E-GOVERNMENT: PRIVACY AND SECURITY CHALLENGES IN THE CONTEXT OF INTERNET OF THINGS

Raja Majid Ali Ujjan
School of Computing, Engineering & Physical Sciences University of the West of Scotland
raja_majidali@hotmail.com
Navid Ali Khan
School of Computer Science and Engineering, Taylors University, Subang Jaya Malaysia
navidali.khan@taylors.edu.my
Loveleen Gaur
Amity University, Noida India
Gaurloveleen@yahoo.com

Abstract

The Internet of Things (IoT) is becoming more significant in everyday life as a mechanism for making major decisions in different fields. As smart devices and data in real-time are connected and updated. IoT is being used in a variety of ways to provide digital services to the public. Online payment, property purchase, and sailing are just a few examples. On the other hand, users' complaints about the safety and privacy of their personal information are growing. The Internet of Things (IoT) is becoming more popular and significantly enhances e-government. This chapter primarily focuses on how potential users can obtain information to use the Internet of Things and its related services within the e-government sectors. There are several technological, administrative, and political challenges to IoT adoption problems in e-government and legal problems that must be solved to develop effective and required applications. It's crucial to explore these problems and potential solutions.

Keywords: IoT, E-government, Domains Applications and privacy and Security Challenges

1. Introduction

IoT works by utilizing gadgets to communicate data and take activity based on information. There can also be moments where a group of devices is cooperating for a shared goal and communicating through the internet. There are a variety of types of situations in which IoT can provide strategic, and operational benefits to management by designing apps to exploit the data collected by these devices. That is predicted by the literature review to increase in the coming years (McKinsey, 2018). Several Internet of Things devices is estimated to reach 65 billion by 2026 (Business Insider, 2019). With the introduction of the IoT, machines and things have become smart and dynamic agents in digital contexts, allowing for digital ideas, while the Internet of Things (IoT) is rapidly changing the nature of work, with a growing level of acceptance in a variety of personal and corporate settings. The better government market is anticipated to be worth USD 53.20 billion by 2027. , according to industry estimates (Reports and Data, 2019). The smart government market is expecting IoT-enabled secret intelligence tools and apps to provide new services. Smart government can be defined as the technological intersection between e-government and smart cities [1]. Hackers and cybercriminals are concentrating their attention on Internet of Things processor architectures and networks that hold [2] ,[3] that is capable of making such intelligent selections while simultaneously saving a duplicate of the information, to ensure data is transmitted and processed swiftly to provide a vital choice that cannot wait till the data is transferred to the clouds. IoT mechanisms and apps allow the delivery of sophisticated solutions to individuals and societies as a whole, enhancing their protection against a range of challenges and in a variety of settings. The government provides these technical services to the public. Furthermore, theis electronic government-to-citizen and government-to-society services remove the risk of putting persons in danger who are responsible for dealing with such occurrences in danger, thanks to the deployment of IoT. They believe that IoT will add the most value to e-government in these key public functions [4]. Protection and shelter are vital to society, and they can take on even greater significance when they are linked to public health. IoT can enable the effective handling of public-sector security and safety concerns [5]. Critical locations can substantially benefit from being monitored using IoT technology to permit appropriate and prompt action in aerial, maritime, and terrestrial contexts figure 1.

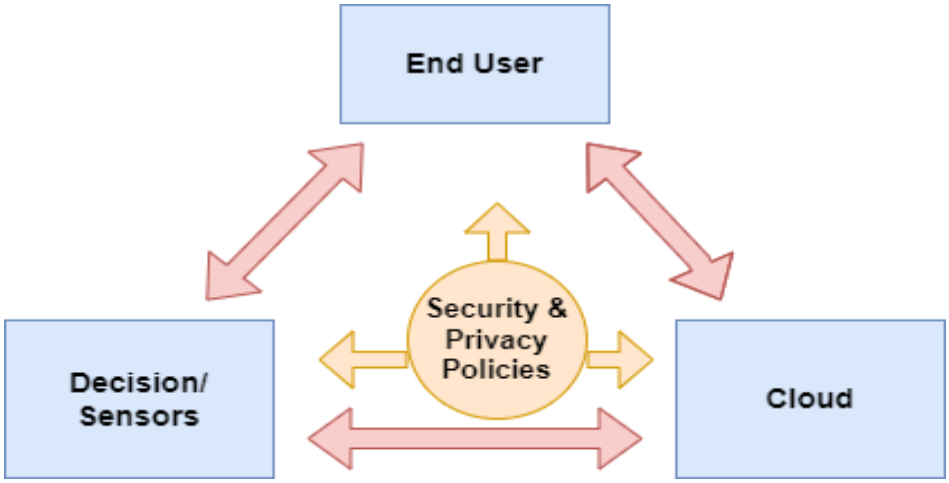

Figure 1 Overview IoT model with privacy and security policies

The chapter question organize as follows points:

1. In IoT E-government Applications, we identify both technological and non-technological challenges?
2. We will present our findings and recommendations?
3. We will highlight the influence of the Internet of Things on E-government?

2. Literature Review

Internet of Things and e-government as a combined issue in several of research publications by AlEnezi et al. (2018) an attention towards IoT facilities. The author demonstrates the assistances of the IoT for economic growth and long-term development [6]. With the advent of the Internet, e-government emerged, and e-government provided the ideal environment and technical assistance for the government to establish a provisional government. [7] Propose connecting electronic government issues and service administration, and further propose that the connection of e-government and provider government is to force the government to adopt new changes and build high-quality, low-cost new service patterns, rather than to be based on current E-government. [8] The architecture and networking platform framework of the E-Government service explained the architecture and networking platform framework of the e-government service, which provided the government with the necessary institutional and technological assistance to build an e-government system [9]. Create the e-government application systems of various municipal management agencies and establish the "digital city" applications of diverse works [10]. A novel way of integrating AJAX and the J2EE framework, which was successfully demonstrated in a real-world E-Government app. presented a network-based E-Government that meets certain standards and creates a typical hierarchical grid system conceptual structure. [11]. In the data age, the e-government authorization form paradigm based on cloud computing was developed. This framework includes the E-Government service mode, meets e-government security standards, adjusts to the background of a large data context, and supports cloud technology operational mechanisms [12]. The separation of the two network systems, the Intranet of Government Affairs and the Extranet of Government Affairs, the government internet, is a specially trained office preform. Because the Internet and other government affairs are physically separated, some flow of information and capacity transfer is possible behind a firewall [13]. Urban environments are becoming increasingly rich in such instrumentation, which is being extensively investigated via the Internet of Things. These big data sets can be exploited and integrated into interconnected systems that bring together unstructured. They use the information to evaluate interconnected data, find trends, correlations, and results, as well as forecasting to find effective and quick solutions to improve production value, system organization, or process outcomes [14]. The society area focuses on the topic from a global or intra-group perspective. Intergovernmental concerns are those that involve various public-sector organizations in e-government operations [15]. In an African context, similar challenges to incorporating ICT into local government were also identified. Low skill base to utilize current equipment, inability to repair, insufficient operating finance, uncoordinated ICT activities, and power fluctuations are among the most common hurdles to successful ICT integration in Uganda's ministry of local government, according to the findings. There have been certain e-Government programs that have fallen short of expectations, trying to make earlier claims of its transformative potential seem too hopeful. It's worth noting that the study has revealed considerable variation in its own approach to e-Government [16]. Competition in the industry has risen due to the fast development of information technology. As a result, customer behaviour has shifted, requiring firms to be more efficient and supply services at a lower cost. This helps to explain why there is such a constant need to accept new technology [17]. However, public sector organizations are slow to implement the same technologies. Meanwhile, research reveals that public organizations are still hesitant to use them, citing technical concerns like security and the fear of losing data control [18]. Furthermore, educational institutions confront other common acceptance problems, such as the uncertainty of the value derived from cloud computing use [19].

It also discusses some of the drawbacks of cloud computing, such as access control and resource ownership difficulties. While the benefits of cloud computing have accelerated its popularity among consumers, the obstacles connected with its use have drawn academics to improve its workability [20]. The study indicates that if the quality of e-government services can be assured, global economies can profit considerably from financial development [21]. Considering the significant early difficulties with e-government adoption, research has shown that this technology is useful, especially when geared towards economic growth. In light of the above framework, it is now time to identify the many e-government theories that are available [22]. Concepts regarding e-government are essential because they have a big impact on how government websites are designed, implemented, benchmarked, and evaluated. It's probably accurate to say that no single theory dominates the current research and practice paradigm. As a result, study and practice in this field follow the lines of stakeholder theory, social exchange theory, and other theories. The fact that these theories have lasted this long and that they can be applied to e-government is ample evidence of their explanatory power [23]. However, it is reasonable to conclude that governments around the world have adopted new technology at a considerably slower pace than business and industry, which is understandable. One reason for this cautious attitude is that, unlike industry, the government must be more cautious and risk-averse because the general public's interests are at stake [24]. E-government programs with a high failure rate incur significant direct and indirect financial expenses. Furthermore, it degrades employee morale, credibility, and confidence, limiting the delivery of e-government advantages. The absence of citizen access to these available online government services is one of the key reasons for failure [25]. E-government refers to when the government uses the Internet and other communications technology capabilities to do activities in a more efficient, productive, and intelligent manner, resulting in high-quality services that meet the needs of the public [26],[27]. When the phrase e-government was originally coined at the end of the 20th century, machines were being sold and popularized, and network infrastructures were being created. The United States was at the forefront of computer design and Internet expansion. Attempts were made by the government to apply digital resources to daily responsibilities to improve efficiency [28]. Intelligent E-Government refers to next-generation E-government that employs cutting-edge intelligence information technology such as the Internet of Things, cloud, artificial intelligence, and big data. It refers to a government that blends intelligent information technology with human creativity to develop government management and create services that people value. It can also support intelligent government actions that communicate with the general population [29]. It can also be characterized as a government that locates and provides personalized services to individual citizens, as well as a government that transparently and securely opens and shares all government-run information. Because it incorporates innovative new technology, intelligent e-government is numerically and qualitatively superior to existing e-government. It needs of an alternate solution to address existing e-government security challenges, such as the leakage of personal information, the propagation of misleading information, and the capture of national classified information. Intelligent e-government is presented as an option in this thesis. Intelligent information technologies, such as blockchains, secure clouds, and constantly changing cybersecurity programs, will be useful instruments for coping with these security concerns [30], [31]. Intelligent e-government keeps constant, continuous connection with the public, with the goal of not only resolving issues expressed by the public but also identifying issues ahead of time and suggesting solutions. Furthermore, citizens, not the government, are in charge of all policies and decisions when it comes to connecting with citizens via various channels such as the internet,

mobile phones, and offline. This is not the same as providing set services; instead, it is the same as providing personalized services to specific citizen's figure 2.

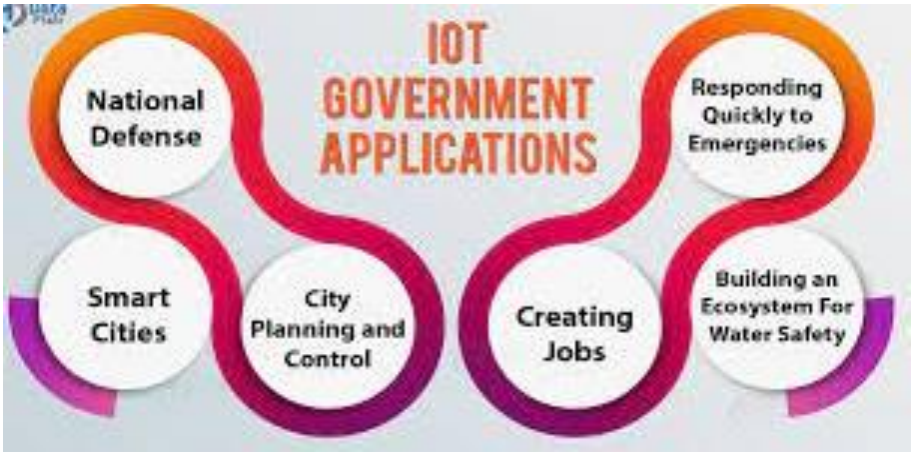

Figure 2 *overview of IoT government application [30]*

3. Establish a Framework for E-government

The primary framework of the E-Government Internet of Things can also be separated into the government collecting layer, the government data link layer, and the government application layer, based on the features of the multiple Internet of Things' main architecture. The auxiliary architecture contains the service security architecture, service assurance architecture, and access terminal layer [32]. E-government is a framework for providing government services to individuals through the use of information technology and technological communications. E-government refers to a variety of factors, including the use of the Internet and equipment like computers, to make government work easier while providing services to residents [33]. Adopting an e-government model can give several benefits to various stakeholders while also improving the functionality of services [34]. Within a perfectly working general pattern, people can use government services directly without going through several providers [35]. It then becomes the responsibility of the government to verify that such networks are safeguarded and, hence, that the entire paradigm of giving services to people is secure. Any e-government structure must include cybersecurity as a key component [36]. In today's society, information systems play a critical role in interpersonal and inter-organizational relationships. They are large-scale sociotechnical, formal, and organizational systems for gathering, processing, storing, and disseminating information [37]. Through the use of computer systems, information systems assist operations, management, and decision-making. Cybersecurity systems must be implemented into any information system to secure its overall integrity and functionality [38]. The core principle of e-government systems is to create a secure framework within which residents can access a variety of services. This framework must be protected to ensure social welfare [39], [40]. Other aspects in the case of Saudi Arabia include the government's competitiveness in achieving efficiency and maintaining a positive view of the global arena in order to secure a variety of economic interests figure 3.

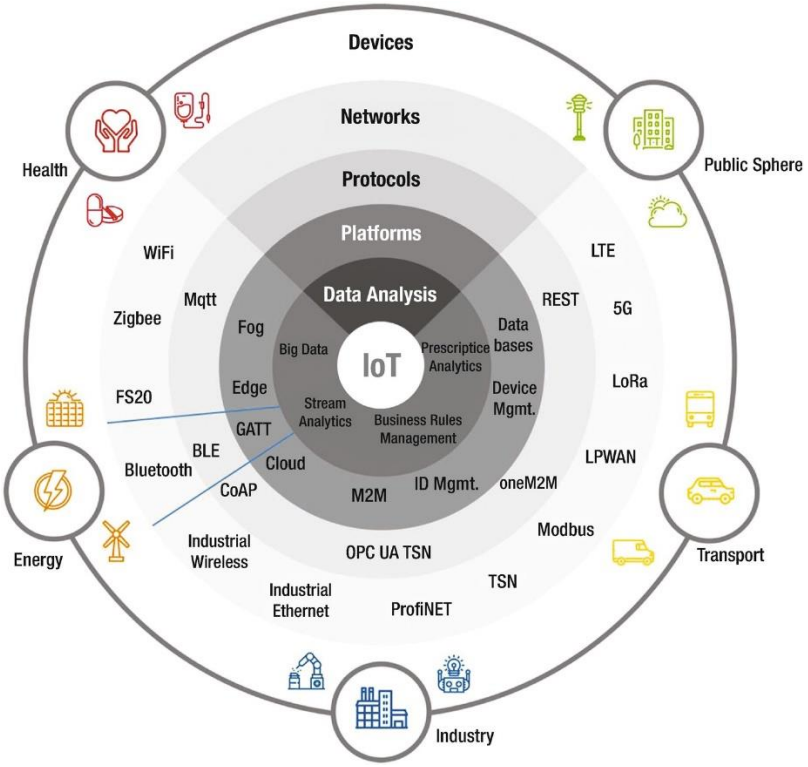

Figure 3 *overview of IoT e-government framework [41]*

4. In E-Government, IoT and Applications

The Internet of Things (IoT) can be used in e-government in a variety of ways. Data collected by IoT devices could be utilized to build several e-government applications. Every one of them might work to improve their analytics offerings to help people make better decisions faster [42], [41]. IoT applications in e-government, with an emphasis on safety and protection of the public, Transport, healthcare, and smart cities are all issues that need to be addressed. The latter is divided into two categories, environmental pollution and natural occurrences such as fire, earthquakes, and weather. The healthcare sector offers a significant possibility for IoT adoption [42] have mobility issues, such as the elderly or those with impairments, may benefit from the adoption of IoT systems. Citizens and society place a high value on security and safety. The Internet of Things (IoT) can help with a variety of security and safety issues. Object detection and sensor information fusion are possible thanks to the autonomous nature of IoT nodes, as well as their sensing and powerful onboard processing capabilities [43]. IoT nodes can be used to monitor country borders, whether they are on land, sea, or air, as well as other important places for the safety and protection of the public figure 4.

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

Figure 4 *overview IoT domain and application in e-government*

5. Overview of Challenges in E-government in the Context of IoT

The use of IoT in e-government can be both exciting and problematic. We ponder on the technical and non-technical issues that arise from the usage of IoT in e-government figure 5.

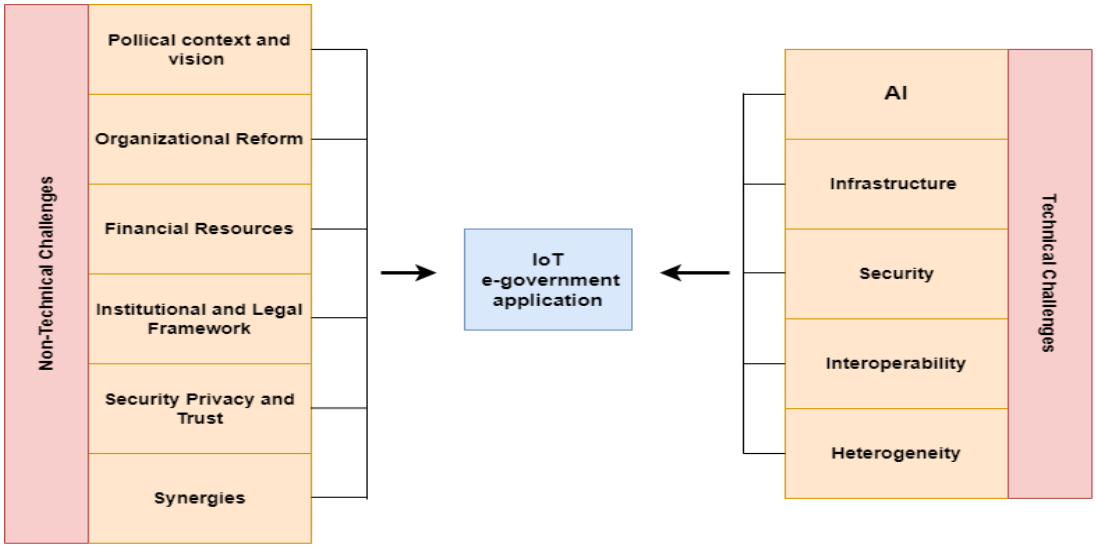

Figure 5 *overview of IoT e-government*

6. Technical Challenges

The core idea of the Internet of Things interacts with one another in this era [44]. Data and information interchange between peers, as well as interaction with cloud-based back-end systems, are examples of such interactions. Because of the autonomous character of IoT devices, we can benefit as a result of numerous operations becoming automated, information and service interoperability, and the examination of automated entity behaviour and characteristics.

- Heterogeneity

Furthermore, device heterogeneity is important in providing technologies that are supportable by the whole collection of nodes that are currently available. We will be able to establish Injecting smart government functions into devices through primary care. The variety of IoT gadgets makes connecting and communicating with them difficult [45]. Connectivity is critical for resolving the aforementioned issue and making data collecting from homogenous or heterogeneous IoT devices easier. The most difficult part is gathering data from sensors and then transforming it into a coherent representation for further processing. On top of the integrated data, effective interfaces can be created to simplify access to the acquired data, allowing knowledge to be generated.

- Interoperability

The sharing of information between communication entities, citizens, in particular, allows multiple authorities to communicate information and boost efficiency by reducing data discrepancies [45]. Technical interoperability is the process of preparing for the technical challenges that arise while connecting computer systems and services. Whereas semantic interoperability is concerned with imparting specific meaning to transmitted information. Finally, legal interoperability refers to the law that is coordinated such that data shared is given adequate legal weight.

- Security

The deployment of IoT in e-government is also beset by security issues. Because e-government services on the Cloud can be accessed by a variety of devices, it's critical to keep allowed info accessibility gathered, and inserted safely. This is one of the issues is severe when it comes to sensitive personal data. The self-contained nature of IoT networks creates issues. There has been a lot of talk regarding the dangers of hacking techniques and gadgets to get information and data. Which size the device, causing it to behave in a dangerous and insecure manner. The architecture of IoT e-government services, adopting multi-layered security services could be a solution for application security [46]. To ensure the necessary level of safety, e-government IoT systems can use firewalls.

- Infrastructure

The vast amount of data collected by IoT devices need a high-capacity [47] Network for storing and analysis to handle both in terms of the amount of information recorded and the rate at which it is produced. For optimal service provision, access to the Internet of Things Data from the e-government must be made public to make educated decisions in real-time and on a wide scale.

- Artificial Intelligence

The use of artificial intelligence (AI) in e-government applications is another obstacle to the implementation of IoT in e-government. AI may be used to create intelligent apps based on data obtained from many sources. Once AI is implemented, the available e-government apps will be able to enable human-like thinking and behaviors once AI is implemented [48]. Machine learning could give systems and gadgets the ability to identify patterns, make judgments on their own, or learn from existing models and alter decisions based on the current state of the environment.

7. Non-Technical Challenges

The Internet of Things (IoT) in e-government includes non-technical difficulties that are just as important, if not more so, than technical ones. These issues include a variety of different institutional and legal concerns. They have a significant impact on the effectiveness of any effort to leverage IoT technology capabilities in electronic government platforms [49]. They must be

cautiously considered and handled, owing to their structural complications, as well as the multiple interrelations between them.

- Political Context and Vision

Many factors may influence the strategic, tactical, and operational decisions that must be made and the actions that must be taken in the use of e-government in the context of IoT technology. Decisions and actions may relate to the expansion of existing e-government systems and services, as well as the development of new ones that take advantage of IoT [50]. These kinds of considerations concerning strategies and activities for advancing smart government initiatives using IoT do not have to come from the top-down but might instead begin at the local level.

- Organizational Reform

Introduce new ones based on IoT, the implementation of IoT in e-government necessitates organizational reform and process redesign. This may necessitate the establishment of new government authorities, institutions [51]. Level of cooperation between organizations, involving the integration of many entities that must interact and rely on one another in an unbroken chain.

- Financial Resources

As noted previously, the shift to e-government with IoT capabilities necessitates the reliability and accessibility of required funds and facilities, like 5G cellular systems [52]. Additional funding for Internet of Things e-government applications is critical for their feasibility and long-term viability, including sufficient funding and proper billing structures.

- Framework for Institutions and Law

IoT-based data sources and services must be formalized by institutional frameworks, meet legal requirements, and adhere to rules. As a result, effective IoT deployment in e-government necessitates substantial institutional backing. At the same time, institutions and legislation can encourage governments to use IoT by requiring technological evolution and implementation in government operations. For example, as part of its 2020 plan, Estonia intends to apply the "no legacy concept," which will be enacted into law and states that the public sector shall not use any ICT solution that is more than 13 years old (e-Estonia, 2018).

- Security, Privacy and Trust

Data security and privacy are concerns that cut across practically every IoT e-government application. Safety and privacy are important challenges in IoT e-government, including components that require a non-technical approach in addition to their technological qualities [53]. Furthermore, personal data protection and administration are essential in nearly every area of e-government based on IoT, operating in highly sensitive sectors like healthcare.

- Synergies

The successful use of IoT in e-government must be encouraged through collaboration with academic and research organizations, as well as public-private area synergies. This will allow for the creation of IoT applications and infrastructure, as well as the infrastructure required to support them effectively. As indicated in the World Bank Group (2017) study by lessons learned during the actual execution of IoT-oriented initiatives in numerous countries, public-private sector collaborations are a crucial aspect for the effective implementation of the Internet of Things in e-government [54]. Such collaborations can also aid in the creation of IoT-based business models with long-term viability.

8. Discussion

We take a comprehensive look at this chapter on IoT adoption in e-government. It gives an overview of the Internet of Things' potential in e-government across numerous application domains, stressing the difficulties that need to be addressed in each. We also look into the challenges that must be addressed and handled for IoT in e-government to achieve its full potential. With the use of IoT in e-government still in its initial stages. The publish-subscribe architecture allows for device interaction. The usage of final point via which gadgets used by end consumers can be connected and obtain information. The data required will be handled by the endpoint, which will be backed up by a data interchange mechanism.

The functions of the cybersecurity framework can provide a high-level and strategic focus of the lifecycle of e-government risk management connected to cybersecurity. The framework core can be considered essential in determining the important discrete outcomes for each e-government platform function. The implementation layers of the framework put the relationship between e-government systems and cybersecurity threats into context [55]. This contextualization takes place inside a complete framework that includes thorough risk mitigation considerations. The tiers are used to describe how far an organization and its cybersecurity risk reduction management system have progressed [56]. A system of sensors could be used to monitor a forest to detect fires.

Our contribution to this chapter is regarding the government's public services and IoT implementation in terms of safety and privacy. Personal information security is discussed from a broad viewpoint. It evaluates how the government offers good public services that are acceptable to the public, as well as specific strategies and plans for achieving them in light of technological advancement and progress. In addition, the application domains and problems connected with IoT implementation in e-government were discussed in this chapter. The e-government platform can be adapted to particular user numbers and can allow various roles. The flexible, strategy based on roles may improve data delivery efficiencies, preparing the ground for a customized e-government platform. Additionally, people and IoT devices must be monitored, for the target application, as well as trackers and location-based information sharing, can only be authorized if citizen data security and privacy are maintained, and user consent is obtained. The application of mobile IoT systems can facilitate a broad range of safety and protection activities, including area monitoring and tracking, advanced threat detection, effective event management, quick response to emergency situations, security/safety risk alerts, and communication of current status to people. Such IoT-enabled activities can be used in a variety of settings, including unauthorized Management and

controls, healthcare, transport, and climate analysis and forecasting are all areas that need to be monitored and forecasted.

9. Conclusion and Future Work

The Internet of Things (IoT) is becoming more significant in everyday life as a mechanism for making major decisions in a variety of fields. As smart devices and data in real-time are connected and updated. IoT is being used in a variety of ways to provide digital services to the public, online payment, property purchase, and sailing are just a few examples. On the other hand, users' complaints about the safety and privacy of their personal information are growing. The Internet of Things (IoT) is becoming more popular and significantly enhances e-government. This chapter primarily focuses on how potential users can obtain information to use the Internet of Things and its related services within the e-government sectors. There are several technological, administrative, and political challenges to IoT adoption problems in e-government and legal problems that must be solved to develop effective and required applications. It's crucial to explore these problems and potential solutions. The adoption of mobile IoT systems can open up a world of possibilities of security and safety-related activities, including area surveillance and monitoring, threat detection, effective event management, quick response to emergency situations, security/safety risk alerts, and communication of current status to people. Such IoT-enabled activities can be used in a variety of settings, including Management and controls, healthcare, transport, and climate analysis and forecasting are all areas that need to be monitored and forecasted.

Reference

[1] Qi, R., Feng, C., Liu, Z., & Mrad, N. (2017). Blockchain-powered internet of things, e-governance and e-democracy. In *E-Democracy for Smart Cities* (pp. 509-520). Springer, Singapore. https://link.springer.com/chapter/10.1007/978-981-10-4035-1_17

[2] Balaji, R. D., Jaboob, S., & Malathi, R. (2021). A Block Chain and IoT Based Hybrid Students Record System for E-Governance. *Current Journal of Applied Science and Technology*, 59-71. https://journalbank.org/index.php/CJAST/article/view/2453

[6] Zaoui, I., Elmaghraoui, H., Chiadmi, D., & Benhlima, L. (2014). Towards a personalized e-government platform. *International Journal of Computer Science: Theory and Application*, *2*(2), 35-40.https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.1018.918&rep=rep1&type=pdf

[7] Saxena, S. (2017). Factors influencing perceptions on corruption in public service delivery via e-government platform. *foresight*. https://www.emerald.com/insight/content/doi/10.1108/FS-05-2017-0013/full/html

[8] Tingjun, Z. (2015). The Analysis of Behavior and Effectiveness of Public Participating in E-government Platform of City Public Service——A Case Study of the Mayor's Hotline in Fuzhou. *Journal of Public Management*, 02. https://en.cnki.com.cn/Article_en/CJFDTotal-GGGL201502003.htm

[9] Tikkanen, E., Gustafsson, S., & Ingelsson, E. (2018). Associations of fitness, physical activity, strength, and genetic risk with cardiovascular disease: longitudinal analyses in the UK Biobank study. *Circulation*, *137*(24), 2583-2591. https://www.ahajournals.org/doi/full/10.1161/CIRCULATIONAHA.117.032432

[10] Alhawawsha, M., & Panchenko, T. (2020, January). Open Data Platform Architecture and Its Advantages for an Open E-Government. In *International Conference on Computer Science, Engineering and Education Applications* (pp. 631-639). Springer, Cham. https://link.springer.com/chapter/10.1007/978-3-030-55506-1_56

[11] Adjei-Bamfo, P., Maloreh-Nyamekye, T., & Ahenkan, A. (2019). The role of e-government in sustainable public procurement in developing countries: A systematic literature review. *Resources, Conservation and Recycling*, *142*, 189-203. https://www.sciencedirect.com/science/article/abs/pii/S0921344918304579

[12] Al-Mushayt, O. S. (2019). Automating E-government services with artificial intelligence. *IEEE Access*, *7*, 146821-146829. https://ieeexplore.ieee.org/abstract/document/8862835

[13] Lv, Z., Li, X., Wang, W., Zhang, B., Hu, J., & Feng, S. (2018). Government affairs service platform for smart city. *Future Generation Computer Systems*, *81*, 443-451. https://www.sciencedirect.com/science/article/abs/pii/S0167739X17311391

[14] Qi, M., & Wang, J. (2021). Using the Internet of Things e-government platform to optimize the administrative management mode. *Wireless Communications and Mobile Computing*, *2021*. https://www.hindawi.com/journals/wcmc/2021/2224957/

[15] Cheng, B., Solmaz, G., Cirillo, F., Kovacs, E., Terasawa, K., & Kitazawa, A. (2017). FogFlow: Easy programming of IoT services over cloud and edges for smart cities. *IEEE Internet of Things Journal*, *5*(2), 696-707. https://ieeexplore.ieee.org/abstract/document/8022859/

[16] Gershon, D., Prince, O., & Opoku, A. M. (2018). Promoting Inclusiveness and Participation in Governance: The Directions of Electronic Government in Ghana. *International Journal of Social Sciences*, *7*(3), 397-406. https://www.indianjournals.com/ijor.aspx?target=ijor:ijsw&volume=7&issue=3&article=007

[17] AlEnezi, A., AlMeraj, Z., & Manuel, P. (2018, April). Challenges of IoT based smart-government development. In *2018 21st Saudi Computer Society National Computer Conference (NCC)* (pp. 1-6). IEEE. https://ieeexplore.ieee.org/abstract/document/8593168

[18] Sava, A. (2018). IoT Technologies: Realities of the Future. *Social-Economic Debates*, *7*(1), 100-105. http://economic-debates.ro/art11-Sava-economic-debates-2018.pdf

[19] Nagowah, S. D., Sta, H. B., & Gobin-Rahimbux, B. A. (2018, October). An overview of semantic interoperability ontologies and frameworks for IoT. In *2018 Sixth International Conference on Enterprise Systems (ES)* (pp. 82-89). IEEE.

[20] Pradhan, P., & Shakya, S. (2018). Big Data Challenges for e-Government Services in Nepal. *Journal of the Institute of Engineering*, *14*(1), 216-222. https://www.nepjol.info/index.php/JIE/article/view/20087

[21] Elezaj, O., Tole, D., & Baci, N. (2018). Big Data in e-Government Environments: Albania as a Case Study. *Academic Journal of Interdisciplinary Studies*, *7*(2), 117. https://www.mcser.org/journal/index.php/ajis/article/view/10285

[22] Henriksen, H. Z. (2018). One step forward and two steps back: e-Government policies in practice. In *Policy Analytics, Modelling, and Informatics* (pp. 79-97). Springer, Cham. https://link.springer.com/chapter/10.1007/978-3-319-61762-6_4

[23] Chishiro, H., Tsuchiya, Y., Chubachi, Y., Abu Bakar, M. S., & De Silva, L. C. (2017, June). Global PBL for environmental IoT. In *Proceedings of the 2017 International Conference on E-commerce, E-Business and E-Government* (pp. 65-71). https://dl.acm.org/doi/abs/10.1145/3108421.3108437

[24] Máchová, R. (2017). Measuring the effects of open data on the level of corruption. In *Proceedings of the 21th International Conference Current Trends in Public Sector Research*. Masarykova univerzita. https://dk.upce.cz/handle/10195/66979

[25] Mahmood, Z. (Ed.). (2016). *Connectivity frameworks for smart devices: the internet of things from a distributed computing perspective*. Springer. https://link.springer.com/book/10.1007%2F978-3-319-33124-9

[26] Le, N. T., & Hoang, D. B. (2016, December). Can maturity models support cyber security?. In *2016 IEEE 35th international performance computing and communications conference (IPCCC)* (pp. 1-7). IEEE. https://ieeexplore.ieee.org/abstract/document/7820663

[27] Koo, E. (2019). *Digital transformation of Government: from E-Government to intelligent E-Government* (Doctoral dissertation, Massachusetts Institute of Technology). https://dspace.mit.edu/handle/1721.1/121792

[28] Chinese Academy of Cyberspace Studies. (2019). The World e-Government Development. *World Internet Development Report 2017: Translated by Peng Ping*, 159-197. https://link.springer.com/chapter/10.1007/978-3-662-57524-6_6

[29] Ma, L., & Zheng, Y. (2019). National e-government performance and citizen satisfaction: a multilevel analysis across European countries. *International Review of Administrative Sciences*, *85*(3), 506-526. https://journals.sagepub.com/doi/abs/10.1177/0020852317703691

[30] Pathak, A., AmazUddin, M., Abedin, M. J., Andersson, K., Mustafa, R., & Hossain, M. S. (2019). IoT based smart system to support agricultural parameters: A case study. *Procedia Computer Science*, *155*, 648-653. https://www.sciencedirect.com/science/article/pii/S1877050919310087

[31] Alexopoulos, C., Lachana, Z., Androutsopoulou, A., Diamantopoulou, V., Charalabidis, Y., & Loutsaris, M. A. (2019, April). How machine learning is changing e-government. In *Proceedings of the 12th International Conference on Theory and Practice of Electronic Governance* (pp. 354-363). https://dl.acm.org/doi/abs/10.1145/3326365.3326412

[32] Muzafar, S., & Jhanjhi, N. Z. (2020). Success Stories of ICT Implementation in Saudi Arabia. In *Employing Recent Technologies for Improved Digital Governance* (pp. 151-163). IGI Global. https://www.igi-global.com/chapter/success-stories-of-ict-implementation-in-saudi-arabia/245980

[33] Hamid, B., Jhanjhi, N. Z., & Humayun, M. (2020). Digital Governance for Developing Countries Opportunities, Issues, and Challenges in Pakistan. In *Employing Recent Technologies for Improved Digital Governance* (pp. 36-58). IGI Global. https://www.igi-global.com/chapter/digital-governance-for-developing-countries-opportunities-issues-and-challenges-in-pakistan/245975

[34] Kumar, P., Kunwar, R. S., & Sachan, A. (2016). A survey report on: Security & challenges in internet of things. In *Proc National Conference on ICT & IoT* (pp. 35-39). https://shop.iotone.ir/public/upload/article/5b8e38ead1f31.pdf

[35] Sharma, P., Zawar, S., & Patil, S. B. (2016). Ransomware Analysis: Internet of Things (Iot) Security Issues, Challenges and Open Problems Inthe Context of Worldwide Scenario of Security of Systems and Malware Attacks. In *International conference on recent Innovation in Engineering and Management* (Vol. 2, No. 3, pp. 177-184). http://www.ijirse.com/wp-content/upload/2016/02/1089B.pdf

[36] CIRNU, C. E. (2016). How EU and Japan Deal with the Challenges of Cybersecurity in the eGovernment Domain in the Emerging Age of IoT?. https://www.kgri.keio.ac.jp/en/docs/GWP_33.pdf

[37] Bhattacharya, K., & Suri, T. (2017). The curious case of e-governance. *IEEE Internet Computing*, *21*(1), 62-67. https://ieeexplore.ieee.org/abstract/document/7839849

[38] SAQIB, M., & Al-Muqrashi, N. (2017). Role and Importance of IoT in the smart city and E-Governance. *Journal of Student Research*. https://jsr.org/index.php/path/article/view/544

[39] Baxter, D. J. (2017). E-governance and e-participation via online citizen budgets and electronic lobbying: Promises and challenges. *World Affairs*, *180*(4), 4-24. https://scholar.google.com/scholar?q=IoT+and+e-governance+challenges&hl=en&as_sdt=0%2C5&as_ylo=2017&as_yhi=2017

[40] NEMÈšANU, F., & PĂŽNZARU, F. (2017). Smart city management based on IoT. *Smart Cities and Regional Development (SCRD) Journal*, *1*(1), 91-97. https://www.ceeol.com/search/article-detail?id=624232

[41] Yadav, E. P., Mittal, E. A., & Yadav, H. (2018, February). IoT: Challenges and issues in indian perspective. In *2018 3rd International Conference On Internet of Things: Smart Innovation and Usages (IoT-SIU)* (pp. 1-5). IEEE. https://ieeexplore.ieee.org/abstract/document/8519869

[42] Elijah, O., Rahman, T. A., Orikumhi, I., Leow, C. Y., & Hindia, M. N. (2018). An overview of Internet of Things (IoT) and data analytics in agriculture: Benefits and challenges. *IEEE Internet of Things Journal*, *5*(5), 3758-3773. https://ieeexplore.ieee.org/abstract/document/8372905

[43] Khan, M. A., & Salah, K. (2018). IoT security: Review, blockchain solutions, and open challenges. *Future generation computer systems*, *82*, 395-411. https://www.sciencedirect.com/science/article/abs/pii/S0167739X17315765

[44] Saleem, J., Hammoudeh, M., Raza, U., Adebisi, B., & Ande, R. (2018, June). IoT standardisation: Challenges, perspectives and solution. In *Proceedings of the 2nd international conference on future networks and distributed systems* (pp. 1-9). https://dl.acm.org/doi/abs/10.1145/3231053.3231103

[45] Papadopoulou, P., Kolomvatsos, K., & Hadjiefthymiades, S. (2020). Internet of Things in E-Government: Applications and Challenges. *International Journal of Artificial Intelligence and Machine Learning (IJAIML)*, *10*(2), 99-118. https://www.igi-global.com/article/internet-of-things-in-e-government/257274

[46] Birkel, H. S., & Hartmann, E. (2019). Impact of IoT challenges and risks for SCM. *Supply Chain Management: An International Journal*. https://www.emerald.com/insight/content/doi/10.1108/SCM-03-2018-0142/full/html

[47] Ahmad, R., Asim, M. A., Khan, S. Z., & Singh, B. (2019, March). Green IOT—issues and challenges. In *Proceedings of 2nd International Conference on Advanced Computing and Software Engineering (ICACSE)*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3350317

[48] Afzal, B., Umair, M., Shah, G. A., & Ahmed, E. (2019). Enabling IoT platforms for social IoT applications: Vision, feature mapping, and challenges. *Future Generation Computer Systems*, *92*, 718-731. https://www.sciencedirect.com/science/article/abs/pii/S0167739X17312724

[49] Wang, N., Wang, P., Alipour-Fanid, A., Jiao, L., & Zeng, K. (2019). Physical-layer security of 5G wireless networks for IoT: Challenges and opportunities. *IEEE Internet of Things Journal*, *6*(5), 8169-8181. https://ieeexplore.ieee.org/abstract/document/8758230

[50] Tawalbeh, L. A., Muheidat, F., Tawalbeh, M., & Quwaider, M. (2020). IoT Privacy and security: Challenges and solutions. *Applied Sciences*, *10*(12), 4102. https://www.mdpi.com/2076-3417/10/12/4102

[51] Gupta, B. B., & Quamara, M. (2020). An overview of Internet of Things (IoT): Architectural aspects, challenges, and protocols. *Concurrency and Computation: Practice and Experience*, *32*(21), e4946. https://onlinelibrary.wiley.com/doi/abs/10.1002/cpe.4946

[52] Nižetić, S., Šolić, P., González-de, D. L. D. I., & Patrono, L. (2020). Internet of Things (IoT): Opportunities, issues and challenges towards a smart and sustainable future. *Journal of Cleaner Production*, *274*, 122877. https://www.sciencedirect.com/science/article/pii/S095965262032922X

[53] Sadeeq, M. M., Abdulkareem, N. M., Zeebaree, S. R., Ahmed, D. M., Sami, A. S., & Zebari, R. R. (2021). IoT and Cloud computing issues, challenges and opportunities: A review. *Qubahan Academic Journal*, *1*(2), 1-7. https://journal.qubahan.com/index.php/qaj/article/view/36

[54] Makhshari, A., & Mesbah, A. (2021, May). IoT bugs and development challenges. In *2021 IEEE/ACM 43rd International Conference on Software Engineering (ICSE)* (pp. 460-472). IEEE. https://ieeexplore.ieee.org/abstract/document/9402092

[55] Sadeeq, M. M., Abdulkareem, N. M., Zeebaree, S. R., Ahmed, D. M., Sami, A. S., & Zebari, R. R. (2021). IoT and Cloud computing issues, challenges and opportunities: A review. *Qubahan Academic Journal*, *1*(2), 1-7. https://journal.qubahan.com/index.php/qaj/article/view/36

[56] Thakkar, A., & Lohiya, R. (2021). A review on machine learning and deep learning perspectives of IDS for IoT: recent updates, security issues, and challenges. *Archives of Computational Methods in Engineering*, *28*(4), 3211-3243. https://link.springer.com/article/10.1007/s11831-020-09496-0

.