Next Generation Smart Built Environments: The Fusion of Empathy, Privacy and Ethics

Denis Gračanin
Department of Computer Science
Virginia Tech
Blacksburg, VA, USA
gracanin@vt.edu

Ramoni O. Lasisi, Mohamed Azab, Mohamed Eltoweissy
Department of Computer and Information Sciences
Virginia Military Institute
Lexington, VA, USA
{lasisiro, azabmm, eltoweissymy}@vmi.edu

***Abstract*—Smart Built Environments (SBEs) and similar cyber-physical environments utilizing the Internet of Things (IoT) have been a growing research area in recent years. Contemporary research primarily addresses technology aspects, while human aspects, such as empathy, privacy and ethics (EPE for short), in relation to SBEs have not yet received adequate attention. In addition to challenges with respect to technology, there are apparent tensions and conflicting requirements involving EPE. On the other hand, opportunities exist for these aspects to support one another. For example, data collected and analyzed for empathic response may be used to alert the privacy-preserving subsystem. An ethical response may turn out to be the most empathic. The main objective of this paper is to present our vision for next generation SBEs and to explore pertinent EPE factors. We propose a unified framework that incorporates a game theoretic model to address EPE interplay in SBEs. Integral to our framework, we also introduce the use of a blockchain infrastructure for the critical need to support data integrity in such data-intensive environments. We illustrate our work in progress using an example. We then present major research challenges for the realization of next generation SBEs with fused EPE.**

***Index Terms*—Smart built environments, Internet of Things, human-centric computing, empathy, privacy, ethics, game theory, blockchains.**

I. Introduction

A primary goal of the Internet of Things (IoT) and related monitoring, analysis and interventions technologies is to support the enhancement of our Quality of Living (QoL). IoT integrates physical and digital worlds to support new services that can benefit from connecting everyday objects (things) and their users (people and other things) via the Internet. The IoT architecture and corresponding implementations differ from the traditional network architecture [1], [2]. IoT implementations usually comprise a large number of heterogeneous devices, with highly varied capabilities and life-spans. IoT devices have to be connected forming a resilient infrastructure in spite of the fragility of many of their components. Additionally, IoT devices are used in different contexts and domains, such as smart homes (appliances and sensors), health and fitness (wearable devices), and manufacturing (Industry 4.0 [3]). They may also be deployed in harsh environments, for example inside a turbine engine, tiny environments, for example inside the human body, as well as large urban environments, for example “smart cities”.

A Cyber-Physical System (CPS) relies heavily on IoT since CPS consists of and interacts with many devices with embedded software. These devices could be integrated in various infrastructure, logistics, and production systems. For example, a CPS directly records and process sensors data, controls actuators, interacts with other CPSs as well as with both physical and digital worlds, etc.

Smart Built Environments (SBE), as a subset of CPS, incorporate connected, interactive smart objects with sensing and actuating capabilities in living spaces. SBEs utilize various sensors that can be leveraged by integration and alignment of sensor data streams with longitudinal qualitative data from self-reported (administered on mobile computer platforms) surveys, questionnaire and other artifacts to identify activities with the goal of minimizing the required data footprint (both environmental and physiological). Such systems can also have mobile and re-configurable components, such as walls and furniture pieces [4], [5].

SBEs provide multiple heterogeneous data streams characterized across many dimensions. That includes human in/outside the loop, centralized versus distributed versus federated control, single domain versus cross domain, governance and jurisdiction, closed versus open, and level of integration. Figure 1 shows SBE’s data flow. Through information fusion from smart meters, smartphones, and specialized sensors (e.g., electromagnetic interference (EMI) sensors or inexpensive occupancy sensors), it has been shown that SBEs’ occupants’ Activities of Daily Living (ADL) and their energy impacts (e.g., switching on/off a particular appliance) can now be construed. In light of the fact that residential and social environments are diversely heterogeneous, the data collection incorporates and adapts multiple data collection solutions, inducing trade-offs among cost, ease of deployment, and back-end complexities.

The environmental data (provided by wearable sensors and IoT-instrumented physical environment) inform about the physical world surrounding the subject (or subjects). Physiological data, from basic ones such as temperature, heart rate or electrodermal activity (EDA) to complex, multi-channel electroencephalogram (EEG) data, provide an insight into the cognitive state, including stress, affect and activity. Cognitive data, provided as a direct input from the subject or gathered

978-1-7281-6739-8/19/$31.00 ©2019 IEEE
DOI 10.1109/TPS-ISA48467.2019.00041

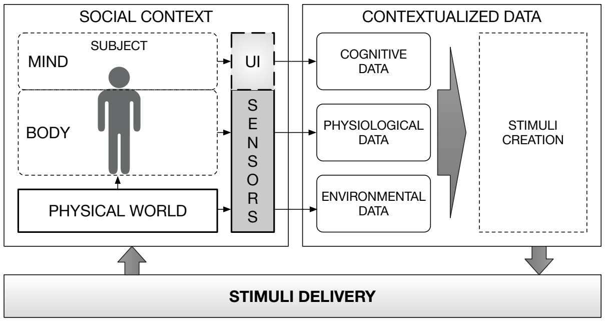

Fig. 1. Alignment of sensor data streams (environmental and physiological) with longitudinal qualitative data from self-reported surveys, questionnaire and other artifacts to identify human activities and cognitive state.

indirectly from social media (e.g., Facebook or Twitter posts) provide information about mood or emotional/mental state. The data has to be collected from a variety of wearable, mobile and embedded devices and correlated with social media posts and activities (including social interactions) in the physical world.

An important problem is collecting, processing, and managing heterogeneous and geographically distributed user and device data related to objects, actions and interactions, both static (built environments, outdoor places) and mobile (vehicles, train) that could also be human controlled or autonomous. Collaborative systems that take advantage of combined data and interactions can reduce spatial, functional and cognitive seams to support better quality of experience and more resident-friendly SBEs.

Technological advances, changes in manufacturing and economic factors result in new approaches to how products and services are identified, developed, produced, distributed, and maintained. The advances in communication and transportation technologies allow us to provide access to services that would otherwise require leaving the SBE. In addition to health, shopping (e.g., delivery using drones) and education (online and distance learning) services could be incorporated within SBEs.

For SBEs to realize their potential, numerous challenges must be addressed. These include asymmetric and seam-full interactions, multi-domain modeling and theories, interoperability, system management, dependability, and security. We discuss some major research challenges in Section IV, while we focus on empathy, privacy and ethics in the next two sections.

II. Empathy, Privacy and Ethics in SBEs

SBE programmers, engineers and technologists consider how the products and services they create Empathy is programmed in SBEs by developers to create products that can improve human well-being [6]. An intelligent SBE can learn to provide services in different ways according to the environmental, social, situational, and user-specific contexts. Context-aware intelligent SBEs can be conceptualized as living spaces embedded with computational intelligence, providing empathy and companionship in our daily lives while cognitively disappearing from our lives, thus becoming "empathic SBEs." However, as a side effect, they might introduce serious privacy and ethical concerns because of interactions between technology and information in domestic settings [7].

Privacy is a universal process [8] that is supported by government policies and laws. It is essential to protect the *confidentiality* and *privacy* of the user's data, both in physical and digital worlds [9]. While SBEs can provide personalized services [10], consumers must be willing to provide access to their personal information. However, even people familiar with IoT are not always aware of privacy risk involved [10]. On the other hand, when it comes to healthcare services, people are not willing to provide personal information since perceived privacy risk is high, although the personal information is neede to provide better service.

The main issue here is that data is like a bullet once it is fired there is no coming back. Once a piece of data is revealed it is out of the SBE's control to manage who is going to have access to it. The main challenge is how we can enable long term assurances for the SBE inhabitants' privacy while enabling the needed access to the data for the SBE to function effectively. For example, artificial intelligence and deep learning approaches can be used to analyze network traffic packets and demonstrate how user privacy can be exploited in SBEs [11]. Even though data in the packets are encrypted, combining and analyzing data transmitted from multiple devices could reveal patterns used to predict the type and time of activities of daily living (ADLs) SBE residents may be engaging in.

Ethics explore what makes one's conduct and actions right and what makes it wrong [12]. Normative ethics creates a set of rules that govern conduct and actions relating to the consequences of actions (consequentialism), the actions themselves (deontology), and the inherent character of an individual (virtue ethics). Applied ethics deals with real-life situations and can be used in creating public policy. For example, in the case of the United States Declaration of Independence [13], while there is a continuous debate about these statements and conclusions drawn from them, the declaration is the foundation for ethics of American political and social democracy. Services and transactions within the SBE should maintain ethical considerations both explicit and implied within the specific contexts.

Computer ethics [14] and information ethics [15] explore ethical issues distinctive to an information society due to the impact of technology on society. The ethical issues are, therefore, present in the development and use of SBEs [16], from the perspective of SBE designers to social factors such as social isolation and equity of access. Similarly, there are ethical considerations from the perspective of the residents' caregivers, including health personnel and social workers [17].

There is a conflict (especially in the SBE context) in using big data at the intersection of privacy and ethical requirements and the demand of innovative empathic uses of the data [18].

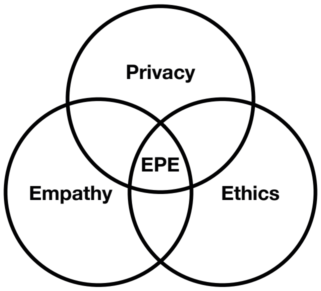

Fig. 2. Empathy, privacy, and ethics (EPE).

This conflict can be explored in the regulatory and social policy context, economic and business context, and technology and design context [18]. The findings can inform better design and control. There are trade-offs with regard to empathy, privacy and ethics in relation to the dynamics in the living environment [7], [19] and the overall performance of the SBEs within that environment. Therefore, we need to investigate how empathy, privacy, and ethics (EPE) affect QoL and develop suitable frameworks for agile management (Figure 2).

III. Towards Next Generation SBEs - with fused EPE

The next generation SBEs must go beyond enhanced control and communication capabilities. When designing such SBEs we need to use a holistic approach that takes into account the residents' interactions with both physical and digital worlds in the context of the SBE data flow (Figure 1). The physical world is a IoT-enabled architectural space with physical constraints and requirements framing ADLs. The digital world is conglomerate of services, such social networks, entertainment, assisted living, education, convenience, etc.

Designing SBEs presents many challenges. One extreme leads to a SBE that is "patronizing" towards its residents and decides for them about the best ways to live in the SBE. Another extreme leads to an SBE that is "detached" and requires its residents to micro-manage daily life in the SBE. Somewhere in between these two extremes is a "sweet spot" where residents feel comfortable and in control without undue burden of control.

This sweet spot is not static. It can change daily or seasonally, as well as evolve over time to adjust to evolving residents' needs and preferences. In order to anticipate and adjust to those variations and changes, an SBE must be able to understand its residents and "share" their feelings. Since the SBE can have more than one resident, the SBE must take into account social and group dynamics among its residents. In short, the next generation SBEs must be empathic. they must serve the residents' needs of privacy and adhere to ethical conducts.

Figure 3 shows our envisioned framework for the next generation empathic SBEs with the fusion of EPE. An empathic SBE combines data from physical world and digital world to identify context for the resident's activities and understand the resident's cognitive and emotional states. These longitudinal observations are stored in data repository and used to develop model(s) of the residents' interactions with SBEs. The developed model serves as a foundation for evaluation of the policy effects possibly using simulation of what-if scenarios. The policy sets the empathy, privacy and ethics requirements to protect the residents' data, including the information about their cognitive and emotional states. However, the ethics requirements included in the policy may overrule the privacy and/or empathic requirements. The evaluation results then serve as basis for prediction, decision and control of empathic SBEs. The interplay of empathy, privacy and ethics shape the evolution of the SBE and its services.

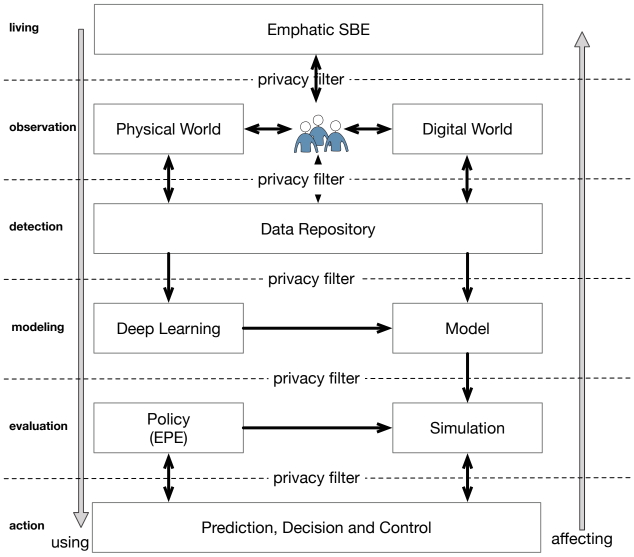

Fig. 3. A unified framework that integrates support for EPE within a IoT-based infrastructure for empathic SBEs.

A. Illustrative Example

The developed countries have increasingly aging population due to increased life expectancy. The consequences are increased healthcare costs and reduced availability of healthcare workers. Therefore, there is an urgent need to understand challenges and opportunities related to healthy and independent living, aging in place and overall quality of life [20], [21]. The developing countries are showing similar trends [22].

Effective tele-health services [23]–[27] can be continuously deployed, e.g., tracking vital signs in the elderly [28] and can benefit from data analytics and other techniques [29]. However, tele-health must address ethics issues [6], [30] and privacy requirements. Related regulations include Health Insurance Portability and Accountability Act of 1996 (HIPAA) [31] and General Data Protection Regulation (GDPR) [32]. For example, HIPAA states "*A major goal of the Privacy Rule is to assure that individuals' health information is properly protected while allowing the flow of health information needed to provide and promote high quality healthcare and to protect the public's health and well being.*" [31].

An important tele-health trend is the deployment of virtual care centers (VCCs) as "*the centralized command center that orchestrates and delivers exceptional patient care*" [33], [34]. The VCC operations scale well since a single VCC can support a large number of people. VCCs provide *Home Health Care* (HHC) by using personalized interventions and coaching (using health behavior models) with remote monitoring. This approach seems to be most successful [35].

SBEs are well suited to support VCCs operations such as emotional wellness and remote monitoring in SBEs [36], [37] thus reducing the need for healthcare facilities. Furthermore, user interfaces and devices deployed in SBEs can be personalized and customized based on health situation and needs [38].

VCC often leverage smart home technology to monitor patients. Smart home examples can include a single residence, a building or a series of assisted living residences and buildings. The common theme is a highly sensed environment that can identify and record ADLs and daily patterns of behavior. That introduces specific privacy and ethical issues that involves residents and caregivers [17].

Significant research currently being undertaken is focusing on the extraction of ADLs from such data, and cases where unhealthy behaviors are found are used to guide interventions. There is a number of academic smart house projects related to aging-in-place that utilize a network of wired and wireless sensors to measure vital signs and track residents and their activities [39]–[41].

Standardization efforts related to tele-health and health informatics [42], [43] have also include privacy related issues [44]. An important aspect of this research are privacy issues [45], [46] in the context of health data [46], domestic environments [47], [48], local community [49], [50] and online collaboration [51].

The right to privacy has long been advocated and promoted [52], [53]. Privacy-aware software development [54] and the role of privacy in computing and online systems was recognized early on in many applications domains, such as mobile computing [55], e-commerce [56], and child protection [57].

Computer and information security [58] has a strong impact on patient safety which is one of the main concerns of healthcare organizations. Knowing privacy risks [59] in the context of IoT-based infrastructures is essential [60] and may depend on regional differences (e.g. between HIPAA and GDPR) [61]. The goal is to ensure the security of patients' healthcare data, realize access control for normal and emergency scenarios, and support smart de-duplication to save the storage space in big data storage system [62].

B. Game Theoretic Model for EPE in SBEs

Game-theoretic techniques are prevalent in analyzing effects of strategic behaviors and interactions among entities in today's CPS [63]–[67]. These interactions are modeled as games between players, such as an attacker and a system's administrator. There appears to be some understanding of players' interactions in CPS using various game-theoretic tools [68].

An example of application of game theory models to IoT systems is smart transportation [69]. The purpose is identify new privacy related threats (e.g., drivers tracking and profiling). Adaptive and context-aware privacy protection solutions are need to address these threats while dealing with the environmental and resource constraints (e.g., memory, energy, communication channel). A game theory model between two actors (data holder and data requester) can find an equilibrium point reaching a compromise between privacy concessions and incentive motivation [69].

Similar extensions to understand strategic interactions among the several actors in SBEs can be made. We employ a game theory model namely, *Qualitative Coalitional Game* (QCG) [70], to explore the EPE interplay in SBEs.

Following the example above, we define a SBE in a HHC domain and define k different types of actors (i.e., agents) in the domain. For example in the HHC domain, we may have three types of agents, namely, *patients*, *caregivers*, and *visitors*. SBEs are built with certain goal(s) in mind. Let $G = \{g_1, \dots g_m\}$ be the set of these possible goals. Furthermore, we assume that agents in a SBE have the capability to exercise *ethic*, *empathic* and *privacy-preserving* behaviors depending on the current goals of their SBE. All goals in the domain are defined to balance the effects of ethics (i.e., maximize adherence to norms or code of conduct), empathy (i.e., maximize the ability to share others' feelings), and privacy-preserving (i.e., maximize protection) behaviors.

Let $A = \{1, \dots, n\}$ be a set of n agents in the SBE consisting of the k types of agents. Let $G_i \subseteq G$ be a set of goals for each agent $i \in A$. G_i is the set of rational outcomes (i.e., goals) that agent i cares about. The agent would be happy if some or all of its goals are satisfied. We assume that the SBE goal is made up of all the goals of the agents it contains, i.e., $G = \cup_i G_i$.

Suppose the overall goal of the SBE is to provide the best healthcare services given good ethics, empathy, and privacy-preserving behaviors by the agents. To achieve this goal, agents in the SBE may need to form coalitions (i.e., subsets) of agents that include appropriate number of agents' types who are able to bring about the SBE goals. For example, a coalition of agents consisting of only caregivers and visitors in the HHC domain without patients will not satisfy the goal of the SBE.

Thus for any coalition $S \subseteq A$ of agents, the coalition's value $v(S)$ is $v(S) \subseteq G$, i.e., the set of possible goals that satisfy all members of S. This interpretation of this version of the QCG game leads to the characteristic function for the game (Equation 1).

$$v : 2^A \to 2^G \tag{1}$$

The goals of coalition S is not satisfied when $v(S)$ is empty or when S does not contain appropriate types of agents. This thus leads to the following research question:*How can*

TABLE I
CHARACTERISTIC FUNCTION OF THE QCG GAME.

S	$\emptyset$	$\{C\}$	$\{P\}$	$\{V\}$	$\{C,P\}$	$\{C,V\}$	$\{P,V\}$	$\{C,P,V\}$
$v(S)$	$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$	$\{r,s,t\}$	$\emptyset$	$\emptyset$	$\{r,s,t\}$

we come about a balance of appropriate number of agents' types in coalitions that may achieve SBEs goals in different domains?

Consider the following example that illustrate the QCG model described above. Charlie (C), Peter (P), and Oscar (O) are three types of players in a HHC domain. Let C be a caregiver, P, a patient, and O, a visitor. Let a SBE be interested in achieving at least any two goals from r, s, and t, which must include goals of the patient and caregiver. Agent C has preference for goal t, agent P has preference for goals r and s, while agent O preference is for goal s.

We can model this SBE problem as a QCG game as follows: agents $A = \{C, P, V\}$, SBE goal, $G = \{r, s, t\}$, agent C goal, $G_C = \{t\}$, agent P goal, $G_P = \{r, s\}$, and agent O goal, $G_O = \{s\}$. The characteristic function of the game that determines the set of possible goals that can be satisfied by each coalition is given in Table I.

For this game to work, we need to have the appropriate tools to enable players to exchange control rights over the data. The main challenge here is in enabling leakage-resilient access to the data. Given the recent advances in blockchains, we believe that it can be very helpful as an infrastructure to hold the data and to enable transparent, leakage-resistant processing in a full distributed and balanced manner.

C. Blockchain Infrastructure for Integrity and Privacy in SBEs

Blockchain is a distributed secure ledger that organizes a list of transactions or data pieces into a long unbreakable chain of blocks [71]. Integrity is enforced using cryptographic and hashing techniques, and verified by a transparent distributed process using a decentralized consensus procedure.

The chain blocks are glued concretely using a cryptographic linkage technique where the hash value of the previous blocks are embedded into the next block waiving any chance of adding unverified blocks to the chain. The management process is totally decentralized in a consensus based technique enforced by the network.

The process controls who is authorized to add transactions, how the transactions are processed, and the read protocol for secure verification of the blockchain. That ensures that once a transaction is verified and added to the chain it cannot be altered or compromised retrospectively. The data integrity of each block is assured. The aforementioned features of the such technology makes it the perfect fit for the game infrastructure.

Blockchains can be the place holder for the data and the SBE agent transactions over this data. Further, it can be used as an enforcement mechanism for policies and procedures. A unique feature about blockchains is that it comes with an intrinsic *pseudonymity* by design that can be used in preserving privacy agent [72]. Pseudonymity refers to a state of disguised identity where users' real identity is a random hash of public keys in the network. The participants use their public key hash (pseudo-identity) to interact with the system without revealing actual identity. One user can have multiple pseudo-identities. The system can generate as many key pairs (multiple addresses) as they want to ensure that the user identity will be kept safe. However, that might not be very effective against inference or *unlinkability*.

Unlinkability refers to the failure to correlate transactions with some pre-knowledge about the actual user with high confidence in an attempt to reveal his/her true identity. If the user uses one pseudo-identity then it will not be hard for attackers to launch a de-anonymization inference attack, that links the user transactions together to uncover his/her true identity For that, SBE's infrastructure should enable the use of multiple pseudonymous identities without losing the ability for the system and authorized agents to correlate these identities together.

Our aim is that by enabling pseudonymous transactions while ensuring unlinkability and the help of regulated access to the data through smart contracts, blockchains can enable users to access the data without losing control on the empathy, privacy and ethics balance. However, technical challenges remain. Unlinkability should be assured by design while successfully integrating the blockchains into SBEs for instant access to the distributed data ledger with all smart operations intrinsically embedded within the chain for the agents to use in a fully trustworthy manner.

IV. Research Challenges

In this section we discuss ten major research challenges, in no specific order, for the next generation of SBEs. Our primary focus is on SBEs as enablers of ADLs and comfortable living in support of QoL while maintaining healthy social fabric.

Conflicting requirements and tension for EPE:

As stated earlier, more detailed and broad information leads to better empathic actions and responses. This is usually in contradiction with preserving privacy. How to achieve the "right balance"? Is it possible to maximize empathy while maintaining high levels of privacy? How do ethics factor in this mix? What would be the extent of human involvement and how? What constitute privacy violations in accordance to regulations and the modern and future use of SBEs?

Lack of comprehensive end-to-end standards, security and management platforms:

At the time of writing this paper, we know of no end-to-end standards guiding SBE development especially on issues of EPE. Such lack of standards make it difficult to design and build systems and management platforms for mass production and various scales. With the vastly diverse user requirements, technologies that are in early stages of development and use, predominantly outdated infrastructure systems, there is a need for new reference architectures and systems for extensible, re-configurable and scalable management platforms with end-to-end security and standards.

Limited data collections and measurement devices and tools, metrics and baseline data:

There is a need to collect bid data sets and synthesize baseline datasets. There is also a need to derive suitable metrics to express the EPE interplay. Research is also needed on the design and construction of complex and noisy data filters, models and tools. It is usually expensive to build physical prototypes of meaningful SBEs for experimentation. Also fitting current environments with adequate SBE gear is a daunting task. Mixed reality environments are showing promise.

Visible seams:

Contemporary SBEs do not adequately address the problem of visible seams, including spatial, temporal, cognitive, cultural, technological, etc. The success of empathic SBEs relies on the disappearance or at least the reduction of such visible seams. How could we integrate and weave together multi-dimensional contexts for a (near) natural feel and experience? How can we build management platforms where human-human, Human-machine and machine-machine interactions and relationships can be intuitively established and effectively maintained across seams? How can we provide end-to-end interactions that are“virtually” seamless while preserving personalized preferences? How to resolve fragmented security across seams?

Social Deficit Multiplier:

SBEs are being used by one or more individuals. Multiple users are likely to introduce contradictions is EPE requirements and also in their conditions and preferences. The gap between the desired system environment and the actual one is likely to increase. The management of EPE is such context has many challenges. How to monitor and collect data for multiple users with conflicting requirements? How to reduce the impact of contradictions while satisfying personal preferences? How to evolve the EPE management in a dynamic environment with ephemeral participation?

Lack of understanding of SBE participants and their ethical and cultural issues:

What are the spectrum of issues that concern SBE participants as individuals and groups? What constitutes SBE ethics? How to formulate policy for highly autonomic and autonomous environments with ethical and cultural considerations? How to manage and make decisions autonomously when different ethics frameworks co-exist and both human and machine make decisions? What ethical code should govern machine to machine interactions, particularly when EPE is at play? Should autonomous things make decisions based on crowd ethics or historical patterns, and how?

SBEs as building blocks for Smart Society:

The rise of IoT and Smart Cities provide opportunities for more efficient management and utilization of the available resources. How to use SBEs as building blocks for Smart Cities? How to integrate SBEs with the supporting utilities infrastructure?

Blockchain and data integrity:

Relying on pseudoanonymity to preserve privacy is not enough for SBEs. Given the recent advances in machine learning , linking pseudo IDs with real identities would be easy. Enabling transparent, distributed and privacy friendly processing of data is a major challenge. we Believe that the use of elaborate techniques such as zero-knowledge proofs and homomorphic encryption might present a responsible solution to such challenge. However, these technologies are very restricted and complicated [73]. In this case the question would be, will it be possible to integrate such complicated techniques in an application like SBEs seamlessly without any impact on its operation, or enabled features?

Impact on law, policy and government:

Privacy requirements (e.g., HIPAA, GDPR) and ethics [6], [30] need to be taken into account when supporting empathy. Similar issues are being addressed for self-driving cars and similar autonomous systems. If empathy enables us to get an insight into SBE's inhabitant mental state, how to use it in accordance with the law? For example, if suicidal tendencies are detected based on the longitudinal SBE's data, is it acceptable to violate privacy laws and inform health services?

Game theory model:

We have demonstrated a possible interplay among EPE in SBEs using the QCG model. The model proposes a possible way to balance the tension among EPE by requiring the selection of appropriate number of agents in coalitions that are formed to meet the overall SBEs goal. Since a naïve representation of the values of the coalitions is exponential in the number, n, of agents, and in our case, as well as the type, k, of agents in the game. The question then arises of how to represent or encode this version of the QCG game as input to a program? Furthermore, are there other more appropriate game models, possibly non-cooperative games, that better explore EPE interplay in SBEs than the cooperative QCG model we have used here?

V. Conclusion

In this paper, we explored the fusion of EPE issues pertaining to SBEs. We presented a framework and game-theoretic model for addressing the relationships that may be in conflict or support of one another. We also discussed important research challenges that need to be resolved for our vision to be realized in practice. Moving forward, researchers and developers of SBEs need to consider the evolution of such environments over the next 10 to 20 years and develop thoughtful solutions for the fusion of EPE in SBEs. We must also develop better understanding of the impact on the workforce and the relationships among people living in small communities to those living in a globalized setting [74].

It is not clear how we can exploit existing social capital and SBEs, particularly in small communities for the benefit of these largely decaying communities. It is also not clear how to transform the retraining spectrum; jobs in the future will require higher skill sets. The retooling programs of today will indeed fall short. Developing, building, using and maintaining next generation SBEs require workforce modernization. Globalization and technological advances have changed the demand for production workers and the nature of production jobs. Information technology continues to transform our society. Consequently, advances in automation, robotics, artificial intelligence, and machine learning require new models of human engagement [75]. Research and serious effort need to be dedicated to incorporate these new and advanced concepts into STEM and workforce education and training the gap is widening and the threat of a perceived "useless class" is real!

References

[1] D. Miorandi, S. Sicari, F. D. Pellegrini, and I. Chlamtac, "Internet of things: Vision, applications and research challenges," *Ad Hoc Networks*, vol. 10, no. 7, pp. 1497–1516, Sep. 2012.

[2] —, "Disruptive civil technologies: Six technologies with potential impacts on us interests out to 2025," SRI Consulting, National Intelligence Council (NIC), Tech. Rep. CR 2008-07, Apr. 2008.

[3] V. Alcácer and V. Cruz-Machado, "Scanning the industry 4.0: A literature review on technologies for manufacturing systems," *Engineering Science and Technology, an International Journal*, vol. 22, no. 3, pp. 899–919, 2019.

[4] D. Gračanin, M. Eltoweissy, L. Cheng, and R. Tasooji, "Reconfigurable spaces and places in smart built environments: A service centric approach," in *HCI International 2018 — Posters' Extended Abstracts (HCI 2018)*, ser. Communications in Computer and Information Science, C. Stephanidis, Ed., vol. 852. Cham: Springer, 15–20 Jul. 2018, pp. 463–468.

[5] A. Sprowitz, S. Pouya, S. Bonardi, J. V. D. Kieboom, R. Mockel, A. Billard, P. Dillenbourg, and A. J. Ijspeert, "Roombots: Reconfigurable robots for adaptive furniture," *IEEE Computational Intelligence Magazine*, vol. 5, no. 3, pp. 20–32, Aug. 2010.

[6] R. C. Arkin, "Ethics and autonomous systems: Perils and promises [point of view]," *Proceedings of the IEEE*, vol. 104, no. 10, pp. 1779–1781, Oct. 2016.

[7] F. Kirchbuchner, T. Grosse-Puppendahl, M. R. Hastall, M. Distler, and A. Kuijper, "Ambient intelligence from senior citizens' perspectives: Understanding privacy concerns, technology acceptance, and expectations," in *Ambient Intelligence*, B. De Ruyter, A. Kameas, P. Chatzimisios, and I. Mavrommati, Eds. Cham: Springer International Publishing, 2015, pp. 48–59.

[8] I. Altman, "Privacy regulation: Culturally universal or culturally specific?" *Journal of Social Issues*, vol. 33, no. 3, pp. 66–84, 1977.

[9] J. D. Halamka, P. Szolovitsa, D. Rind, and C. Safran, "A WWW implementation of national recommendations for protecting electronic health information," *Journal of American Medical Informatics Association*, vol. 9, pp. 320–330, 2002.

[10] D. Kim, K. Park, Y. Park, and J.-H. Ahn, "Willingness to provide personal information: Perspective of privacy calculus in IoT services," *Computers in Human Behavior*, vol. 92, pp. 273–281, 2019.

[11] R. A. Ameedee and W. Lee, "Exploiting user privacy in IoT devices using deep learning and its mitigation," in *Twelfth International Conference on Emerging Security Information, Systems and Technologies*, 2018, pp. 43–47.

[12] P. Kleinman, *Philosophy 101 From Plato and Socrates to Ethics and Metaphysics, an Essential Primer on the History of Thought*. Avon, MA: Adams Media, 2013.

[13] —, *The Constitution of the United States with the Declaration of Independence and the Articles of Confederation*. New York: Barnes & Noble, 2005.

[14] P. Brey, *Ethical Aspects of Information Security and Privacy*. Berlin, Heidelberg: Springer, 2007, pp. 21–36.

[15] L. Floridi, "Information ethics: On the philosophical foundation of computer ethics," *Ethics and Information Technology*, vol. 1, no. 1, pp. 33–52, May 1999.

[16] G. Birchley, R. Huxtable, M. Murtagh, R. ter Meulen, P. Flach, and R. Gooberman-Hill, "Smart homes, private homes? an empirical study of technology researchers' perceptions of ethical issues in developing smart-home health technologies," *BMC Medical Ethics*, vol. 18, no. 1, p. 23, 2017.

[17] J. Chung, G. Demiris, and H. J. Thompson, "Ethical considerations regarding the use of smart home technologies for older adults: An integrative review," *Annual Review of Nursing Research*, vol. 34, no. 1, pp. 155–181, 2016.

[18] K. R. Sollins, "IoT big data security and privacy vs. innovation," *IEEE Internet of Things Journal*, 2019.

[19] Institute of Medicine and National Research Council, *Fostering Independence, Participation, and Healthy Aging Through Technology: Workshop Summary*. Washington, D.C.: The National Academies Press, 2013.

[20] S. T. Peek, E. J. Wouters, J. van Hoof, K. G. Luijkx, H. R. Boeije, and H. J. Vrijhoef, "Factors influencing acceptance of technology for aging in place: A systematic review," *International Journal of Medical Informatics*, vol. 83, no. 4, pp. 235–248, 2014.

[21] K. K. Walman, "Older Americans 2016: Key indicators of well-being," Federal Interagency Forum on Aging-Related Statistics, Washington, D.C., Tech. Rep., 2016.

[22] World Health Organization, "World report on ageing and health," World Health Organization, Geneva, Switzerland, Full report, 2015.

[23] Z. Mahmood, H. Ning, A. Ullah, and X. Yao, "Secure authentication and prescription safety protocol for telecare health services using ubiquitous IoT," *Applied Sciences*, vol. 7, no. 10, pp. 1–22, 2017.

[24] National Research Council, *Computational Technology for Effective Health Care: Immediate Steps and Strategic Directions*. Washington, D.C.: National Academies Press, 2009.

[25] President's Information Technology Committee, "Revolutionizing healthcare through information technology," The Networking and Information Technology Research and Development (NITRD) Program, Alexandria, VA, PITAC Reports, Jun. 2004.

[26] Telligen and gpTRAC, "Telehealth start-up and resource guide," Office of the National Coordinator for Health Information Technology (ONC), Version 1.1, Oct. 2014.

[27] B. Sinclair, *IoT Inc.: How Your Company Can Use the Internet of Things to Win in the Outcome Economy*. New York: McGraw-Hill Education, 2 Jun. 2017.

[28] P. Sundaravadivel, E. Kougianos, S. P. Mohanty, and M. K. Ganapathiraju, "Everything you wanted to know about smart health care: Evaluating the different technologies and components of the Internet of Things for better health," *IEEE Consumer Electronics Magazine*, vol. 7, no. 1, pp. 18–28, Jan. 2018.

[29] M. Martin, R. Weibel, C. Röcke, and S. M. Boker, "Semantic activity analytics for healthy aging," *IEEE Computing Edge*, vol. 4, no. 12, pp. 36–40, Dec. 2018.

[30] K. A. Stroetmann, L. Kubitschke, S. Robinson, V. Stroetmann, K. Cullen, and D. McDaid, "How can telehealth help in the provision of integrated care?" World Health Organization, Regional Office for Europe, Copenhagen, Denmark, Policy Brief 13, 2010.

[31] Office for Civil Rights, "Summary of the HIPAA privacy rule," U.S. Department of Health & Human Services, Washington, DC, OCR Privacy Brief, May 2003.

[32] —, "Regulation (EU) 2016/679 of the European parliament and of the council of 27 april 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing directive 95/46/Ec (General Data Protection Regulation)," European Parliament and the Council of the European Union, Official Journal of the European Union L 119/1, 4 May 2016.

[33] Vidyo, "Saving lives, saving money: Why you need a virtual care center," Vidyo, Inc., Hackensack, NJ, Tech. Rep., 2018.

[34] ——, "Making telehealth work for you: The ultimate guide," Vidyo, Inc., Hackensack, NJ, Tech. Rep., 2018.

[35] B. Noah, M. S. Keller, S. Mosadeghi, L. Stein, S. Johl, S. Delshad, V. C. Tashjian, D. Lew, J. T. Kwan, A. Jusufagic, and B. M. R. Spiegel,

"Impact of remote patient monitoring on clinical outcomes: an updated meta-analysis of randomized controlled trials," *npj Digital Medicine*, vol. 1, no. 20172, 2018.

[36] D. Gračanin, R. B. Knapp, T. L. Martin, and S. Parker, "Smart virtual care centers in the context of performance and privacy," in *Proceedings of the 15th International Conference on Telecommunications (ConTEL)*, 3–5 Jul. 2019.

[37] G. Sprint, D. J. Cook, R. Fritz, and M. Schmitter-Edgecombe, "Using smart homes to detect and analyze health events," *Computer*, vol. 49, no. 11, pp. 29–37, Nov. 2016.

[38] C. LeRouge, J. Ma, S. Sneha, and K. Tolle, "User profiles and personas in the design and development of consumer health technologies," *International Journal of Medical Informatics*, vol. 82, no. 11, pp. e251–e268, 2013.

[39] F. Cicirelli, G. Fortino, A. Giordano, A. Guerrieri, G. Spezzano, and A. Vinci, "On the design of smart homes: A framework for activity recognition in home environment," *Journal of Medical Systems*, vol. 40, no. 9, pp. 1–17, Sep. 2016.

[40] P. Rashidi and D. J. Cook, "COM: A method for mining and monitoring human activity patterns in home-based health monitoring systems," *ACM Transactions on Intelligent Systems and Technology*, vol. 4, no. 4, pp. 64:1–64:20, Oct. 2013.

[41] J. Doyle, E.-J. Hoogerwerf, J. Kuiper, E. Murphy, C. Hannigan, J. Dinsmore, T. van der Auwermeulen, J. Albert, A. Jacobs, L. Maluccelli, L. Desideri, and V. Fiordelmondo, "Designing a proactive, person-centred, digital integrated care system," *International Journal of Integrated Care*, vol. 17, no. 5, p. A211, 2017.

[42] ISO/TR, "Health informatics — interoperability of telehealth systems and networks – part 1: Introduction and definitions," International Organization for Standardization, Standard ISO/TR 16056-1:2004, 2004.

[43] ——, "Health informatics — interoperability of telehealth systems and networks – part 2: Real-time systems," International Organization for Standardization, Standard ISO/TR 16056-2:2004, 2004.

[44] ——, "Health informatics — security and privacy requirements of ehr systems for use in conformity assessment," International Organization for Standardization, Standard ISO/TR 14441:2013, 2013.

[45] D. J. Solove, "A taxonomy of privacy," *University of Pennsylvania Law Review*, vol. 154, no. 3, pp. 477–560, Jan. 2006.

[46] A. J. Gill, A. Vasalou, C. Papoutsi, and A. N. Joinson, "Privacy dictionary: A linguistic taxonomy of privacy for content analysis," in *Proceedings of the 2011 Annual Conference on Human Factors in Computing Systems (CHI '11)*. New York: ACM, 2011, pp. 3227–3236.

[47] P. J. Radics and D. Gračanin, "Privacy in domestic environments," in *Proceedings of the 2011 Annual Conference Extended Abstracts on Human Factors in Computing Systems (CHI EA '11)*. New York: ACM, 7–12 May 2011, pp. 1735–1740.

[48] P. J. Radics, D. Gracanin, and D. Kafura, "Preprocess before you build: Introducing a framework for privacy requirements engineering," in *Proceedings of the 2013 International Conference on Social Computing (SocialCom)*, 8–14 Sep. 2013, pp. 564–569.

[49] S. Codio, D. Kafura, M. Pérez-Quinonez, A. Kavanaugh, and D. Gracanin, "Identifying critical factors of community privacy," in *Proceeding of the 2012 Symposium On Usable Privacy and Security (PASSAT 2012)*. IEEE, 3–5 Sep. 2012, pp. 666–675.

[50] D. Kafura, T. DeHart, M. Pérez-Quinonez, D. Gracanin, and A. Kavanaugh, "Enhancing tools for community privacy," in *Proceeding of the PETools: Workshop on Privacy Enhancing Tools*, 9 Jul. 2013.

[51] J. Kolter, T. Kernchen, and G. Pernul, "Collaborative privacy management," *Computers & Security*, vol. 29, no. 5, pp. 580–591, 2010.

[52] S. D. Warren and L. D. Brandeis, "The right to privacy," *Harward Law Review*, vol. 4, no. 5, pp. 193–220, 15 Dec. 1890.

[53] A. F. Westin, *Privacy and Freedom*. New York: Atheneum, 1967.

[54] A. Hazeyama, H. Washizaki, N. Yoshioka, H. Kaiya, and T. Okubo, "Literature survey on technologies for developing privacy-aware software," in *Proceedings of the IEEE 24th International Requirements Engineering Conference Workshops (REW 2016)*, Sept 2016, pp. 86–91.

[55] V. Bellotti and A. Sellen, "Design for privacy in ubiquitous computing environments," in *Proceedings of the third conference on European Conference on Computer-Supported Cooperative Work*. Norwell, MA: Kluwer Academic Publishers, 1993, pp. 77–92.

[56] M. S. Ackerman, L. F. Cranor, and J. Reagle, "Privacy in e-commerce: Examining user scenarios and privacy preferences," in *Proceedings of the 1st ACM conference on Electronic commerce (EC '99)*. New York: ACM, 1999, pp. 1–8.

[57] Federal Trade Commission, "How to comply with the children's online privacy protection rule," Federal Trade Commission, Direct Marketing Association, Internet Alliance, Washington, DC 20580, A Guide, 20 Jun. 1999.

[58] P. Carayon, "Human factors of complex sociotechnical systems," *Applied Ergonomics*, vol. 37, no. 4, pp. 525–535, Jul. 2006.

[59] K. Mindermann, F. Riedel, A. Abdulkhaleq, C. Stach, and S. Wagner, "Exploratory study of the privacy extension for system theoretic process analysis (STPA-Priv) to elicit privacy risks in eHealth," in *Proceedings of the 25th IEEE International Requirements Engineering Conference Workshops (REW 2017)*, Sep. 2017, pp. 90–96.

[60] H. Mora, D. Gil, R. M. Terol, and J. A. J. Szymanski, "An IoT-based computational framework for healthcare monitoring in mobile environments," *Symmetry*, vol. 17, no. 10, p. 2301, Oct. 2017.

[61] S. A. Tovino, "The HIPAA privacy rule and the EU GDPR: Illustrative comparisons," *Scholarly Works*, no. 1066, 2017.

[62] Y. Yang, X. Zheng, W. Guo, X. Liu, and V. Chang, "Privacy-preserving smart IoT-based healthcare big data storage and self-adaptive access control system," *Information Sciences*, vol. 479, pp. 567–592, 2019.

[63] J. Grossklags, N. Christin, and J. Chuang, "Secure or Insure? A Game-Theoretic Analysis of Information Security Games," in *Proceedings of the 17th ACM International Conference on World Wide Web*, 2008, pp. 209–218.

[64] F. He, J. Zhuang, and N. S. V. Rao, "Game-Theoretic Analysis of Attack and Defense in Cyber- Physical Network Infrastructures," in *Proceedings of the Industrial and Systems Engineering Research Conference*, 2012.

[65] M. H. Manshaei, Q. Zhu, T. Alpcan, T. Basar, and J.-P. Hubaux, "Game Theory Meets Network Security and Privacy," *ACM Computing Surveys*, vol. 45, no. 3, pp. 25–39, 2013.

[66] H. Narasimhan, V. Varadarajan, and P. Rangan, "Towards a Cooperative Defense Model Against Network Security Attacks," in *Proceedings of the 9th Workshop on the Economics of Information Security*, 2010.

[67] S. Shiva, S. Roy, and D. Dasgupta, "Game Theory for Cyber Security," in *Proceedings of the 6th Annual Workdhop on Cyber Security and Information Intelligence Research*, 2010.

[68] S. Roy, C. Ellis, S. Shiva, D. Dasgupta, V. Shandilya, and Q. Wu, "A Survey of Game Theory as Applied to Network Security," in *Proceedings of the 43rd Hawaii International Conference on Systems Sciences*, 2010.

[69] A. R. Sfar, Y. Challal, P. Moyal, and E. Natalizio, "A game theoretic approach for privacy preserving model in IoT-based transportation," *IEEE Transactions on Intelligent Transportation Systems*, 2019.

[70] M. Wooldrige and P. E. Dunne, "On the computational complexity of qualitative coalitional games," *Artificial Intelligence*, vol. 4, no. 158, pp. 28–73, Dec. 2004.

[71] R. Zhang, R. Xue, and L. Liu, "Security and privacy on blockchain," 2019.

[72] A. Narayanan, J. Bonneau, E. Felten, A. Miller, and S. Goldfeder, *Bitcoin and cryptocurrency technologies: a comprehensive introduction*. Princeton University Press, 2016.

[73] N. Patel, P. Oza, and S. Agrawal, "Homomorphic cryptography and its applications in various domains," in *International Conference on Innovative Computing and Communications*. Springer, 2019, pp. 269–278.

[74] M. Eltoweissy, M. Azab, S. Olariu, and D. Gračanin, "A new paradigm for a marketplace of services: Smart communities in the IoT era," in *Proceedings of the 2019 International Conference on Innovation and Intelligence for Informatics Computing, and Technologies (3ICT 2019)*, 22–23 Sep. 2019.

[75] National Academies of Sciences, Engineering, and Medicine, *Making Value for America: Embracing the Future of Manufacturing, Technology, and Work*. Washington, D.C.: National Academies Press, 2015.