

USE OF ARTIFICIAL INTELLIGENCE TO ENHANCE E-GOVERNMENT SERVICES

¹Uralova Iroda Abduvali qizi, ²Karimova Gavhar Samandar qizi

¹i.abduvaliyevna@tuit.uz

²karimovagavhar50@gmail.com

¹Assistant at the Tashkent university of information technologies named after Muhammad al-Khwarizmi

²Master's student at the Tashkent University of Information Technologies named after Muhammad al-Khwarizmi

Abstract: E-governance plays a crucial role in delivering government services efficiently and cost-effectively to citizens. With rapid technological advancements, governments face challenges such as integration issues, data security risks, and limited accessibility of services. To overcome these challenges, the use of Artificial Intelligence (AI) and the Internet of Things (IoT) is essential. AI and IoT technologies can improve service quality, enhance security by detecting cyber threats, and enable real-time monitoring in areas such as healthcare, transportation, and public safety. However, successful implementation requires a unified, platform-independent framework that ensures usability, efficiency, and security. The proposed approach focuses on using AI-driven IoT systems to enhance e-government services, reduce risks, and improve overall service delivery for all stakeholders.

Keywords: E-Government, Artificial Intelligence (AI), Internet of Things (IoT), Smart Governance, Data Security and Privacy, Interoperability, Citizen-Centric Services, Digital Transformation

The Internet of Things (IoT) is a model in which connecting items with various sensors and actuating devices over the Internet allows for collecting, sharing, and analyzing data to enable creative applications. IoT can assist the creation of numerous new services for people, corporations, and governments by allowing interaction with a wide range of things such as household items, CCTV, smartwatches, cellphones, corporate sensors, and automobiles. This framework is used in various disciplines, including transport, electricity and utilities, education, medical services, equipment, public security, and defense [1,2].

The challenges in the current development of IoT and AI applications and services must be overcome if such applications and services are to enhance public governance and people's livelihoods.

Interoperability

The framework of the Internet-of-things AI applications is made up of many core components, including sensor systems or surveillance systems that collect information from people, entities, and the surroundings, communications networks and systems, and toolkits or devices for storing and processing data, all of which use various technologies [1]. Furthermore, the system could be interoperable with many other governmental apps. Moreover, the large number of technologies may cause issues with maintenance services and sustainability.

Proposed framework for smart government

The significant challenges are posed by the type of data received through IoT and the smart government AI applications. Considering the complexities of these applications, a holistic approach is required that accounts for essential components and combines them in a comprehensive research framework.

The framework is represented in Fig. 1 and is used to identify gaps in the existing literature.

Input: Domain knowledge is provided as input to IoT-enabled AI system. Influence: The IoT-enabled AI system in turn, influences decision-making and outcome in the various domains of the smart governance.

Support: Indicates that IoT-enabled AI system in turn, supports the activities of the stakeholders.

In this paper, Internet of Things and Artificial Intelligence frameworks are evaluated for smart governance to identify shortcomings, then describe our suggested framework, which integrates Internet of Things and Artificial Intelligence aspects to create a more comprehensive framework. The majority of Internet of Things and Artificial Intelligence frameworks are focused on smart government, specifically, cloud computing [3], m-hospital [4], sustainable energy [5] or security and privacy [6,7] while the standard IoT models [8,9] do not incorporate AI applications, as is important in our studies.

They are notable exceptions, proposing an educational system for sustainable city applications that mixes IoT with AI (machine learning) approaches [10]. A smart city is split into units on the physical entity layer, and real-time information is recorded via sensing devices and social networks. Sensing data is arranged depending on logical meaning and common facilities like social networks, water quality, and traffic patterns. All this data is further standardized and linguistically labeled at the abstraction entity layer. The streaming data layer combines relevant information into frames based on the needs of various smart city applications, and the fusion layer aggregates and converts this information to domain expertise.

In the same manner [11], suggested, implemented, and provided feedback on a “360 Degree Model” for ordering sustainable urban activities, including municipal authorities, people, and specialists. IoT and AI-related activities were identified as the main prospects for execution in the near-term, if they have not already been realized in certain situations, according to their research.

The “360 Degree Model” represents a comprehensive governance approach aimed at ensuring sustainable development in smart cities and e-government systems. Within this model, government authorities, citizens, and experts collaboratively participate in decision-making processes, ensuring the involvement of all key stakeholders. The model relies on Internet of Things (IoT) and Artificial Intelligence (AI) technologies to enable real-time data collection, analysis, and the formulation of effective governance decisions. As a result, urban infrastructure, social services, and economic processes are managed in an integrated manner, leading to increased efficiency and enhanced transparency.

Governments have tried to build an IoT legislative framework, which might guide the administration of Internet - of - things better structures for governing Internet-of-Things smart apps and services [12]. The involvement component focuses on key stakeholders working together to create an accessible IoT ecosystem. Ethical norms, laws, and contractual structures are examples of ways to facilitate successful participation.

In this paper, a scientific framework using the IoT-enabled AI system technology aspects is addressed. It includes various gadgets and sensing devices. The data representation, social platforms and process, transmission, predictive analysis, and AI-based smart government services and applications are proposed. The IoT and AI standards to control such systems, and legislation and regulation would aid in resolving the issues are also incorporated. The model also includes all the stakeholders for such services and applications, specifically, governments, businesses, academics, and the general public and their distinct features.

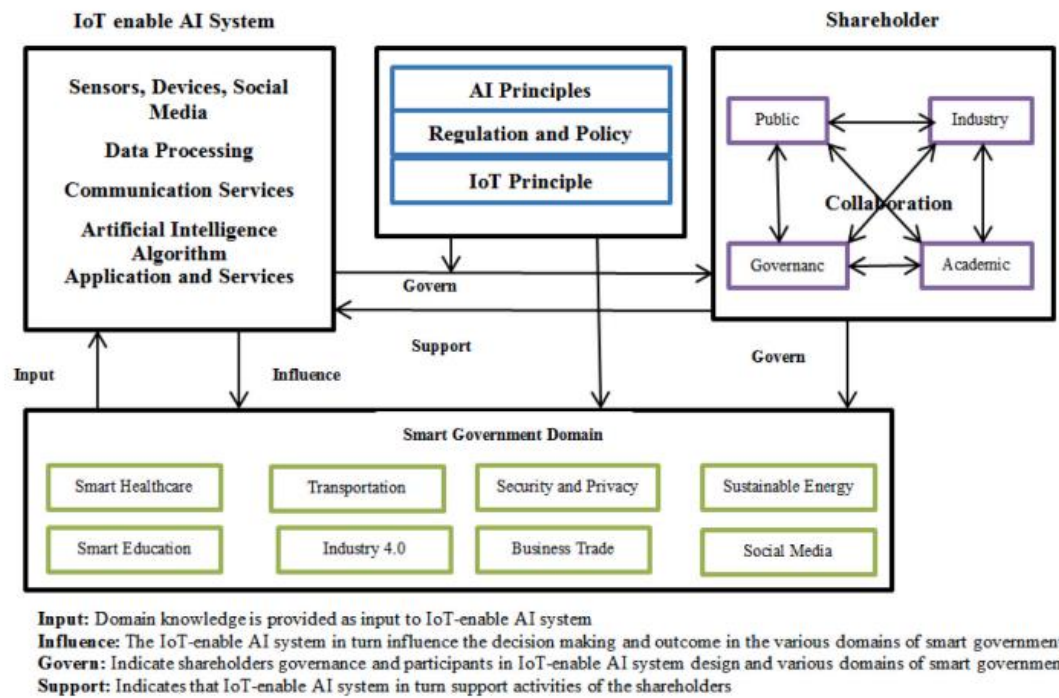


Figure 1. The proposed framework.

REFERENCES

1. J.Gubbi, R.Buyya, S.Marusic, M.Palaniswami, Internet of Things (IoT): a vision, architectural elements, and future directions, *Future Generat. Comput. Syst.* 29 (7) (2013) 1645–1660.
2. S.Chatterjee, A.K.Kar, M.P.Gupta, Success of IoT in smart cities of India: an empirical analysis, *Govern. Inf. Q.* 35 (3) (2018) 349–361.
3. R.Lea, M.Blackstock, City hub: a cloud-based iot platform for smart cities, in: 2014 IEEE 6th International Conference on Cloud Computing Technology and Science, 2014, pp. 799–804.
4. M.M.Hassan, H.S.Albahr, H.Al-Dossari, Internet of things framework for pervasive healthcare, in: 1st International Workshop on Emerging Multimedia Applications and Services for Smart Cities vol. 1, EMASC, 2014.
5. S.Khan, D.Paul, P.Momtahan, M.Aloqaily, Artificial intelligence framework for smart city microgrids: state of the art, challenges, and opportunities, in: 2018 Third International Conference on Fog And Mobile Edge Computing, FMEC, 2018, pp. 283–288.
6. A.T.Chatfield, C.G. Reddick, A framework for Internet of Things-enabled smart government: a case of IoT cybersecurity policies and use cases in US federal government, *Govern. Inf. Q.* 36 (2) (2019) 346–357.
7. S.Haque, S.Zeba, M.Alimul Haque, K.Kumar, M.P.Ali Basha, An IoT model for securing examinations from malpractices, *Mater. Today Proc.*, Apr. (2021), <https://doi.org/10.1016/j.matpr.2021.03.413>.
8. B.W.Wirtz, J.C.Weyerer, F.T.Schichtel, An integrative public IoT framework for smart government, *Govern. Inf. Q.* 36 (2) (2019) 333–345.
9. N.Almrezeq, M.A.Haque, S.Haque, A.A.El-Aziz, Device access control and key exchange (DACK) protocol for internet of things, *Int. J. Cloud Appl. Comput. (IJCAC)* 12 (1) (Jan. 2022) 1–14, <https://doi.org/10.4018/IJCAC.297103>.
10. N.Zhang, H.Chen, X.Chen, J.Chen, Semantic framework of internet of things for smart cities: case studies, *Sensors* 16 (9) (2016) 1501.

- 
11. Y.Charalabidis, C.Alexopoulos, N.Vogiatzis, D.E.Kolokotronis, A 360-degree model for prioritizing smart cities initiatives, with the participation of municipality officials, citizens and experts, in: *E-Participation in Smart Cities: Technologies and Models of Governance for Citizen Engagement*, Springer, 2019, pp. 123–153.
 12. A.Kankanhalli, Y.Charalabidis, S.Mellouli, IoT and AI for smart government: a research agenda, *Govern. Inf. Q. Elsevier* 36 (2) (2019) 304–309.