IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 30 May 2024, accepted 22 July 2024, date of publication 31 July 2024, date of current version 9 August 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3436048

RESEARCH ARTICLE

Defining and Modeling Forced Trust and Its Dependencies in Smart Environments

LAURI HALLA-AHO, JOUNI ISOAHO, AND SEPPO VIRTANEN, (Senior Member, IEEE)
Department of Computing, University of Turku, 20014 Turku, Finland
Corresponding author: Lauri Halla-aho (lauri.m.halla-aho@utu.fi)

ABSTRACT In this paper, the concept of forced trust in smart environments is defined. Consequently, a trust model for mapping trust dependencies within these environments is proposed to aid in early detection and mitigation of issues caused by forced trust. The model represents the trust relationships between parties with regard to data transfers occurring in smart environments. Using three example projects utilised in smart environments, the applicability of the model is demonstrated for identifying common risks experienced by citizens in such environments, including undisclosed data utilisation, mass surveillance, and regionally weak privacy and data protection laws. The proposed model is a basis for forming an overview of the trust landscape in information system and service-related projects. Additionally, it aids with analysing how the actions of these contributing parties could pose risks, for example, to the privacy or security of the data, and consequently propagate to the denizens of these environments.

INDEX TERMS Forced trust, smart environment, trust dependency, trust model.

I. INTRODUCTION

Smart cities are inherently reliant on data and several types of information systems and services that utilise them [1], [2], [3]. The chosen solutions, whether readily available commercial products or tailor-made for the city, are consequently utilised to optimise and enhance pre-existing functions or to introduce new, technology-enabled public utilities. Regardless of the methodology and approach to the implementation of these systems, members of these societies occasionally have no alternative to trusting the systems, as well as their operators, to be dependable. The compulsion of this trust is further emphasised under circumstances where the said citizens are negatively affected in their daily lives if they choose not to use these systems. This type of trust is called *forced trust*.

While the majority of the discussion in this paper is concerned with the public sector, citizens in an information society are also inevitably in a forced trust -relationship with multiple third parties in the private sector. These parties include device manufacturers and service providers as well as utility companies, for example for power or Internet access. In order to utilise the services provided by the city, the citizens must rely on them in their daily routines. Additionally, data collection and processing performed by said parties force the citizens to trust them to appropriately manage and use their information.

The trust terminology used in this paper is based on the definitions by the Oxford English Dictionary (OED) [4] and Marsh and Dibben [5]. In particular, the OED definitions 1a and 1c, that is "Firm belief in the reliability, truth, or ability of someone or something; confidence or faith in a person or thing, or in an attribute of a person or thing" and "to take on trust: to believe or accept a statement, story, etc., without seeking verification or evidence for it", respectively, are used. Henceforth, the terms *truster* and *trustee* are used for the source and recipient of trust, respectively. Additionally, Marsh and Dibben described positive trust as confidence in the trustee to have your best interests in mind, negative trust (distrust) as belief in a trustee to have negative intents; untrust as an insufficient amount of trust to base decisions on; and mistrust as misplaced or betrayed trust.

Taking these into consideration, it is vital for smart cities to minimise the amount of forced trust the citizens experience and ensure they feel the trust they give the city is earned. Mismanagement of public services, systems, and the personal

The associate editor coordinating the review of this manuscript and approving it for publication was Giacomo Fiumara.

data of citizens are bound to cause mistrust and distrust, as well as other subsequent negative effects discussed in detail later in this paper.

In this paper, we produce a definition for the concept of forced trust in the context of smart environments. Understanding the nature of this phenomenon and its effects on systems and services deployed in smart environments will aid in their adoption and further development by reducing user avoidance and resistance. Additionally, we examine the structure of trust relationships between various involved parties, such as service providers and governmental bodies, to identify how data utilisation can reflect as risks for the citizens. As such, the main contributions of this paper are the definition of the concept of forced trust, a proposed model for the trust dependencies between parties involved in smart environments for examining the effects of forced trust, and the validation of this model using applicable cases. The definitions of forced trust and smart environments, presented in sections II-D and III-A, respectively, are partially based on and extended from the first author's master's thesis [6].

The rest of this paper is organised as follows: the concept of forced trust is defined after a systematic literature review in section II, followed by a description of smart environments and their areas of interest in section III. The trust model is proposed and validated through three distinct example scenarios in section IV. This is followed by an analysis and discussion on forced trust and the results of the model validation in section V. Finally, the conclusions of this paper are provided in section VI.

II. SYSTEMATIC LITERATURE REVIEW

A systematic literature review is required for the later discussions on the effects of forced trust in the context of smart cities and their design. This review was carried out in September 2023 and it covers the results from seven different online databases: ACM Digital Library, arXiv, IEEE Xplore, ScienceDirect, Scopus, Springer Link, and Volter. To cover the articles as well as possible, each of the databases was queried with the exact search terms ''forced trust'', ''involuntary trust'', ''mandat* trust'', and ''compuls* trust''. The combined results were initially filtered based on their titles and the contents of their abstracts. Finally, duplicate results were removed to produce the remaining nine results. These stages and their respective counts for pieces of literature are shown in Figure 1. As can be seen from the number of results, this research subject, in the context of information societies, is novel, having emerged within the past decade.

In total, 286 matches were found for the search terms across the seven databases, subsequently filtered to 22 matches in fields relating to trust in the public sector or information systems. Finally, these were narrowed down to nine articles that discussed the topic beyond a cursory glance. Eight articles ([7], [8], [9], [10], [11], [12], [13], [14]) were found directly through the database searches and one, [15], via a footnote in [14]. While they all discuss the topic of

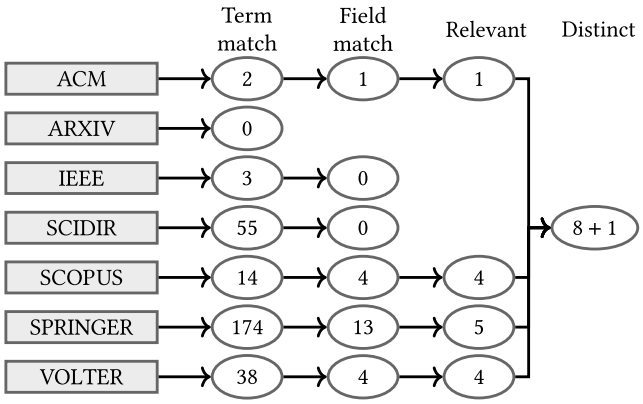

FIGURE 1. Result counts from each of the seven databases throughout the filtering process.

forced trust, these articles are divided into three distinct areas: forced trust in information societies [7], [8], [16] discussed in section II-A, software and systems [9], [10], [11], [12], [17] covered in section II-B, and the Soviet Union [13], [14], [15]. Albeit the forced trust experienced by the Soviet citizens is not strictly identical to the titular topic of this paper, it is analogous as shown in their coverage in section II-C. Finally, a definition for forced trust is given in II-D.

A. LITERATURE ON FORCED TRUST IN INFORMATION SOCIETIES

The literature search resulted in the works by Hakkala [7], as well as Hakkala et al. [8] that both discuss the effects of forced trust in information societies. Hakkala [7] describes forced trust as a ''situation in which a user is dictated to use and to trust an information system or an [Information and Communications Technology (ICT)] product''. Such a situation often applies with the services offered by the public sector, such as social services or healthcare. He also notes that the trust relationship is sometimes bi-directional, as ''the designer of the information system has to take into account the potential misbehavior of users'', highlighting the need for system designers to account for potential attack vectors and known vulnerabilities while still being in a forced trust relationship with their users.

A forced trust situation, as defined by Hakkala et al. [8], is one where ''an entity–whether a customer, an organization, or even a governmental agency–does not have a privilege to choose but is instead mandated to use a dictated information system''. The involuntary nature of such use can have a detrimental effect on the users' attitudes and behaviour, leading to partial use or even deliberate misuse. This places additional pressure on the system designers and developers to implement protections against malicious user actions, increasing the overall cost of the system.

Both texts, then, describe *acceptance*, *avoidance*, and *resistance* as the three outcome scenarios that follow from forced trust in information systems. By accepting the systems, the users decide to use them despite their

potential flaws. This decision could be based on e.g. trust earned from prior experiences with the system provider or operator, finding the identified risks too minor to be a deterrent against its use, or ignorance of issues in the design, implementation, or operation of the systems. In the second scenario, avoidance, some users lack trust in the proposed or implemented systems and do not fully utilise them or provide false information. Avoidance, then, leads to misuse or even disuse of these information systems. In extreme cases, the users can have malicious intent and attempt to, for example, sabotage or deny services. This type of behaviour is called resistance and can be detrimental for the operation of future development of the systems due to user interference.

B. LITERATURE ON FORCED TRUST IN SOFTWARE AND SYSTEMS

While the specific subjects of their articles vary, the articles by Madhisetty and Williams [9], [10], Kanakakis et al. [11], and Bimrah et al. [12] discuss forced trust in the context of software solutions or information systems and services.

Madhisetty and Williams [9], [10] discuss the trust users of social media have on the platforms when they publish their own content, such as images and videos. In particular, they focus on the confidence the users have in the service provider, defining four main characteristics of confidence: trust, control, risk, and uncertainty. All of these characteristics play a factor in forced trust, as ''[it] is experienced by participants who have no alternative but to trust that sharing their data as photos or videos will not violate their notion or expectations of privacy.'' [9], [10] As such, they classify forced trust as a consequence of the users' lack of control on the data they share.

Kanakakis et al. [11] describe forced trust as ''trust without trustworthiness evidence and with a possible presence of cautious feelings'' within their proposal for a trust model for estimating user trust levels when using online systems. They deem it to apply to the ''ambivalent'' user segment, the members of which are not capable of examining the trustworthiness of products or have ''a certain need to trust in order to avoid, or to lower the omnipresence of cautious and other negative feelings''. As a result, this user segment is likely to assess trustworthiness based on information and experiences available from their peers.

In their paper on a trust modelling language for information systems, Bimrah et al. [12] define forced trust as one of two levels of trust, the other being independent trust. They use an example of a bank employee interacting with a customer trying to invest their money. In this scenario, the trust between the customer and the employee, with the customer as the truster, is forced. They incorporate forms of trust like those of Marsh and Dibben's positive and negative trust in their *trusting intention* element. Their model can be used to describe the trust relationships between a smart city and its citizens, as discussed later in section IV.

C. LITERATURE ON FORCED TRUST IN SOVIET SOCIETY

The works discussing forced trust experienced by Soviet citizens are by Ledeneva [13], Tikhomirov [14], and Hosking [15]. Ledeneva [13] explores the concept of *krugovaya poruka*, collective responsibility, in the Soviet Union. This responsibility was applied on groups and communities, making the collective responsible for the misdeeds and misbehaviour of their individual members, but also benefited from their accomplishments. It functioned as a form of social pressure that kept the citizens disincentivised from acting against the state or the Communist Party. A consequence of krugovaya poruka was a forced trust among the populace, as trusting your peers to act as was expected of them became a necessity. Additionally, it was commonly weaponised by Soviet bureaucrats to keep themselves in power, even when their misdeeds were brought into light by a member of the society below them. Doubt would be cast onto the legitimacy of the claims by questioning the motives of the denouncer, using the threat of negative consequences from fallacious accusations as a deterrent to communities.

Tikhomirov [14] bases his discussion on the forced trust -concept introduced by Ledeneva and applies it to communications within the Soviet Union. The Communist Party cultivated an atmosphere of distrust within the society, encouraging citizens to turn in and denounce their neighbours and acquaintances, be it for suspicious behaviour or simply to gain the favour of the state. This especially promoted a forced trust -relationship between the Party and its subjects. Division of the populace into one's friends and foes enabled the formation of a personal relationship with the local and state leadership, allowing them to ''escape the oppressive feeling of distrust''. Additionally, retaining a good relationship with the Communist Party was vital for many to avoid labour camps and execution.

As Hosking [15] explains, the sociopolitical upheaval, through the abolishment and replacement of traditions and institutions, experienced in the Soviet Union resulted in an environment where scapegoats were needed to explain the lack of success of the new systems. In the 1920s and 1930s, the communications, for example the news and media, were heavily controlled by the party allowing them to mould the trust landscape of the people with an emphasis on the ''with us or against us''-mentality. Party leadership was presented as infallible and trustworthy. Potential enemies, regardless of their current stature or position, were met with distrust and were likely to face punishment. In these uncertain circumstances, the only option one had was to absolutely trust the Communist Party, and hope for reciprocated trust.

D. DEFINITION OF FORCED TRUST

In both previously discussed contexts, the term *forced trust* is applied in scenarios where a trusting party, in these cases the citizens, is forced through circumstance to trust another party, such as a public government or an information system or service. This trust, albeit effectively forced, can still be

perceived by the truster as earned. Nevertheless, once this trust is lost, e.g. the trust in the Soviet leaders or the public services provided by local governments, their daily lives are likely to be negatively affected in a noticeable way.

In digitalised societies, previously physically accessible public services are often fully replaced by electronic equivalents. These replacements are decided on, ordered, and operated by an applicable public authority or outsourced to a third party selected by the said authority. The citizens rarely have a say on their details and are thus forced to trust and use them or be unable to perform a task which had previously been accessible via physical means. Additionally, data-driven, or data-collecting, products produced by the private sector can become de facto systems and services utilised both by the public sector as well as individual citizens, forcing the data providers to trust each individual private entity not to misuse their access to personal data. In the Soviet society, on the other hand, the trustee was the reigning political party or its high-ranking representatives instead of an information system.

To summarise this literature review and provide a concrete reference to the following discussion on its effects on smart environments, such as smart cities, a definition for the concept of forced trust, in the scope of this paper, is provided below.

Definition 1 Forced trust: A situation where a truster is forced to trust a trustee, or services provided by a trustee, with minor to no opportunity or possibility to influence the function or behaviour of the target of trust, that is the trustee or the services. A truster can be seen to be in forced trust with a trustee if they are mandated to provide, or use services that utilise, personal data in order to prevent the quality or ease of their life from being negatively affected.

III. SMART ENVIRONMENTS

The concept of smart environments has emerged alongside that of smart cities as communities have developed and are developing towards increased connectivity and automation. As such, their definitions are nebulous, and often vary between sources. To find a suitable definition for smart environments, three definitions for smart cities, given by Deakin and Al Waer [18], Frost & Sullivan [19], and IEEE [20], are examined in section III-A. Then, in section III-B we define the beneficiaries of smart environments in the context of this paper.

A. DEFINITION OF A SMART ENVIRONMENT

Deakin and Al Waer make a distinction between a city simply utilising technologies in its operation, an intelligent city, and a smart city. They list four requirements a city should fulfil before claiming to be a smart city: wide utilisation of ICT, use of those technologies to transform life, embedding the previous ICT in the city, and bringing them and the people together to aid innovation, learning, knowledge, and problem solving [18]. Additional emphasis is placed on involving the citizens in the development of the city to take advantage of the social capital in the adoption of technologies.

Frost & Sullivan list eight parameters, a minimum of five of which are required for a city to possess to be considered a smart city. These parameters are smart governance and education, smart healthcare, smart building, smart mobility, smart infrastructure, smart technology, smart energy, and smart citizen. They also distinguish four types of market participants that shape these cities: integrators, network service providers, product vendors, and management service providers. [19]

Finally, the IEEE Smart Cities Community define six sectors that make a city smart: smart water, smart energy, smart mobility, smart health, smart food and agriculture, and smart waste [20]. Additionally, they specify five domains that enable the various applications in smart cities. These domains are sensors and intelligent devices, networks and cyber security, systems integration, intelligence and analytics, and management and control platforms [20].

Each of the above definitions involve ubiquitous use of smart technologies in the basic functions of the city, and the involvement of the citizens in their integration into the communities and systems. However, Frost & Sullivan's and IEEE's definitions specify explicit fields of application but do not establish recommended approaches for execution. On the other hand, Deakin and Al Waer's list is applicable to each of these fields but does not specify any of its own.

Based on the previous discussion, the definitions proposed by Frost & Sullivan [19] and IEEE [20] are succinct and can be combined to provide the following definition for smart environments, as an extension of smart cities, will be used for the rest of this paper.

Definition 2 Smart environment: A smart environment realises five or more of the following properties: smart governance, smart education, smart healthcare, smart construction, smart mobility, smart infrastructure, smart technology, smart utilities, smart citizen, smart waste, and smart agriculture.

B. SMART ENVIRONMENT BENEFICIARIES

The main focal points, and as such beneficiaries, of smart environments vary and depend on the specific use cases and demands of involved communities and circumstances but the properties specified in Definition 2 can be combined into four major categories that, while not guaranteed to cover all potential aspects, describe most of the important goals of smart societies. These foci are *smart citizenship*, *smart services*, *smart infrastructure*, and *smart architecture*, as shown in Figure 2.

Smart citizenship, as a category, covers properties related to enabling the citizens to participate in the smart environment, whether at home or in the open. Smart services, on the other hand, include all services provided for the citizens in smart environments. Additionally, Smart infrastructure comprises of the networks and services forming the backbone of the environments, such as transportation and utility networks. Finally, smart architecture includes the use cases

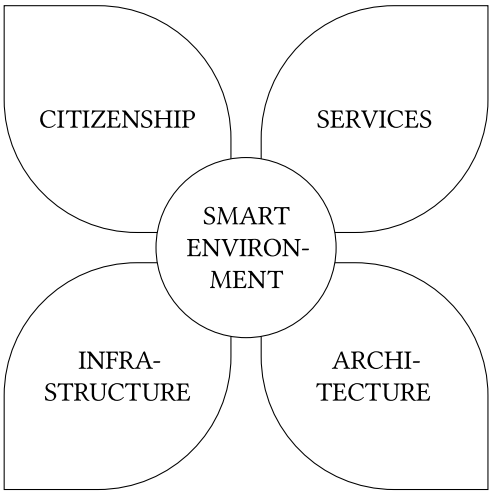

FIGURE 2. Common important focus points in the development of smart environments.

for smart technology within, for example, construction, industry, and agriculture to optimise and enhance their functions.

Digitalisation introduces an opportunity to improve citizen involvement in public decision-making. Digital platforms can be used to lower the participation threshold for people who, inter alia, are interested in local governance but have been previously unable to participate or have perceived their chances of affecting local decision-making via conventional methods insufficient. This can be achieved with online discussions and electronic advisory voting on topical subjects, as well as channels for providing feedback about the performance of their local government. Additionally, digitalisation enables opportunities for the local governance to be more transparent, for example via broadcast meetings.

Public services can benefit from the introduction of recent technologies, whether hardware- or software-based, by optimising their operation as well as expanding existing capabilities. Notable examples are advances in healthcare and education. Portable, light-weight cyber-physical devices enable increased mobility in patient monitoring, both inside and outside medical facilities. This mobility eases the lives of patients by allowing them to remain at home until direct medical attention is necessary. While this is also beneficial in centres of population, its benefits are highlighted in areas of low-density population. In the latter case, however, it is vital to ensure a sufficient medical infrastructure to compensate for longer distances to the nearest medical centres. More generally, advancement in small-scale medical devices and implantable medical-grade devices can be used to automate the dosage of medicine.

Among the primary benefits of digitalisation on education are its effects on the availability, accessibility, and interactivity of material, as well as improved capabilities to detect learning difficulties and provide early aid to pupils and students before these issues begin to harm their progress. Digitised teaching material can be easier distributed to the students, especially with the use of open access material, without the restrictions of physical media. Assistive technologies can also be used to improve the accessibility of digitised material. Additionally, technological solutions increase the diversity of methods and approaches to present topics and problems in challenging subjects to students. Finally, increased interactivity in education, for instance through gamification, can effectively increase students' interest and engagement.

Public infrastructure is another primary beneficiary of the development of smart environments and technologies. This includes, inter alia, utility, transportation, as well as communication networks. The production, distribution, and consumption of energy, whether heat or electricity, and water can be optimised with the use of smart meters and a smart delivery network. Using these technologies, smart load balancing enables a fast recovery from outages in the utility or communication networks as the smart network itself can reroute the flows to reduce the impact of the outage. This can also be applied to the smart transportation network, which can similarly redirect traffic whenever a section of a road is closed due to, for example, maintenance or an accident.

Architecture, whether public or private, can also be enhanced within a smart environment. Strain, wear, and other changes in the condition of buildings and structures can be measured, and consequently pre-emptive measures taken before permanent damage occurs. In buildings, smart devices could be used to, for example, prevent water damage or optimise heating. On the other hand, in structures such as bridges, sensors can be used to measure and detect deterioration of their integrity, increasing their longevity and reducing the need for large-scale maintenance if issues are detected sufficiently early.

IV. FORCED TRUST IN SMART ENVIRONMENTS

Public data utilisation, depending on its nature, can affect citizens both positively and negatively. As each distinct data processor accessing a given piece of data during its lifetime can pose a risk to the owner of the data, that is the citizen, it is important to map the participating parties involved in smart city projects. These risks can be exacerbated by the presence of forced trust, as described in Definition 1, as citizens wanting to retain their quality and ease of life cannot avoid participation. The mapping is performed for the trust relationships between relevant parties by modelling their dependencies in section IV-A. Additionally, this model is examined further through example cases covering potential scenarios in smart cities, discussed in section IV-B.

A. MODELLING TRUST DEPENDENCIES

The trust relationships between individual participants of smart cities form a complex network. To model this concept, these trust dependencies can be summarised as a network containing seven distinct major parties. An end-user, primarily a

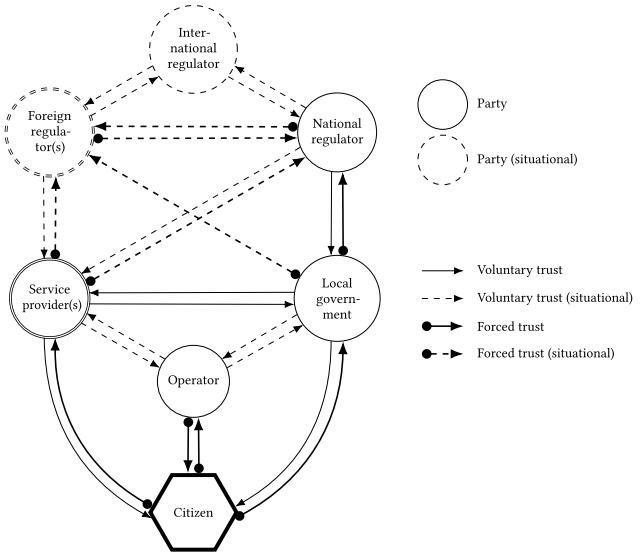

FIGURE 3. The Trust Dependency Model depicting relations between involved parties in the context of smart environments. Parties shown with dual borders can have multiple instances simultaneously, such as distinct service providers.

citizen, is a typical user of the smart systems and services comprising the smart environment. As such, their point of view on trust is the main concern of this paper. The citizens rely on the *local government* with the information systems or services (ISSs) they provide. The local government is the most immediate public authority to the end-users, and are responsible for the planning, implementation, and operation of the locally operated public ISSs. This process can be performed via the use of internal or external *service providers* that provide the hardware and software required. The *operators*, and consequently administrators, of the ISSs can be directly employed by the public authorities or an external service provider. An operator can be a specialised end-user of a governmental system, such as a healthcare or social worker utilising the systems, in addition to those responsible for running them. Additionally, the citizens are likely to have to use nation-wide ISSs, for example to interact with social services. The local government is also dependent on the actions of the *national*, *foreign*, and *international regulators* due to data-related national and international laws. They can notably affect details related to, inter alia, data processing and storage if end-user data are transmitted internationally. The *Trust Dependency Model (TDM)*, shown in Figure 3, covers the *citizenship* and *services* focal points shown in Figure 2 and further accounts for the nature of the relationships between distinct entities.

In the figure, parties denoted with solid circles are always present and those with dashed borders participate in some situations. For example, if a foreign service provider is utilised, their respective regulator would be included in the graph whereas with a domestic service provider it would be unnecessary. Additionally, parties with dual borders can include multiple distinct parties.

In the model, there are four distinct types of trust relationships that can exist between two parties. The two binary variables for each relationship are the truster's willingness for participation, that is voluntary or forced; and the universal applicability of the relationship, that is always present or situational depending on external circumstances. A voluntary trust relationship is freely formed without external influence. If one or more of the parties lack an alternative to trusting another, the trust relationship is forced. On the other hand, some relationships depend on, among others, the location of operation for the parties. These trust relationships are not always present but arise based on applicable situations. For example, a foreign service provider forces the local government to also trust the foreign regulator, as the service provider operates under their authority.

At the highest level of the trust "hierarchy", the international regulators and lawmakers, such as the European Union, define the extents to which individual nation states and companies can collect and process data. These regulators, both international and national, share a mutual trust as they partake in the planning, development, and lobbying of the transnational regulations. However, nations are in forced trust with each other as they rely on their peers to comply with the agreed-upon international regulations. Similarly, local governments such as municipalities and cities are, to an extent, forced to trust their national regulator to create an environment favourable for developing and implementing smart environments, while enjoying the regulators' voluntary trust.

The local governments are responsible for the public ISSs that are introduced to transform towns and cities into smart cities. As such, they are in a trust relationship with the chosen service providers, their respective regulators if foreign, the operators and administrators of the ISSs, and the end-users, that is their citizens. The service providers, often outsourced due to cost-effectiveness, are expected to deliver their products as required by the government, and to comply with applicable privacy and data protection regulations when the processing of citizen data is required. As a direct consequence, the government can be forced to trust a foreign regulator if a non-domestic service provider is chosen. In these situations, the service provider would also be forced to trust the local national regulator.

Conflicts may arise regarding the extent of data collection and processing between this network, that is government, regulators, and service provider, if the parties have significant differences in their valuation of, for example, privacy protection. A privacy-conscious city, for instance, might want to avoid invasive data collection as a side effect caused by the operation of the smart city. They could be forced by the national, or foreign, regulator to collect more personal data than they want, to comply with the applicable laws or national interests. In such cases, the city must rely on the enforcing party to abstain from breaching the privacy rights of the owners of the data.

Service providers are responsible for appropriate storage and handling of personal information relevant to their operation. They are also responsible for minimising the collected data to what are strictly necessary. Akin to the cities, the service providers can be forced by states to perform invasive data collection. It can also be in the interests of the company to profile their users if they supply the city with a sufficiently comprehensive, or a sizeable number of, ISSs. Potential cases of data misuse include collection of personally identifiable information from users without their consent or awareness, mismanagement, sharing or selling the information to third parties, and failure to store the data confidentially and securely. These cases should be against the goals and intentions of the developing smart cities and their inhabitants, and as such the trust relationships between the service providers and the regulators are mutual forced trusts.

The operators of the city-commissioned ISSs commissioned by the city can be employed by either the service providers or the cities themselves, depending on whether they are operated locally under the supervision of the government, or remotely by the service providers. This group includes, in addition to the system administrators, anyone with access to the stored personal data. As a direct result, the end-users are forced to trust the operators with whatever personal data they must contribute to utilise the ISSs. Simultaneously, the operators must remain aware of users that misuse the systems, for example maliciously or as a form of avoidance. Finally, the citizens rely on their local governments to implement the smart city in a manner that benefits its people in the least invasive manner available.

Unlike other parties, citizens are inevitably in a forced trust -relationship with all other participants. This is emphasised notably by the inability for the users to fully understand the intricacies and details of ISS implementations due to, for example, a low amount of openly available information. As such the end-users are forced to trust entire systems based on limited knowledge [16], [17].

B. SCENARIOS

To further explore the trust dependencies shown in Figure 3, three scenarios and their dependency maps are considered. They are considered from the point of view of a citizen of a developing smart city. In Scenario I the local government is utilising a foreign service provider and operator. Scenario II considers a situation where a smart city has chosen a domestic service provider while directly employing an operator themselves. Finally, Scenario III discusses a city planning to utilise a combination of national and international service providers.

Each of the covered cases is handled as follows. Initially, the participatory parties are identified and their roles are assigned according to their tasks and responsibilities described in the case. The potential set of roles are the nodes shown in Figure 3. The next step is to determine the connections, and the respective trust relationships, between each participant. These relationships are additionally classified as either voluntary or forced, depending on their nature. Finally, risks each of the participants are subjected to because of the forced trust relationships are addressed, and their reflections on the citizens are explored.

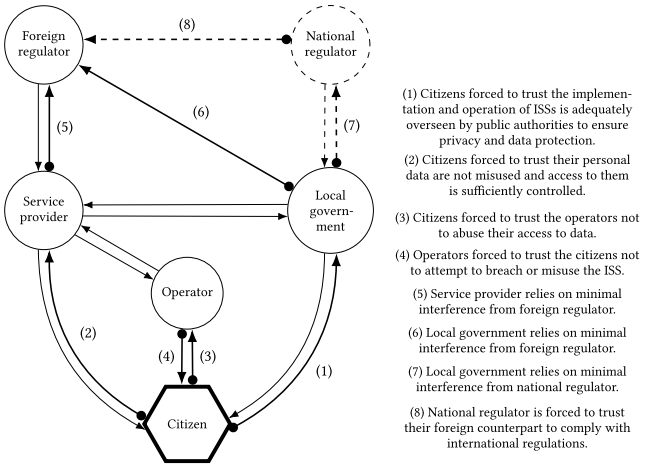

FIGURE 4. Scenario I: The city utilises foreign cloud storage and processing services for collected data.

1) SCENARIO I: FOREIGN CLOUD SERVICE PROVIDER AND OPERATOR

The first scenario concerns a situation where a local governmental body has chosen to utilise a foreign service provider to implement and operate an ISS for a public service. This naturally introduces limitations to the range of use cases allowed while ensuring sufficient data and privacy protection for the data owners. In addition to these participants, the citizens are in a direct forced trust relationship with the administrators, and potential end-users, of the systems. By providing their data to a third party, potentially operating under looser data protection regulations, the citizens are subjected to risks related to the misuse of their data, for example by the service provider or a foreign national agency. This situation is shown below in Figure 4.

Simultaneously, the citizens rely on their local government to sufficiently monitor the design and development, where possible, as well as operation of the systems and services they delegate to external companies or organisations. However, being unable to affect the applicable foreign regulators, the local government and the service provider are forced to trust them to minimally interfere with the requirements and operation of such systems. Processing citizens' personal data abroad would otherwise expose them to increased risks of their information being misused to the benefit of, e.g., foreign states.

The local government, as well as the service provider, is reliant on regulations affecting the operation of the selected service provider, set by the foreign state. The local government must either actively search for a service provider from a country known for suitable laws related to privacy and data security, among others, or attempt to minimise

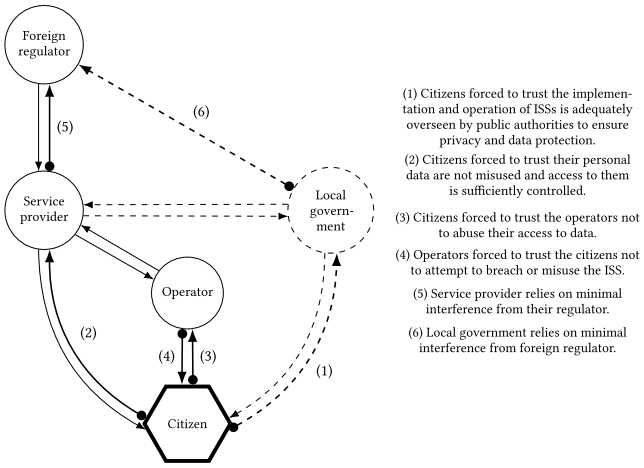

FIGURE 5. Case I: Smart home surveillance cameras.

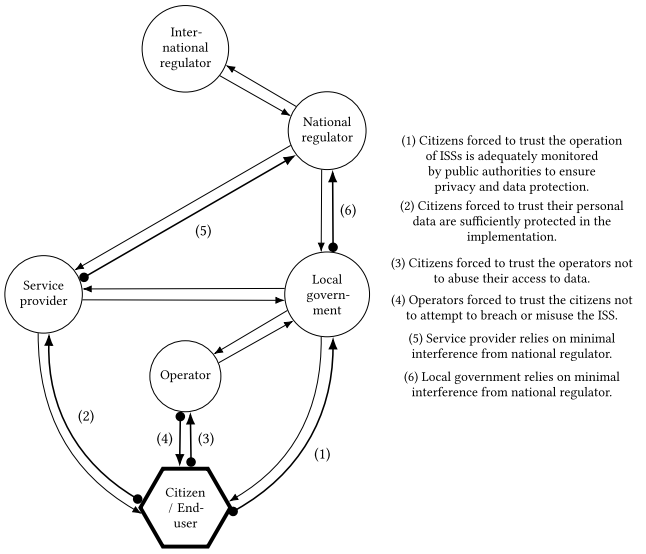

FIGURE 6. Scenario II: A domestic service provider with an operator employed by the local government.

potential risks the citizens will be exposed to. Additionally, the national regulator can occasionally partake in the project and is then similarly forced to trust the foreign regulators to follow international data utilisation regulations.

An exemplary case of this scenario is the use of smart home surveillance cameras to monitor and protect private property. Unless situated within the country of origin of the surveillance system manufacturer, the citizen is likely to have to agree for their data to be sent abroad for processing and storage. If insufficiently configured, either by the manufacturer or the homeowner, such systems can even expose the live feeds of the cameras to the Internet due to insufficient access control. The trust landscape for this case is shown in Figure 5.

Citizens interested in protecting their homes with smart home surveillance, or IP cameras, are likely to have to store their security footage on servers located across state borders to be able to fully utilise the systems they have acquired. As such, the service provider, also acting as the operator of their own services, has full access to such data. The citizen is then forced to trust the service provider to respect their rights to privacy, as well as of the passers-by recorded by the cameras facing public areas. Additionally, they are directly affected by any invasive laws the service provider operates under, such as sharing footage with law enforcement without notice.

In cases, the local government is directly participating in the adoption of smart home surveillance, for example through security recommendations or a public ISS aiming to utilise the IP camera network in co-operation with the service provider. They then have a responsibility to provide the citizens guidance about major available options and their benefits and disadvantages.

Insufficiently protected or misused smart home surveillance data can expose individual homes, as well as neighbourhoods, to involuntary third-party surveillance. IP cameras open to the public can also expose their owners to potential home invaders by allowing those with enough technical knowledge to map out neighbourhoods and discover when homeowners leave for extended periods of time. Additionally, storing the surveillance records, as well as any other type of personal data, abroad opens the data owners up to increased privacy risks. These risks grow in severity, for example, with the invasiveness of the intelligence services of said states and can as such lead to unauthorised use of security footage.

2) SCENARIO II: DOMESTIC SERVICE PROVIDER AND LOCAL OPERATOR

In an example case of the second scenario, a model of which is shown in Figure 6, the city orders a bespoke ISS for local or regional use in the field of smart healthcare. The system could be used to introduce new functions or services in the city, or to replace older implementations. Due to the domestic nature of the participants, the trust network is notably simplified. As in Scenario I, the citizens are in a forced trust relationship with the service provider and the local government, including the operator. However, as both the data production and consumption are performed domestically, the potential for personal data misuse allowed by laxer privacy laws or regulations is significantly lower compared to the first scenario. Additionally, since the ISS is operated by the local government, the strength of the forced trust between the citizens and the service providers is weakened, as their ability to negatively affect the citizens is limited to the given system requirements and implementation details. It should also be noted that while there exists a forced trust -relationship, citizens do not directly interface with the service provider in practice but experience this trust indirectly through the healthcare services.

When considering a healthcare ISS, the utilised data are inherently personal and sensitive. As such, it is the responsibility of the local government, operator, and the service provider to ensure the management of confidentiality, integrity, and access (CIA) to patient data are appropriately

incorporated into the design of the system and its daily usage routines. A direct consequence of this is the potential for increased complexity of the ISS, reducing its usability for the end-users, that is medical staff. As the citizens are forced to trust their medical information is securely and confidentially input, stored, and, when necessary, shared with authorised personnel, and the medical staff are forced to trust the ISS implementation not to make their routines slower or more difficult, the staff, as end-users, can also be seen to be in a forced trust relationship with the service providers.

The effects of this compounding forced trust can be notably observed, for example, whenever a new ISS is found to contain a lacklustre implementation of the CIA or to reduce work efficiency by slowing down regular routines. A practical example of these issues can be found in the development and deployment of the Apotti patient record system in the Helsinki metropolitan area, Finland [21], [22]. The system reportedly limited the number of personnel able to access a given patient's record to one while simultaneously allowing unlawful access to such data to unrelated members of the staff. Additionally, its usability issues slowed their workflow down by 20–30 %, when compared to the previous system, significantly reducing the amount of time available to care for patients.

The local government and the service provider are in mutual trust during the development and deployment of the ISS. They both operate in an environment defined by the regulations and decrees set by the national regulator, which can affect the potential for utilised systems. Such effects can be either positive or negative from the point of view of the citizen, as the state could require the ISSs to be stricter in protecting their right to privacy and thus restricting the types and use cases of data that can be collected. Alternatively, the state could mandate the service provider to further infringe these rights by forcing the implementation to gather additional information or share personal information with third parties.

A representative example of this type of a scenario is the i-voting, or Internet voting, system utilised in Estonia with elections. The system imitates the behaviour of letter voting by encrypting the votes with an election-specific public key to form an inner envelope and signing the vote with the voter's personal identification card. The organiser is responsible for distributing the tasks of vote collecting and processing to the various systems and, holding the decryption key for the votes, tallies anonymised votes. The trust dependency of this case is shown in Figure 7.

In this case, the citizen is strongly dependent on each of the other parties: the state, the service provider, and the organiser. The state sets the requirements for the security, confidentiality, and reliability, inter alia, of the votes handled by the utilised systems, and is responsible for ensuring these requirements are met. The service provider, on the other hand, is responsible for securely and reliably implementing the voter identification, vote encryption and signature processes, vote anonymisation, as well as tallying. Finally, the organiser

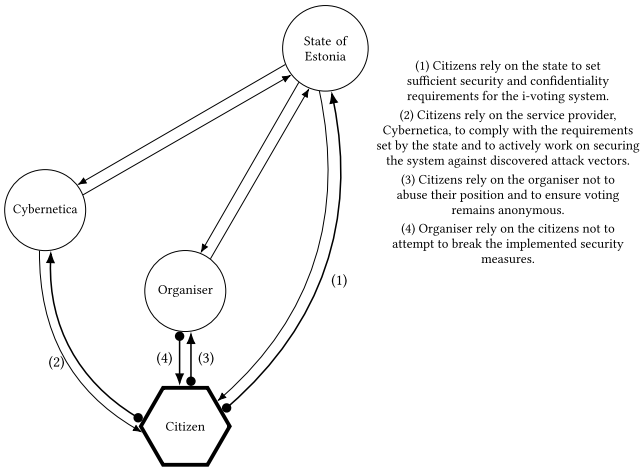

FIGURE 7. Case II: Estonian i-voting with a system provided by Cybernetica.

has direct access to the votes, both as the operator of the system and the tallier of votes, and thus the voters are forced to trust them to properly handle the votes. The responsibilities combined must be fulfilled by their respective parties for i-voting to be a viable alternative to conventional voting alternatives, as by its nature it is susceptible to attacks across the Internet.

One of the design goals of the Cybernetica i-voting system is to allow the voters to vote multiple times, retaining only the last vote. This effectively protects the voters against potential attempts at coercion. A coerced voter can later vote for their intended candidate, negating the effects of coercion assuming it does not occur at the end of the voting period. [23]

As a crucial part of functional democracy, the secrecy and integrity of voting must be well-protected especially with voting over the Internet. An i-voting system requires strong voter identification both to protect the rights of the voters and to prevent the insertion of falsified votes. Unforeseen issues or flaws in the design or implementation can allow attackers to compromise the integrity of the vote, an example of which was demonstrated by Pereira [23]. In the said attack, a compromised voting application could be used to, unknown to the voter, replace their vote after deliberately crashing following their original vote. Unaware of the success of the vote, the voter would proceed to vote again, albeit with an altered vote. After successfully voting with the replaced vote, the voter is shown the receipt for the first vote.

Such a compromise of the integrity of the vote is severely detrimental to the voter, especially if the i-voting system is used to replace conventional means of voting. Under such circumstances, the voter has no choice but to either trust the system or not participate in the election.

3) SCENARIO III: MULTIPLE SERVICE PROVIDERS OF DIFFERENT NATIONALITIES, SERVICE PROVIDER ACTS AS AN OPERATOR

Often the systems and services utilised in smart environments themselves rely, directly or indirectly, on other systems or

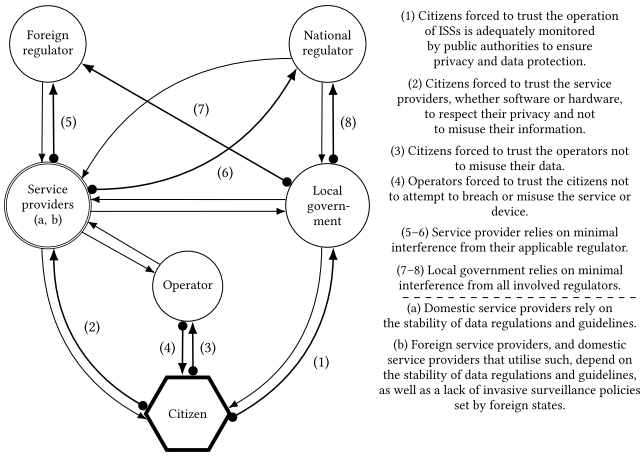

FIGURE 8. Scenario III: Several service providers, both domestic and foreign, utilised or endorsed by public authorities.

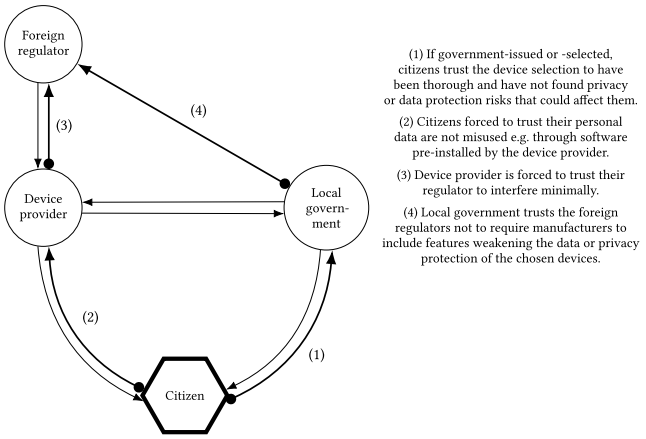

FIGURE 9. Case III-A: Foreign device provider.

services supplied by other providers. In these situations, there can be interdependencies, and thus trust relationships, between some of the chosen service providers; the local government could choose to, inter alia, use the software of one independent provider on hardware from another, or use a service provider which itself builds its products on another provider's platform. Such a situation could be further complicated through the utilisation of service providers of different nationalities. This naturally complicates the overall trust dependencies of affected smart environments or cities, as shown in Figure 8.

The trust relationships the citizens are in vary based on the types of service providers used. Assuming both devices and applications are used in combination, some of which sourced domestically and others abroad, the citizens' data are potentially transmitted across multiple state borders. Nevertheless, as in the prior scenarios, they depend on the public authorities to select reliable platforms and services to be integrated into the public ISSs. Similarly, any service providers and operators with access to the citizens' data, whether through services or software embedded on the utilised hardware, are expected to respect the citizens' data rights. However, due to the internationality of the scenario, related protections can be weaker than the data owners expect.

Service providers are, naturally, forced to trust their respective regulators and, through the suppliers they utilise, any additional foreign regulators. As such, providers willing to minimise personal data usage could still be obligated to gather additional information as a requirement for operation. Information about these circumstances should be made publicly available either by the service providers or the responsible public authorities.

As an example case, consider a city aiming to homogenise their services under a singular system. To simplify payments, for example for public transit or services, they choose a domestically developed electronic payment service. However, this service also requires a device to be run on, such as a smart phone or a public terminal. Alas, these devices are only produced internationally, and thus must be imported. The city is then dependent on both nationally and internationally sourced service providers, independently from each other. The trust dependencies for both service providers are shown below in Figure 9 and Figure 10.

In a situation as the one shown in Figure 9, internationally sourced devices can range from smaller personal devices or items to larger computers or terminals used to interface with the software-based service. The severity of the risks faced by their users varies with, for example, the service type and the frequency of use of these devices. Whether they are publicly distributed or chosen, or certain brands or models of smart devices are recommended for the citizens to personally acquire, the local government has the responsibility to guarantee they are not known to be susceptible to contemporary attacks.

The device providers have control over the hardware and software the devices contain and come pre-installed with, and as such the citizens rely on them not to knowingly include or enable excessive data collection, for example through in-built back doors. Such vulnerabilities could occur incidentally or due to compliance with national regulations. The latter would be an example of a negative consequence of the device provider's forced trust towards their applicable regulator. Similarly, the citizens' local government, if they have distributed the chosen devices, can be seen to be responsible for any present privacy and data protection risks they failed to identify beforehand. However, the overall risks the end-users are exposed to due to the utilised hardware can be expected to be minor.

On the other hand, the range of potential use cases and purposes for software and the increased complexity in the trust landscape, as shown above in Figure 10, are large enough to allow for more severe risks to personal data. In the case of payment information, both the service provider and the operator have access to the citizens' payment methods in addition to other personally identifiable information. As such,

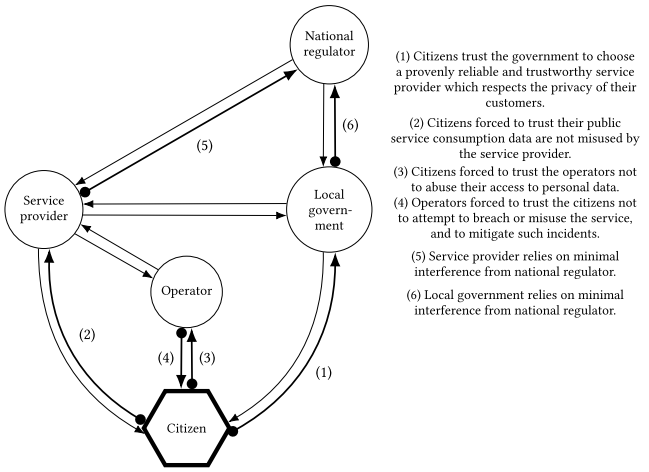

FIGURE 10. Case III-B: Domestic service provider.

it is important for the issuing government to check the background of the chosen service provider to ensure they have not been previously found to have mismanaged or compromised their security or customer data. Additionally, the chosen service provider, covering the public services of the entire city, could further monetise the consumption data collected from their users such as by selling them to advertisers. Such practices should be accounted for while choosing the provider for the unified payment interface to minimise privacy risks for the citizens. Simultaneously, given the large coverage of services the service provider, as an operator, is responsible for, they are also a potential target for malicious users.

As a domestic service provider, they, together with the responsible local government, rely on the stability and predictability of the regulatory environment with regards to financial services and public service consumer data. Notably, restrictions and limitations on their use for product development and revenue are affected by requirements and obligations set for companies handling such data.

V. ANALYSIS AND DISCUSSION

The phenomenon of forced trust, previously identified and discussed in-depth by Hakkala et al. [7], [8] and defined in section III-A, can have detrimental effects within smart environments if left uncontrolled. Their strength depends on the severity of the negative impact a citizen would experience were they to avoid or refuse to utilise services, especially those provided or commissioned by the public sector. Pre-emptively avoiding circumstances that would lead to a noticeable portion of denizens preferring avoidance or resistance to participating in the environment is advantageous to the sustainability of the development of smart cities. Defining the phenomenon of forced trust clearly and exhaustively is then crucial in being able to analyse and mitigate its effects on public ISS projects that do not allow the citizens to avoid their use. To be able to effectively perform this type of process, the Trust Dependency Model was proposed.

As the dependency of people living within increasingly digitising environments on smart information systems and services, both in the public and private sectors, increases and the availability of alternatives diminishes, the importance of utilising trustworthy service providers is highlighted. When their users do not have a choice but to provide their personal data to third parties, they are forced to trust these service providers. As such, a thorough overview of the parties participating in or affecting the design, implementation, and operation of such services should be formed. This overview can then be used to gain insight into the direct and indirect effects this trust can have on the citizens, and consequently for mitigating its negative impact.

The Trust Dependency Model, displayed in Figure 3, focuses on the major parties involved in public information system projects. In particular, the parties immediately involved are of interest, namely the local government, service provider, operator, and any relevant national regulators. Utilising the model to map out trust relationships between the citizens and their immediate trust subjects, and further the trust relationships of these participants, will enable us to more effectively detect potential data-related risks that could eventually affect citizens. This mapping of risks for each involved party consequently helps in trying to minimise the likelihood and severity of citizens being negatively affected, for instance, by data leaks and misuses further down the line. Additionally, by recursively identifying all applicable parties data are transferred to, the model is apt for identifying underlying citizen-facing risks in ISS projects in a wider variety of use cases in addition to mapping forced trust. Extending the model by incorporating risk analysis and management into it could provide a useful tool for evaluating the impact forced trusts between parties have on smart environments and cities.

The most common risks experienced by citizens in the scenarios discussed previously include undisclosed collection or utilisation of personal data, mass surveillance [24], and weak applicable privacy and data protection laws when utilising international services. In this context, undisclosed collection and processing of data include both cases where the data owners are not informed of their performance and where the information is difficult to find within another lengthy, verbose document. In certain cases, especially with i-voting and smart surveillance, the effects on citizens can vary from slight to significant based on the severity of the breach of privacy and confidentiality. With the former, voter anonymity is crucial to guarantee a free and equal election. The party implementing the required systems, then, has the responsibility to ensure the voters cannot be identified by an adversary with the information collected, despite any potential external pressure to introduce vulnerabilities. In the case of surveillance, for example in relation to smart homes and neighbourhoods, the privacy of citizens living in or passing through the area can be jeopardised were the surveillance data to leak or the surveillance systems to be breached. Additionally, widespread forms of data collection,

such as those in smart environments, expose the data owners to data breach risks [25], the severity of which depends on the type of data collected.

Whether the utilised services are domestic or foreign of origin, the risk of mass surveillance will remain present throughout the lifetime of a smart environment, regardless of it existing during its planning and implementation phases. Additionally, advances in smart surveillance, such as subject identification using collected data [26], techniques significantly increase the significance of privacy risks. These risks could manifest themselves either directly, e.g., the service performing data processing or profiling not required by its operation on their users' personal data and sharing the information with interested state authorities, or indirectly, for example by implementing backdoors into the systems responsible for data collection or processing. The surveillance, depending on its type and openness, can potentially cause a chilling effect on the citizens due to the ubiquitous nature of the data collection in affected environments. Finally, utilising services that store collected data abroad in states or countries with weaker privacy or data protection legislature increases the risks experienced by the citizens providing their data.

It is important to only utilise service providers found to operate reliably, both in terms of continuity of service and how they treat and utilise data, to minimise the frequencies of service interruptions as well as data-related risks for the citizens. However, attention should be paid to avoid circumstances where any single company accrues a practical monopoly over the services utilised by the city as their sole provider. This enables them to potentially design their systems to exclude future services from other providers from being able to interact with the pre-existing solutions. Simultaneously, reliance on a singular service provider, regardless of their perceived reliability, strengthens the forced trust in them experienced by the citizens.

VI. CONCLUSION

In this paper, we studied and defined the concept of forced trust in the context of smart environments. As a part of the definition process, we conducted a systematic literature review across seven online databases with the search terms ''forced trust'', ''involuntary trust'', ''mandat* trust'', and ''compuls* trust''. The literature review revealed that the concept is not sufficiently defined or covered in existing literature. Utilising our definition, we proposed a trust model for mapping the trust relationships between parties involved in data transfers for projects related to smart environments, such as smart cities. This model was consequently validated with three example cases and scenarios, which were used to identify common risks for citizens providing their personal information to systems and services operating in such environments.

The forced trust -phenomenon occurs in smart environments whenever the utilisation of the systems and services cannot be avoided by the citizens without suffering negative impacts on the quality or ease of their daily lives. Examples of such situations include public services transferring from physical to electronic and online services, and the utilisation of products or services from private service providers becoming de facto solutions within given environments or communities. This definition was reached after a thorough review of existing literature on the concept of forced trust in the contexts of information societies, software and systems, as well as in the former Soviet society, and forms the basis for future research into the subject.

The model is suitable for mapping and visualising trust relationships, which occur within smart environment -related projects and implementations as data are transferred between participants. It is especially beneficial in determining the effects and consequences of these data transfers on the citizens acting as the source of the data of interest, personal data in particular. As they provide their data to the directly adjacent parties, they lose all control over the forms of future utilisation of their information. As such, the model is apt for examining the cascading effects the forms of distant data utilisation propagate onto the citizens. This was shown through three distinct example scenarios of systems and services used in smart environments and cities.

The proposed model could further be extended with analysis and management of the risks identified while analysing the effects of forced trust between the parties. Together, with risk detection and mapping, the model could be used to mitigate the severity of forced trust experienced by citizens, as well as the risks they are subjected to when providing their personal information pre-emptively during the development phase of smart environments. This extension remains a topic for future research.

REFERENCES

[1] V. Kostakos, T. Ojala, and T. Juntunen, ''Traffic in the smart city: Exploring city-wide sensing for traffic control center augmentation,'' *IEEE Internet Comput.*, vol. 17, no. 6, pp. 22–29, Nov. 2013.

[2] L. Calderoni, D. Maio, and S. Rovis, ''Deploying a network of smart cameras for traffic monitoring on a 'city kernel,''' *Expert Syst. Appl.*, vol. 41, no. 2, pp. 502–507, Feb. 2014.

[3] R. Verma, ''Smart city healthcare cyber physical system: Characteristics, technologies and challenges,'' *Wireless Pers. Commun.*, vol. 122, no. 2, pp. 1413–1433, Jan. 2022.

[4] Oxford English Dictionary and Oxford University Press. (2015). *Trust*. Accessed: Sep. 13, 2022. [Online]. Available: https://oed.com/view/Entry/207004

[5] S. Marsh and M. R. Dibben, ''Trust, untrust, distrust and mistrust—An exploration of the dark(er) side,'' in *Trust Management* (Lecture Notes in Computer Science), vol. 3477. Berlin, Germany: Springer, 2005, pp. 17–33.

[6] L. Halla-aho, ''On the effects of forced trust on implementations of small smart cities,'' M.S. thesis, Dept. Future Technol., Univ. Turku, Turku, Finland, 2020. [Online]. Available: https://urn.fi/URN:NBN:fi-fe202003259254

[7] A. Hakkala, ''On security and privacy for networked information society: Observations and solutions for security engineering and trust building in advanced societal processes,'' Ph.D. dissertation, Dept. Future Technol., Univ. Turku, Turku, Finland, 2017. [Online]. Available: https://urn.fi/URN:ISBN:978-952-12-3607-5

[8] A. Hakkala, O. I. Heimo, S. Hyrynsalmi, and K. K. Kimppa, ''Security, privacy'); drop table users;–And forced trust in the information age? When trusting an information system is not optional and why it matters,'' *ACM SIGCAS Comput. Soc.*, vol. 47, no. 4, pp. 68–80, Jul. 2018.

[9] S. Madhisetty and M.-A. Williams, "The role of trust and control in managing privacy when photos and videos are stored or shared," in *Proc. Future Technol. Conf. (FTC)*, in Advances in Intelligent Systems and Computing. Vancouver, BC, Canada: Springer, 2018, vol. 881, no. 2, pp. 127–140.
[10] S. Madhisetty and M.-A. Williams, "Managing privacy through key performance indicators when photos and videos are shared via social media," in *Intelligent Computing* (Advances in Intelligent Systems and Computing), vol. 857. London, U.K.: Springer, 2019, pp. 1103–1117.
[11] M. Kanakakis, S. van der Graaf, C. Kalogiros, and W. Vanobberghen, "Computing trust levels based on user's personality and observed system trustworthiness," in *Trust and Trustworthy Computing* (Lecture Notes in Computer Science), vol. 9229. Heraklion, Greece: Springer, 2015, pp. 71–87.
[12] K. K. Bimrah, H. Mouratidis, and D. Preston, "A language for modelling trust in information systems," in *Information Systems Development*. Boston, MA, USA: Springer, 2009, pp. 599–608.
[13] A. Ledeneva, "The genealogy of krugovaya poruka: Forced trust as a feature of Russian political culture," in *Trust and Democratic Transition in Post-Communist Europe*. Oxford, British Academy, 2004, ch. 5, pp. 85–108.
[14] A. Tikhomirov, "The regime of forced trust: Making and breaking emotional bonds between people and state in Soviet Russia, 1917–1941," *Slavonic East Eur. Rev.*, vol. 91, no. 1, pp. 78–118, 1917.
[15] G. Hosking, "Trust and distrust in the USSR: An overview," *Slavonic East Eur. Rev.*, vol. 91, no. 1, pp. 1–25, 2013.
[16] M. M. Rantanen and J. Koskinen, "Respecting the individuals of data economy ecosystems," in *Well-Being in the Information Society. Fruits of Respect* (Communications in Computer and Information Science), vol. 1270. Turku, Finland: Springer, 2020, pp. 185–196.
[17] P. D. Chowdhury, B. Christianson, and J. Malcolm, "Anonymous authentication," in *Security Protocols* (Lecture Notes in Computer Science), vol. 3957. Berlin, Germany: Springer, 2006, pp. 299–305.
[18] M. Deakin and H. Al Waer, "From intelligent to smart cities," *Intell. Buildings Int.*, vol. 3, no. 3, pp. 133–139, Jul. 2011.
[19] S. Singh. (2014). *Smart Cities—A $1.5 Trillion Market Opportunity*. Forbes. Accessed: May 30, 2024. [Online]. Available: https://www.forbes.com/sites/sarwantsingh/2014/06/19/smart-cities-a-1-5-trillion-market-opportunity/#2feab3f86053
[20] IEEE Smart Cities. (2017). *What Makes a City Smart?* Accessed: May 30, 2024. [Online]. Available: https://smartcities.ieee.org/images/files/pdf/IEEE_Smart_Cities-_Flyer_Nov_2017.pdf
[21] T. Kuukkanen. (2019). *Kolmen Lääkärin Tyly Arvio 600 Miljoonan Euron Jättijärjestelmästä: Edelleen Täysin Keskeneräinen, Ei Pitäisi Laajentaa Muualle*. Yle. Accessed: May 30, 2024. [Online]. Available: https://yle.fi/a/3-10700107
[22] P. Kosonen, and S. Hirvonen. (2019). *HS: Apotti-Järjestelmästä on Paljastunut Potilaiden Tietosuojan Vaarantava Ongelma*. Accessed: May 30, 2024. [Online]. Available: https://yle.fi/a/3-10891042
[23] O. Pereira, "Individual verifiability and revoting in the Estonian internet voting system," in *Financial Cryptography and Data Security. FC 2022 International Workshops*. The Lime, Grenada: Springer, 2022, pp. 315–324.
[24] G. Galdon-Clavell, "(Not so) smart cities? The drivers, impact and risks of surveillance-enabled smart environments," *Sci. Public Policy*, vol. 40, no. 6, pp. 717–723, Dec. 2013.
[25] M. Aslam, M. A. K. Abbasi, T. Khalid, R. U. Shan, S. Ullah, T. Ahmad, S. Saeed, D. A. Alabbad, and R. Ahmad, "Getting smarter about smart cities: Improving data security and privacy through compliance," *Sensors*, vol. 22, no. 23, p. 9338, Nov. 2022.
[26] M. Maqsood, S. Yasmin, S. Gillani, M. Bukhari, S. Rho, and S.-S. Yeo, "An efficient deep learning-assisted person re-identification solution for intelligent video surveillance in smart cities," *Frontiers Comput. Sci.*, vol. 17, no. 4, Aug. 2023, Art. no. 174329.

LAURI HALLA-AHO received the M.Sc. (Tech.) degree in information security and cryptography from the University of Turku, Finland, in 2020, where he is currently pursuing the Ph.D. degree with the Department of Computing. His research interests include software and communication security, trust in information systems, and privacy protection.

JOUNI ISOAHO has been a Professor of communication systems with the University of Turku, Finland, since 1999. His research interests include the security of autonomous systems and AI, human and societal cyber security, and communication-intensive smart technologies.

SEPPO VIRTANEN (Senior Member, IEEE) is currently a Professor of cyber security engineering with the University of Turku, Finland. His research interests include cyber security in communication and network technology, especially in contexts of smart environments and AI applications.