internet of things in disaster management: technologies and uses", *Environmental Hazards*, Vol. 20 No. 5, pp. 493-513.

Dugdale, J., Moghaddam, M.T. and Muccini, H. (2021), "IoT4Emergency: internet of things for emergency management: challenges and envisioned solutions", *ACM SIGSOFT Software Engineering Notes*, Vol. 46 No. 1, pp. 33-36.

El-Haddadeh, R., Weerakkody, V., Osmani, M., Thakker, D. and Kapoor, K.K. (2019), "Examining citizens' perceived value of internet of things technologies in facilitating public sector services engagement", *Government Information Quarterly*, Vol. 36 No. 2, pp. 310-320.

Engin, Z. and Treleaven, P. (2019), "Algorithmic government: automating public services and supporting civil servants in using data science technologies", *The Computer Journal*, Vol. 62 No. 3, pp. 448-460.

Gigerenzer, G. (2017), "A theory integration program", *Decision*, Vol. 4 No. 3, pp. 133-145.

Gil-Garcia, J.R., Pardo, T.A. and Gasco-Hernandez, M. (2020), "Internet of things and the public sector", *Public Administration and Information Technology*, Vol. 30, pp. 3-24.

Grant, C. and Osanloo, A. (2014), "Understanding, selecting, and integrating a theoretical framework in dissertation research: creating the blueprint for your 'house'", *Administrative Issues Journal: Connecting Education, Practice, and Research*, Vol. 4 No. 2, pp. 12-26.

Guler, A. and Demir, F. (2020), "Identifying security challenges in the IoT for the public sector: a systematic review", *Public Administration and Information Technology*, Vol. 30, pp. 69-84.

Hewei, G., Sadiq, A.S. and Tahir, M.A. (2022), "Fuzzy-Logic approach for traffic light control based on IoT technology", in Balas, V.E., Semwal, V.B. and Khandare, A. (Eds), *Intelligent Computing and Networking. Lecture Notes in Networks and Systems*, Springer, Singapore, Vol 301.

Hoy, M.B. (2015), "The 'Internet of Things': what it is and what it means for libraries", *Medical Reference Services Quarterly*, Vol. 34 No. 3, pp. 353-358.

Javaid, M. and Khan, I.H. (2021), "Internet of Things (IoT) enabled healthcare helps to take the challenges of COVID-19 pandemic", *Journal of Oral Biology and Craniofacial Research*, Vol. 11 No. 2, pp. 209-214.

Kankanhalli, A., Charalabidis, Y. and Mellouli, S. (2019), "IoT and AI for smart government: a research agenda", *Government Information Quarterly*, Vol. 36 No. 2, pp. 304-309.

Kim, S.-T. (2013), "Next generation e-government strategies and asks for the smart society – based on Korea's case", *Journal of E-Governance*, Vol. 36 No. 1, pp. 12-24.

Konashevych, O. (2017), "The concept of the blockchain-based governing: current issues and general vision", *Proceedings of the European Conference on eGovernment, ECEG*, pp. 79-85.

Lipford, H.R., Tabassum, M., Bahirat, P., Yao, Y. and Knijnenburg, B.P. (2022), "Privacy and the internet of things", in Knijnenburg, B.P., Page, X., Wisniewski, P., Lipford, H.R., Proferes, N. and Romano, J. (Eds), *Modern Socio-Technical Perspectives on Privacy*, Springer, Cham.

Lysaght, Z. (2011), "Epistemological and paradigmatic ecumenism in 'Pasteur's Quadrant Tales:' tales from doctoral research", *Official Conference Proceedings of the Third Asian Conference on Education in Osaka, Japan*, available at: https://papers.iafor.org/proceedings/conference-proceedings-ace2011/

Meena, G. and Choudhary, S. (2019), "Biometric authentication in internet of things: a conceptual view", *Journal of Statistics and Management Systems*, Vol. 22 No. 4, pp. 643-652, doi: 10.1080/09720510.2019.1609722.

Miorandi, D., Sicari, S., De Pellegrini, F. and Chlamtac, I. (2012), "Internet of things: vision, applications and research challenges", *Ad Hoc Networks*, Vol. 10 No. 7, pp. 1497-1516.

Mittelstadt, B. (2017), "Ethics of the health-related internet of things: a narrative review", *Ethics and Information Technology*, Vol. 19 No. 3, pp. 157-175.

Noura, M., Atiquzzaman, M. and Gaedke, M. (2019), "Interoperability in Internet of Things: taxonomies and open challenges", *Mobile Networks and Applications*, Vol. 24 No. 3, pp. 796-809.

Oke, A.E., Arowoiya, V.A. and Akomolafe, O.T. (2023), "Influence of the Internet of Things application on construction project performance", *International Journal of Construction Management*, Vol. 22 No. 13, pp. 2517-2527, doi: 10.1080/15623599.2020.1807731.

Ølnes, S., Ubacht, J. and Janssen, M. (2017), "Blockchain in government: benefits and implications of distributed ledger technology for information sharing", *Government Information Quarterly*, Vol. 34 No. 3, pp. 355-364.

Palau, C.E. *et al.* (2021), "Introduction to interoperability for heterogeneous IoT platforms", *Interoperability of Heterogeneous IoT Platforms: Internet of Things*, Springer, Cham, doi: 10.1007/978-3-030-82446-4_1.

Pawar, A., Kolte, A. and Sangvikar, B. (2021), "Techno-managerial implications towards communication in internet of things for smart cities", *International Journal of Pervasive Computing and Communications*, Vol. 17 No. 2, pp. 237-256.

Peck, D., Bakker, C., Kandachar, P. and de Rijk, T. (2017), "Product policy and material scarcity challenges: the essential role of government in the past and lessons for today", in Bakker, C. and Mugge, R. (Eds), *Plate Product Lifetimes And The Environment, Amsterdam*, IoS Press, pp. 347-352, doi: 10.3233/978-1-61499-820-4-347.

Peterson, R., Ribbers, P. and O'Callaghan, R. (2000), "Information technology governance by design: investigating hybrid configurations and integration mechanisms", *ICIS 2000 Proceedings*, Vol. 41, available at: https://aisel.aisnet.org/icis2000/41

Pinochet, L.H.C., Lopes, E.L., Srulzon, C.H.F. and Onusic, L.M. (2018), "The influence of the attributes of 'Internet of Things' products on functional and emotional experiences of purchase intention", *Innovation & Management Review*, Vol. 15 No. 3, pp. 303-320.

Rai, S.K., Ramamritham, K. and Jana, A. (2020), "Identifying factors affecting the acceptance of government to government system in developing nations – empirical evidence from Nepal", *Transforming Government: People, Process and Policy*, Vol. 14 No. 2, pp. 283-303.

Ronzhyn, A., Wimmer, M.A., Spitzer, V., Viale Pereira, G. and Alexopoulos, C. (2019), "Using disruptive technologies in government: identification of research and training needs", *Electronic Government, Lecture Notes in Computer Science*, Springer, Cham, doi: 10.1007/978-3-030-27325-5_21.

Saxena, S. (2017), "Factors influencing perceptions on corruption in public service delivery via e-government platform", *Foresight*, Vol. 19 No. 6, pp. 628-646.

Schilling, J. and Kluge, A. (2009), "Barriers to organizational learning: an integration of theory and research", *International Journal of Management Reviews*, Vol. 11 No. 3, pp. 337-360.

Silcock, R. (2001), "What is e-government", *Parliamentary Affairs*, Vol. 54 No. 1, pp. 88-101.

Sniatala, P., Iyengar, S. and Ramani, S.K. (2021), "IoT security", *Evolution of Smart Sensing Ecosystems with Tamper Evident Security*, Springer, Cham, doi: 10.1007/978-3-030-77764-7_3.

Tchagna Kouanou, A., Tchito Tchapga, C., Sone Ekonde, M., Monthe, V., Mezatio, B.A., Manga, J., Simo, G.R. and Muhozam, Y. (2022), "Securing data in an internet of things network using blockchain technology: smart home case", *SN Computer Science*, Vol. 3, pp. 1-10, doi: 10.1007/s42979-022-01065-5.

Velsberg, O., Westergren, U.H. and Jonsson, K. (2020), "Exploring smartness in public sector innovation-creating smart public services with the Internet of Things", *European Journal of Information Systems*, Vol. 29 No. 4, pp. 350-368, doi: 10.1080/0960085X.2020.1761272.

Wahyudi, A., Matheus, R. and Janssen, M. (2017), "Benefits and challenges of a reference architecture for processing statistical data", *Digital Nations – Smart Cities, Innovation, and Sustainability, I3E 2017, Lecture Notes in Computer Science*, Springer, Cham, doi: 10.1007/978-3-319-68557-1_41.

Wirtz, B.W., Weyerer, J.C. and Schichtel, F.T. (2019), "An integrative public IoT framework for smart government", *Government Information Quarterly*, Vol. 36 No. 2, pp. 333-345.

Young, M.M., Bullock, J.B. and Lecy, J.D. (2019), "Artificial discretion as a tool of governance: a framework for understanding the impact of artificial intelligence on public administration", *Perspectives on Public Management and Governance*, Vol. 2 No. 4, pp. 301-313, doi: 10.1093/ppmgov/gvz014.

Zhao, F. and Khan, M.S. (2013), "An empirical study of e-government service adoption: culture and behavioral intention", *International Journal of Public Administration*, Vol. 36 No. 10, pp. 710-722.

Further reading

Ahmed, M. and Kazar, O. (2023), "A comprehensive review of the internet of things security", *Journal of Applied Security Research*, doi: 10.1080/19361610.2021.1962677.

Dutton, W. (2014), "Putting things to work: social and policy challenges for the internet of things", *Info*, Vol. 16 No. 3, pp. 1-21.

Ulrika, H. and Jonsson, K. (2020), "Exploring smartness in public sector innovation – creating smart public services with the internet of things", *European Journal of Information Systems*, Vol. 29 No. 4, pp. 350-368.

Author affiliations

Deo Shao is based at the Department of Computer Science, University of Dodoma College of Informatics and Virtual Education, Dodoma, Tanzania and Department of Virtual Educational Technologies and Applications, University of Dodoma College of Informatics and Virtual Education, Dodoma, Tanzania.

Fredrick R. Ishengoma is based at the University of Dodoma College of Informatics and Virtual Education, Dodoma, Tanzania.

Charalampos Alexopoulos is based at the Department of Information and Communication Systems Engineering, University of the Aegean, Mytilene, Greece.

Stuti Saxena is based at the Department of Humanities and Social Sciences, Graphic Era Deemed to be University, Dehradun, India.

Anastasija Nikiforova is based at the Faculty of Science and Technology, Institute of Computer Science, University of Tartu, Tartu, Estonia.

Ricardo Matheus is based at the Faculty of Technology, Policy and Management, TU Delft, Delft, The Netherlands.

Corresponding author

Stuti Saxena can be contacted at: stutisaxenaogd.vishnu@gmail.com