K-tech

Government of Karnataka
Dept. of E, IT & Bt

World Economic Forum

International Institute of Information Technology Bangalore

Ethical Assessment Framework for IoT Solutions in Smart Cities

January 2025

Centre for Internet of Ethical Things (CIET)
IIIT-Bangalore

Table of Contents

Preface

This policy brief is an outcome of a research study that was carried out for a period of one year, funded by the Government of Karnataka. This research was part of a project that is the result of a tripartite agreement entered between IIIT-Bangalore, the Government of Karnataka, and the World Economic Forum. The objectives of this project are multi-fold and call for both technical and policy research at the intersection of Ethics and Internet of Things (IoT) in the following application domains – Smart cities, Manufacturing, Agriculture, Healthcare, and Education. The project is planned for five years with different teams at IIIT-B working on various technical and policy aspects. The following work is based on the policy strand of this project which in the first year focused on building an ethical assessment framework for IoT interventions in one of the said application domains: smart cities. Through the policy strand we also, for the long term, plan to contextualize research output from other technical teams working on the project.

For feedback and more information on the effort, please write to ciet-admin@iiitb.ac.in

CIET Policy Team

Amit Prakash Professor, **Bidisha Chaudhuri*** Associate Professor,
Vinay Reddy Venumuddala** Post-doctoral Researcher,
Deepa Austin Post-doctoral Researcher, **Swati Ganeshan** Research Associate

*Current Affiliation - University of Amsterdam
**Current Affiliation - Mahindra University, Hyderabad

Acknowledgements

We thank our interview respondents from academia and industry who provided valuable inputs for the ethical framework. We are also grateful for the reviews and inputs that we received on the ethical framework from the participants of the stakeholders' meet held in June 2024. We thank the Secretary, Managing Director, General Manager, and other representatives of the Department of Electronics, Information Technology and Biotechnology, Government of Karnataka and officials from the World Economic Forum for their continued support to CIET.

Overview

Objective

In this study, we aim to arrive at a contextually adaptable policy framework to evaluate the ethical concerns of IoT interventions in smart city initiatives keeping the context of urban governance in mind.

Our objective here was to arrive at a contextually adaptable framework by starting from a detailed study of real-world IoT interventions proposed in one application domain, i.e., smart cities.

We do so by looking at four main ethical dimensions: **Justice & Equity, Fairness, Trust & Consent and Dignity of life and work.**

Methodology

To arrive at this framework, we relied on an extensive literature review, semi-structured interviews with pertinent stakeholders from the industry, academia, and the government.

We also looked at reports, tenders, project proposals, and policies around the planned smart city IoT interventions.

Ethical Dimesions

01

Justice and Equity

Defined in terms of equal opportunities to end-users irrespective of socio-economic and digital divides, and equal opportunities for small and large firms in contributing to delivery of domain-specific services

02

Fairness

Refers to the unbiasedness of both outcomes of the system as well as the intentions and convictions underpinning a system

03

Trust and Consent

Refers to the end-user confidence in the intervention to fulfil its intended function. It depends on features such as privacy, safety and security, and accountability built into the system

04

Dignity of Life and Work

Signifies meaningful role and autonomy of operational staff, and meaningful choices for end-users to access the system without forgoing agency

IoT and Urban Governance

IoT interventions are known to facilitate interoperability between different civic-service related systems and enable data-driven decision making with the help of uniquely identifiable devices. They have three critical features - central data-driven decision-making, predominance of online channels and a one-size-fits-many approach. Each of these features give rise to distinct ethical dilemmas. Moreover, such interventions may ignore the existing socio-economic, and spatial realities. They may also fail to account for the autonomy of citizens and their rights. In addition, such centralised control and online modes of service delivery would need to be tackled through appropriate modes of governance.

Against this backdrop, the role of the ethical framework developed is twofold:

To equip decision-makers with the capacity to evaluate any IoT-intervention in a way that does not require extensive technical understanding of the IoT-intervention's inner workings.

To ensure that all relevant agents who are participating in the delivery of a particular service are acknowledged. Through this, authorities will also be able to gauge the potential impact the IoT intervention might have on such agents.

The Case of Smart Cities

In the domain of Smart Cities, we looked at four IoT interventions - Public Bike Sharing (PBS) system, Intelligent Transport Management System (ITMS), Solid Waste Management (SWM), and Integrated Command and Control Centre (ICCC). Interventions like PBS, and some use-cases within ITMS require citizens to access civic services through complete online channels. In interventions like SWM, and some use-cases within ITMS human intermediaries (like frontline-staff) facilitate online channels of access for civic services to the citizens. ICCC is a typical IoT intervention which is a platform that facilitates the integration of data generated from the above interventions, and many more.

We gathered a detailed understanding about the potential use-cases entailed through these IoT interventions through interviews, and archival study of tenders and detailed project reports. We then analysed the findings through the lens of the four ethical dimensions introduced earlier in order to arrive at the ethical assessment framework. We present the framework along the four ethical dimensions and along the three important roles played by the authorities while governing such interventions - executive, legislative, and standard setting.

Recommendations

- Carry out a stakeholder mapping to identify both the existing and prospective stakeholders with a clear understanding of their roles and responsibilities.
- Engage with the identified stakeholders (including citizens) to ensure that their dignity of life and work is safeguarded.
- Assess whether the identified stakeholders have equitable access to the intended services.
- Ensure that there are mechanisms in place for ascertaining whether the proposed processes are fair and just.
- Implement transparent data sharing and accountable governance practices to instil trust amongst the identified stakeholders, including the citizen-beneficiaries.
- Conduct an outcome-based analysis by revisiting the objectives and the ground realities post-implementation.

The questions presented in the framework below are the outcome of an extensive **ethical elicitation process** that has been carried out by CIET. While the agencies engage in the activities recommended above, they may use the suggested questions from the framework and come up with more concrete technical and procedural requirements that may need to be adopted to mitigate any potential ethical concerns from AI/IoT interventions related to Justice, Trust, Fairness, and Dignity for their specific use-case.

The Ethical Framework

Justice and Equity

LEGISLATIVE	EXECUTIVE	STANDARD SETTING
What according to you are the rights of the citizens that are likely to be impacted by this IoT intervention?	Who are the existing (before the IoT intervention) agents participating in the service delivery process? (Kindly include decision makers, last-mile operational staff, informal business, local, on-ground services if any)	What methods and technical specifications do you suppose the IoT intervention should adhere to in order to deliver expected outcomes? (Right from requirements gathering to implementation phases)
How does the intervention change/alter the rights and roles of the existing agents?	How will the role of the agents mentioned above change with the introduction of the IoT intervention?	Have the methods adopted taken voices of all agents/citizens into account?
What are the new interactions amongst the agents and between agents, citizens and devices (list new agents if any) that the IoT intervention has given rise to (if any)?	Are there any new agents introduced into the IoT-enabled system?	If not, what kind of technical additions/changes can be put in place to facilitate the equitable participation of agents associated with the service delivery?
What are the prescribed workplace protocols that agents need to adhere to in order to safeguard the respect of other agents within the system? (Please mention any instructions or guides on professional behaviour of agents in the IoT system)?	What differences do you see in the service delivery process with the introduction of the IoT intervention?	Is the IoT intervention technically equipped to accommodate the existing channels that are facilitating smooth service delivery to citizens across demographic and geographic diversities?
Has the intervention covered and serviced the intended purposes for citizens across targeted socio-economic groups, and agents, without any discrimination?	Has the IoT-intevention led to any change(s) in the service channels (such as exclusion of service channles enabled by last-mile operators)?	What are the technical resource additions/changes that have been/need to be implemented as part of the IoT intervention?
What are the human and technological resources (existing and new) that are in use/have been allotted for this IoT intervention?	Have you noticed any service delivery value additions or gaps since the introduction of the IoT intervention?	
With the introduction of new agents and technology components/players how is the accountability mapping done?	If so, what is the composition of citizens affected in terms demography and geography?	
Does the intervention help to achieve efficiency without comrpomising the quality of service?		

Fairness

LEGISLATIVE	EXECUTIVE	STANDARD SETTING
What mechanisms are available to ensure that the IoT-enabled system is transparent to the agents and citizens involved?	What channels does the existing system (without IoT) have to ensure transparency to the agents and citizens involved?	What technical measures are in place to ensure transparent and fair representation in data within the IoT-enabled system? (Technical agents will have to elaborate on the typology and choice of data, and means of data collection)
What mechanisms are available to ensure that the IoT-enabled system is explainable and comprehensible to the agents and citizens involved?	What changes in such channels are seen in the system with the introduction of the IoT intervention? (These channels should ensure that the system is transparent to the agents and citizens involved)	What technical measures are in place to ensure the comprehensibility of the IoT-enabled system and its functioning? (Technical agents will have to explain the functionality of the IoT-enabled system in a simple, clear and concise format/language)
What prescribed record-keeping and logging mechanisms are in place w.r.t the current system (without IoT intervention)?	What processes does the existing system (without IoT) have to ensure explainability to the agents and citizens involved?	What technical measures are in place to facilitate clear record-keeping and logging in order to ensure reviewability? (Technical agents will have to list out the processes to ensure concerned agents are answerable and that the system is reviewable)
What are the changes to the abovementioned record-keeping mechanisms with the introduction of the IoT intervention?	What changes in such processes are seen/expected in the system with the introduction of the IoT intervention? (These processes should ensure that the system is understandable and comprehensible to the agents and citizens involved)	What technical measures are in place to offer entry points for different agents to raise/address concerns within the abovementioned areas?
What other mechanisms need to be in place to ensure fairness in intent and conviction? (The decisioin-making agent has to assess if the intention and objective behind introducing the IoT intervention is unbiased and non-discriminatory)	What according to you are existing biases associated with the current system (without IoT)?	
What other mechanisms need to be in place to ensure fairness in outcomes of the IoT-enabled system? (The decisioin-making agent has to assess if the intended outcomes and consequences of the IoT intervention are unbiased and non-discriminatory)	What according to you are expected biases associated with the IoT-enabled system?	
	What are the channels and agents available to the citizens and agents to challenge abovementioned biases?	

Trust and Consent

LEGISLATIVE	EXECUTIVE	STANDARD SETTING
What according to you are existing privacy and security concerns in the current system (without IoT)?	What interactions (among those listed) involve the sharing or exchange of sensitive, personally identifiable information?	What technical measures are in place to ensure that agents have avenues to manage their data within the IoT-enabled system? (This includes processes that they need to know and data that they choose not to reveal)
What measures have been prescribed to ensure that privacy is maintained in every interaction in order for the IoT-enabled system to be trustworthy? (This includes interactions of all kinds that involves agents, citizens and devices in any capactity)	What according to you are the potential roadblocks in ensuring that privacy and security is upheld within the IoT-enabled system?	What technical measures are in place to ensure that agents have avenues to protect/safeguard their data within the IoT-enabled system? (This includes the data utilisation includes a right to withdraw if necessary)
What consent-seeking mechinisms support the IoT-intervention to safeguard privacy and instill trust in the IoT-enabled system?	What are the ways in which interoperability of data and functionalities unfold without compromising on privacy and security?	Are the consent management mechinisms technically comprehensible and meaningfully executed for the agents?
What measures have been prescribed to ensure that security is maintained in every interaction in order for the IoT-enabled system to be safe? (This includes interactions of all kinds that involves agents, citizens and devices in any capactity)	Are there any intermediate agents that bridge any potential trust gaps?	What technical measures are in place to offer channels for citizens and agents to raise accountability concerns?
What are the regulatory mechanisms in place to allow for agents and/or citizens to hold certain parties answerable? (These mechanisms must be mapped for every interaction amongst agents, citizens and devices).	How is the consent management made transparent and explainable to agents and citizens?	
What are the mechanisms available to agents and citizens to check whether those involved in an interaction(s) are in compliance with the prescribed regulatory policies?	What are the grievance redressal channels available to the agents and citizens? (Kindly include the processes that lie outside those listed)	
Are there adequate and appropriate forums to address accountability concerns raised by agents and citizens? (This forum must be external to the agents involved with the IoT-enabled service delivery system. The composition of this forum must have representation from relevant social groups and subject matter experts)	Are the agents: a) aware of their roles b)acknowledge their responsibilities c)understand what parties that they are accountable to	

Dignity of Life and Work

LEGISLATIVE	EXECUTIVE	STANDARD SETTING
Does the IoT-enabled system recognise the identity of all the agents/citizens involved? (Here identity refers to who they are in terms of gender, caste, disability, age etc. while also keeping in mind any changes to these over time)?	What are the current concerns regarding freedom of choice within the system (without IoT)?	In what ways are the current technical guidelines posing rigid boundaries for the agents and citizens to operate within? (These boundaries might impose certain courses of action on the agents and citizens, thereby compromising their dignity and autonomy)?
What prescribed conduct protocols are in place that agents need to adhere to in order to safeguard the respect of citizens? (Please mention any instructions or guides on behaviour of agents in the IoT system)?	Has the IoT intervention - resolved or - intensified or - had no effect on these freedom of choice concerns?	What kind of technical preparedness does the IoT-enabled system posess to address repeated service failure for a particular agent or citizen? (Here, failure means any denial of entitlements arising from technical processes. This denial undermines the agent's/citizen's identity and therefore dignity)
Does the IoT-enabled system give citizens the avenues to exercise freedom of choice (autonomy) in accessing their entitlements?	How are the tasks reallocated/delegated differently to existing agents with the introduction of the IoT intervention?	What additional technical skills are agents/citizens required to equip themselves with in order to navigate the IoT-enabled system?
In the event of technical issues/failure, are there agents (intermediaries) who will interact with citizens to ensure that they are treated and guided with respect?	What according to you are the reasons for this reallocation? (Kindly justify any significant changes in professional responsibilities that arise from the introduction of the IoT intervention)?	What technical measures are in place to ensure that appropriate authority (and the autonomy that comes with it) recogition and corresponding decision-making avenues are available to agents?
What are the prescribed workplace protocols that agents need to adhere to in order to safeguard the respect of other agents within the system? (Please mention any instructions or guides on professional behaviour of agents in the IoT system)?	Does the current system (without IoT) involve the surveillance of agents or citizens in any way?	What technical measures are in place to ensure that citizens can exercise autonomy while choosing channels for service delivery within the IoT-enabled system?
Does the IoT-enabled system give agents the avenues to exercise freedom of choice (autonomy) in carrying out their professional responsibilities within the IoT-enabled system?	Within these surveillance mechanisms, what are the existing concerns w.r.t. dignity and freedom of choice?	Are the agents provided with avenues to enhance their existing technical capabilities to work with dignity?
In the event of failure, does the system allow for alternate mechanisms to be devised dynamically by the agents without compromising on the dignity of the agent or citizen?	Does the IoT-intervention necessitate any additional surveillance of any agents or citizens?	
	What additional groups/sections of agents and/or citizens are being surveilled within the IoT-enabled system?	
	Within these surveillance mechanisms, what are the possible concerns w.r.t. dignity and freedom of choice for these groups?	

The Center for Internet of Ethical Things (CIET) was set up to foster research and innovation in the area of Internet of Things (IoT) technologies. The Center explicitly engages with ethical and moral aspects of technologies to ensure better progress towards the 2030 Sustainable Development Goals (SDGs) and to nurture a thriving innovation ecosystem in the area of IoTs within the State of Karnataka.

International
Institute of Information
Technology Bangalore

International Institute of Information Technology Bangalore

26/C, Opposite of Infosys gate 1
Electronics City Phase 1, Hosur Road
Bengaluru - 560100
Ph: 080-4444 7777