Liberalization of Digital Twins of IoT-Enabled Home Appliances via Blockchains and Absolute Ownership Rights

Cankal Altun, Bulent Tavli, and Halim Yanikomeroglu

IoT-enabled home appliances are still in their infancy, especially from the perspective of customers, which hinders widespread market penetration. To relieve this skeptical attitude of customers toward IoT appliances, it is important to design human-centric business models rather than corporate-centric ones. IoT ecosystems that make use of cognitive outputs from the social network of things can assist in the establishment of such business models.

Abstract

IoT-enabled home appliances are still in their infancy, especially from the perspective of customers, which hinders widespread market penetration. To relieve this skeptical attitude of customers toward IoT appliances, it is important to design human-centric business models rather than corporate-centric ones. IoT ecosystems that make use of cognitive outputs from the social network of things can assist in the establishment of such business models. The contributions of this article are twofold. First, we propose a reference model that grants the absolute ownership of the fog-located digital twin (DT) of a home appliance to its owner and promotes human-centric services and applications on this twin by utilizing blockchains (BCs) and BC-enabled clouds. Second, by enabling customers to have absolute ownership rights over the fog-located DTs, the model paves the way for the liberalization of DTs as well as the appliances coupled to them, which is an important step in revealing the true value that underlies human-centricity and things-to-things collaboration.

Introduction

Since the beginning of this century, the Internet of Things (IoT) has been paving the way for a variety of home appliance applications based mostly on human-to-things interactions and increasingly on things-to-things interactions. Despite the benefits and initiatives brought by such applications, consumers still show hesitation in adopting IoT-enabled appliances [1], mainly since they see very limited added value or no real difference in their lives in what IoT promises or brings. Besides, most appliance owners view IoT applications as potential threats to their privacy and the core functionality of their appliances. As people's attitude toward the Internet has taken on a new dimension with the penetration of social media applications, it is also crucial to give a social structure to IoT in order to bring out the true value of IoT for appliance owners. The paradigm of "social network of intelligent objects" has been introduced by [2] and named Social IoT (SIoT). Similarly, [3] came up with another paradigm called Cognitive IoT (CIoT) that pushes the current IoT one step further by incorporating cognitive computing technologies in conjunction with data generated by connected devices. Equipping IoT with such cognitive tasks, that can benefit from things-to-things social collaboration, will enable further business cases which have the potential to bring a breakthrough in customer perception in IoT-enabled appliances.

IoT designs have faced a number of challenges, such as issues of heterogeneity, scalability, identification, constrained resources, mobility, security, and privacy [4]. Unlike Industrial IoT, IoT applications for home appliances with social and cognitive capabilities will face even more complexity due to extra requirements, such as ease of use, customer satisfaction management, incentive mechanisms, extensive interoperability, and ownership management. Today's IoT applications on home appliances seem to bring more value to their manufacturers than they do to their customers, making them more corporate-centric than human-centric. To break the ice between consumers and IoT, business models arising from the integration of social and cognitive capabilities shall be in consumers' favor.

To address the aforementioned issues in IoT applications on home appliances, the following three strategic enablers are proposed as solution building blocks:

- Digital twins (DTs) for addressing heterogeneity and mobility
- Fog computing for addressing scalability, constrained resources of edge systems, and the limitations of cloud systems
- Blockchain (BC) for addressing centricity, security, and privacy, and enabling micro-payments

Our main contribution is the creation of a DT architecture and careful definition of its constituents (e.g., fog and BC) specifically for IoT-enabled home appliances. To the best of our knowledge, the novel model proposed in this article is the first in the literature to assign absolute ownership of DTs of IoT-enabled home appliances to their owners and to liberalize their usage on fog systems via BCs and BC-enabled clouds.

In the rest of this article, the basic building blocks are presented and the key requirements of DTs are outlined. Subsequently, the proposed model for the DT architecture and use cases are elaborated. Finally, concluding remarks are provided.

Digital Object Identifier:
10.1109/MCOM.001.1900072

Cankal Altun and Bulent Tavli are with TOBB University of Economics and Technology; Halim Yanikomeroglu is with Carleton University.

0163-6804/19/$25.00 © 2019 IEEE

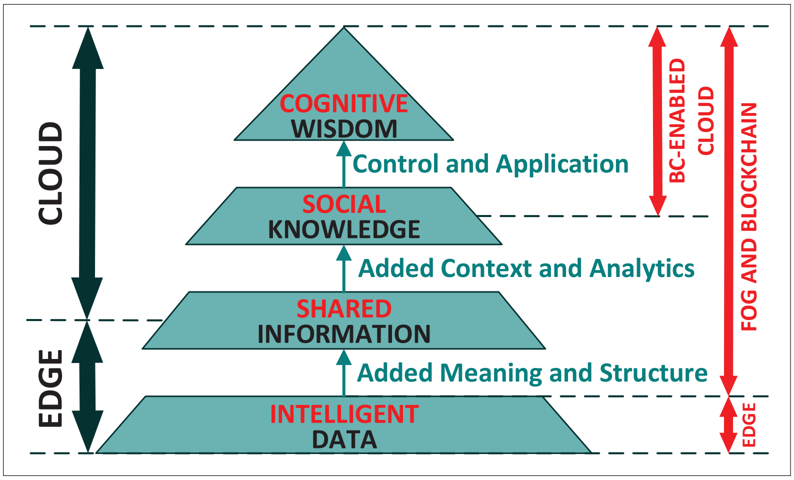


Figure 1. Despite the difficulty of defining clear boundaries on the data-information-knowledge-wisdom (DIKW) pyramid [9] and exact demarcation, we opted to compare traditional (left side) and proposed (right side) handling of the data.

Preliminaries

The novel DT architecture depends on several concepts and constituents, which are concisely overviewed in this section. We explain the characteristics of SIoT and CIoT relevant to our proposed architecture. Then we establish fog computing as an intermediary between resource-constrained IoT devices and the Internet. We then advocate the convenience of DTs as agents of IoT devices at the cyber space. Following that, we introduce BCs, which bring secure transactional capabilities to our architecture.

Social and Cognitive IoT

As discussed in [2], SIoT enables object-initiated interactions (as opposed to human-initiated interactions) via virtualization of objects and paves the way for creating, managing, controlling, and monitoring social objects intelligently and cognitively in real time [5]. The cognitive aspect is strengthened in [3] with the CIoT paradigm to promote the object's learning, context-aware perception-action cycle, semantic derivation, and knowledge discovery via social networks with other objects. The IoT framework proposed by [6] enables the cognitive management and abstraction of the heterogeneity of real-world objects (RWOs) via their virtual counterparts. However, the cognition still relies on a central server and interaction of it with smart home RWOs.

Fog Computing

Fog is a compromise between a resource-constrained, bandwidth-limited, hardly extendable edge and a centralized, edge-distant, limitedly mobile cloud. As opposed to a replacement or an alternative to cloud, fog operates in conjunction with cloud and can act as an extension of cloud, which is closer to the edge for enabling new services and applications [7]. By offering capabilities such as location awareness, edge closeness, low latency, mobility, heterogeneity, high availability, extendibility, bandwidth and energy conservation, rapid action and response on time-sensitive data, and filtering and preprocessing data pushed to cloud, fog computing is considered to be a key enabler for overcoming limitations in IoT and driving IoT's social-cognitive future [7, 8]. Besides its distinctive features as an intermediary, fog also renders the applicability of BC in IoT more feasible (i.e., hosting BC on resource-constrained end nodes has been one of the biggest challenges for BC-IoT interoperability [8]). As shown in Fig. 1, considering the demanding IoT applications and emerging issues, creating wisdom out of data can be shifted from cloud to BC-enabled fog systems.

Digital Twins

DTs can be considered direct boosters for ontology-based semantic interoperability for addressing the issue of heterogeneity in IoT applications by providing an abstraction between the physical and virtual worlds. DTs, especially in tandem with fog systems, can be regarded as key enablers for SIoT and CIoT applications in home appliances by addressing mobility and scalability in IoT. In [10], the authors present a DT architecture for a cloud-based cyber-physical system, which is closer to the domain of home appliances by taking a different owner for each DT or a group of DTs into account.

Blockchain

As a trustless network for keeping a tamper-proof distributed ledger via decentralized consensus, BC is considered to be one of the most impressive disruptive technologies of the last decade (arguably the most revolutionary technology after the Internet). The story of BC began with Satoshi Nakamoto's Bitcoin (named, retrospectively, Blockchain 1.0), which snowballed with many other financial BCs, that have just been used for monetary purposes. Blockchain 2.0 has been developed based on Nick Szabo's smart contract idea, with the purpose of enabling peer-to-peer and decentralized transfer of programmable transactions (e.g., Ethereum). Afterward, Blockchain 3.0 platforms (e.g., IOTA, Cardano) have arisen for addressing the challenges of former BCs such as scalability, interoperability, sustainability, privacy, and governance. With the introduction of Blockchain 3.0, BC-IoT association has gained significant momentum.

Despite struggling with resistance from business and the public, decentralized storage (e.g., Filecoin), computing (e.g., Golem), authentication, digital identity, and access control [11], as well as many other useful services for IoT are already available on BC.

Key Requirements for the System

The requirements outlined in this section are particularly important in ensuring added value and trust, especially the trustworthiness of the business cases, within the model.

For highlighting the motivation behind the proposed model and establishing a concrete basis for requirement specification, we present a user scenario including some use cases that may arise after the liberalization of DTs of consumer electronics as follows:

A customer, interested in buying a heating system, decides to buy the system and its DT rights in the form of a secure element (e.g., as a SIM card). To use the digital applications offered for this heating appliance, she registers herself as an owner of the appliance and activates the DT via the manufacturer's BC on which this particular appliance *has been identified with a chain of trust and coupled to its DT before leaving the manufacturer's production facilities. After registration, she installs the DT to her smart home gateway, which is capable of using services from several BC applications and is paired to her digital wallet. The gateway can be considered as a fog node that can interact with several BCs for purchasing and accessing services such as storage, DT backup, and computation of cognitive algorithms. Within this system, she, as the owner of the appliance, may now decide to sell a set of data from the heating appliance to the manufacturer via the manufacturer's BC in exchange for the manufacturer's crypto-coins, which can be spent on technical services (e.g., repair), new products in the manufacturer's stores, or applications (e.g., predictive maintenance) from DT application markets. Besides, she may decide to sell data to third-party data aggregators via public BCs and use the earnings in other compatible platforms to buy applications for the heating system (e.g., improved heating control with weather forecast). Finally, she may even leave certain controls of this heating system to the manufacturer or any third-party service provider (ideally certified by the manufacturer) to ensure efficient operation.*

Albeit this scenario is far from covering all possibilities and cases, it provides insight on being able to generate a basic set of key requirements among many.

Physical Appliance and DT Coupling

The appliance and its DT shall be coupled in a way that all measurement, operational, and status data are pushed from the appliance to the twin through a secured link, while the twin is also able to drive controls, applications, and updates (wisdom in general) back to the appliance through the same secured link, as also suggested in [12]. In other words, the DT shall be designed like a remote mastermind for the appliance. However, this link does not have to be a real-time link, since it is not intended to be used for controlling real-time and safety-critical operations on the appliance but more for altering the settings, tuning the algorithms, and defining the long-term strategies in perception and actuation.

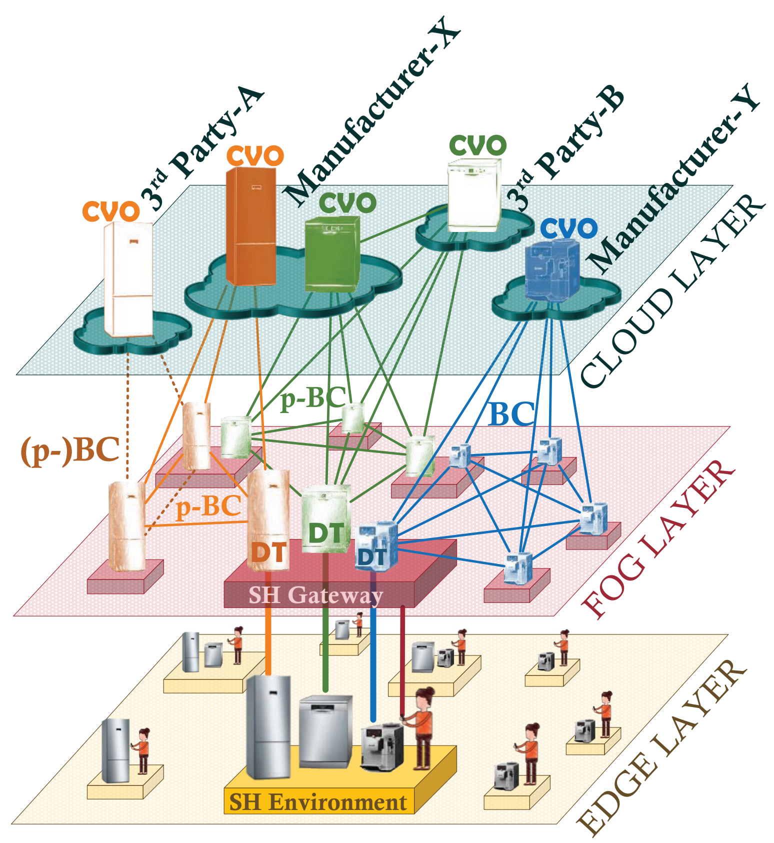
Avoiding Digital Figments

We define a digital figment (DF) as a mock twin that imitates the behavior of a DT without any link to a physical appliance. Such DFs can arise due to a broken link between a physical appliance and its DT (e.g., due to the expiration of the appliance), copying another DT illegally, or creating a new DT coupled to a mock appliance or another digital mate that can drive doctored data. DFs threaten the reliability of the data, the availability of the services, the accuracy of the analysis, and the trust in data and service trading. Therefore, the proposed model shall ensure that there is one and only one true and authenticated DT coupled to one and only one uniquely identifiable physical appliance [13].

Absolute Ownership of DTs

Absolute ownership is free and absolute control of the owner over her/his appliance, and its DT is maintained from the time of purchase until expiration for the following:

- To register, revoke, manage, and transfer the DT
- To decide on the storage location (fog, cloud, or BC)
- To decide on the computational resources, such as fog, cloud, or distributed ones (BC)
- To hand over/take back the control of DTs to/from services providers



p-BC	: permissioned Blockchain
(p-)BC	: permissioned or public Blockchain
SH	: Smart Home
DT	: Digital Twin
CVO	: Composite Virtual Object

Figure 2. Model overview.

Many studies estimate 20–50 connected devices per household by 2020. As such, the DT-host of the proposed model should be able to handle ownership operations of at least several dozen DTs.

Liberalization of DTs

Many connected appliances on the market push some data in the background of the manufacturer's cloud without the awareness or benefit of the owner. However, as discussed in [11], appliance owners are willing to exchange the data from their appliances in return for economic benefits. To make the most of IoT, a free flow of data among appliances, appliance owners, and service providers must be facilitated in an open IoT ecosystem by enabling innovative, user-centered, and novel business models. In light of the fact that a free flow of data is desirable for all participating entities with economic interests, our model will ensure the liberalization of DTs of the appliances.

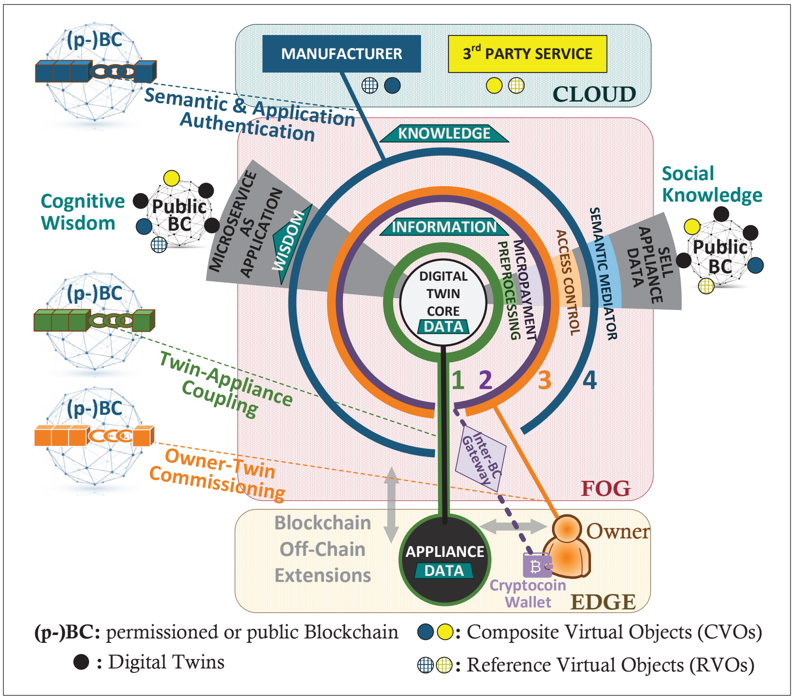


Figure 3. Detailed structure of a digital twin.

Reference Model

The proposed model consists of edge, fog, and cloud layers that are interconnected by permitted or public BCs (Fig. 2). For reference, we assume that edge and fog layers together form a smart home (SH) environment composed of the owner's mobile device(s), SH appliances, and a resourceful SH gateway that hosts the DTs of these appliances. In the model, the DTs of the same appliance type are able to participate in permitted or public BC(s) for establishing social bonds with other DTs to implement cognitive algorithms at the fog layer. Manufacturers and third parties located at the cloud layer also interact with DTs via BCs simply for collecting (buying) data from DTs and pushing (selling) applications/services back to them. Therefore, the cloud layer is employed as a BC-enabled service generator and distributor, contrary to its current role of being a central service provider and executor. Each layer and their interactions via BCs are examined further in the subsequent subsections.

Edge Layer

In the proposed model, the edge layer contains:

- Mobile device(s) of the appliance owner for controlling/monitoring appliances and communicating with the SH gateway
- Smart appliances from a variety of manufacturers
- Digital wallet(s) of the owner, for sending/receiving micropayments

The appliances at the edge layer are considered to have limited storage and processing capabilities (e.g., most appliances have a few kilobytes of RAM) for maintaining a perpetual BC node, which requires, typically, hundreds of megabytes of RAM, and executing cognitive algorithms, which easily requires gigabytes of RAM depending on the algorithm. Therefore, after commissioning (via Shell-1: Twin-Appliance Coupling in Fig. 3), each appliance relies on its own DT for participating BCs and to make use of distributed cognitive algorithms for converting data into wisdom. However, the appliances are still assumed to have memory and processing power margins and are thereby extensible to get any update (as a result of generated wisdom) pushed from their DTs.

Fog Layer

Fog is utilized for the management of DTs in accordance with the characteristics of fog systems mentioned above. DTs located at this layer provide an abstraction between resource-constrained appliances and resource-hungry applications.

DT Hosting: For concreteness, we modeled our system with an SH gateway, the basic properties of which are listed as follows:

- It has memory and processing resources that are sufficient to host or support (if DT is already provided as a hardware) multiple DTs. For example, running a full Ethereum node requires 3 GB RAM, therefore, SH Gateway shall have at least several GBs of RAM.
- It is assumed to have interfaces for secure DT attachment and to be extendible in storage and processing power. A variety of technologies can be used, especially for DT attachment, such as SIM, eSIM, or secure USB flash to name but a few.
- It is capable of communicating via several standards, such as WiFi, Bluetooth, Thread, Zigbee, Z-Wave, KNX, and Powerline, and can be extended via its standard interfaces (e.g., via USB dongles) to support additional protocols.
- It can participate in BCs and enable the owner to send/receive micropayments via various types of digital coins (inter-BC gateway).
- The SH owner has full authorization and absolute control over it.

DT Structure: The detailed structure of a fog-hosted DT is illustrated in Fig. 3. The design follows the onion principle. Therefore, in all applications, shells around the DT core issue their own checks and ensure that the applications penetrate to and are delivered from the real appliance in a safe, secure, and privacy preserving way.

DT Core: A manufacturer is responsible for modeling all sensing and control capabilities of its appliances (either via proprietary methods or via some industry standards). While the appliance sends its sensor and status data to the DT core, the DT core will send control and status update requests back to the appliance over a secure and authenticated channel. Furthermore, any software updates (e.g., algorithms) will also be conveyed through the DT core to the physical device.

Shell-1: Twin-Appliance Coupling: This shell enables the authenticated and secure coupling of DT to its appliance as required above. Any application, accessing the data at the core, can verify the twin and its link to a real physical appliance via its respective BC. The appliance and the twin are considered to be certified within a chain of trust as offered by the authentication, digital identity, and access control BCs mentioned earlier. Therefore, this shell also meets the requirement of avoiding DFs by ensuring that DT has a one-to-one link with a uniquely identifiable physical appliance.

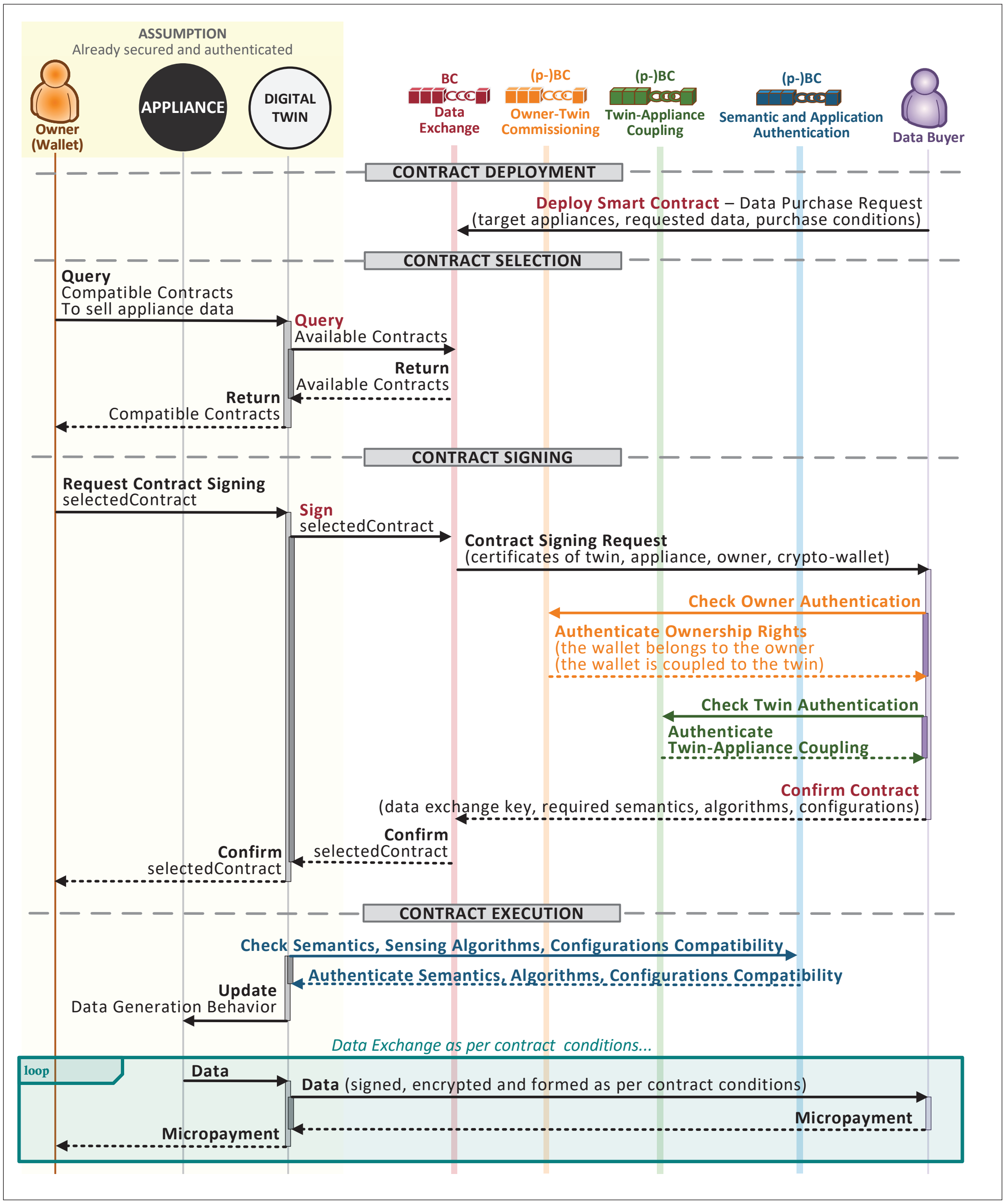

ASSUMPTION
Already secured and authenticated
Owner
(Wallet)
APPLIANCE
DIGITAL
TWIN
BC
Data
Exchange
(p-)BC
Owner-Twin
Commissioning
(p-)BC
Twin-Appliance
Coupling
(p-)BC
Semantic and Application
Authentication
Data Buyer
CONTRACT DEPLOYMENT
Deploy Smart Contract – Data Purchase Request
(target appliances, requested data, purchase conditions)
CONTRACT SELECTION
Query
Compatible Contracts
To sell appliance data
Query
Available Contracts
Return
Available Contracts
Return
Compatible Contracts
CONTRACT SIGNING
Request Contract Signing
selectedContract
Sign
selectedContract
Contract Signing Request
(certificates of twin, appliance, owner, crypto-wallet)
Check Owner Authentication
Authenticate Ownership Rights
(the wallet belongs to the owner
(the wallet is coupled to the twin)
Check Twin Authentication
Authenticate
Twin-Appliance Coupling
Confirm Contract
(data exchange key, required semantics, algorithms, configurations)
Confirm
selectedContract
Confirm
selectedContract
CONTRACT EXECUTION
Check Semantics, Sensing Algorithms, Configurations Compatibility
Authenticate Semantics, Algorithms, Configurations Compatibility
Update
Data Generation Behavior
Data Exchange as per contract conditions...
loop
Data
Data (signed, encrypted and formed as per contract conditions)
Micropayment
Micropayment

Figure 4. Selling the data of an appliance application.

In the proposed model, we regard the cloud systems (especially the manufacturer cloud) as the provider of the algorithms and high-value inputs, such as Composite Virtual Objects and Reference Virtual Objects, required by DTs in order to transform knowledge into wisdom locally at fog level.

Shell-2: Micropayment Control: The middle shell (Shell-2 and 3), in general, is the linkage of the twin to the appliance owner and enables the owner to exercise absolute ownership rights over the DT for meeting the absolute ownership requirements. The middle-inner shell is coupled to the owner's digital wallet(s) which is responsible for receiving/sending micropayments according to smart contract(s) defined during the installation of the respective application. Moreover, this shell is able to make digital currency conversions if required. The functionality of this shell can be considered the most important element for the liberalization of DTs by making micropayments and trade of data and microservices possible.

Shell-3: Ownership Control: As in the trusted coupling between the appliance and its twin, the relationship between the owner and the appliance means that its DT will also be commissioned to a BC. The middle-outer shell, in this manner, enables the owner to apply her/his permissions and to access control decisions for the flow of data to/from the DT.

Shell-4: Interoperability Control: Finally, the outer shell is responsible for all manufacturer defined checks in order to protect the twin from uncertified applications and to equip genuine semantic mediators. Moreover, this shell can ensure interoperability by integrating the semantic mediators from the manufacturer.

Cloud Layer

In the proposed model, we regard the cloud systems (especially the manufacturer cloud) as the provider of the algorithms and high-value inputs, such as composite virtual objects (CVOs) and reference virtual objects (RVOs), A manufacturer can make micropayments with its proprietary crypto-currency and offer the opportunity to buy services or products with this crypto-currency. A very fitting example of the third party data aggregators can be Dbrain BC which enables sharing of training datasets to crowdworkers and data scientists to develop Artificial Intelligence applications.

required by DTs in order to transform knowledge into wisdom locally at the fog level. In general, the manufacturer and third-party BC-enabled clouds have the following missions within the model:

- Collecting information from DTs via BC and clustering this information into CVOs
- Maintaining and providing (especially by the manufacturer) simulated (ideal) twins as RVOs
- Providing (especially by the manufacturer) semantic mediators for interoperability
- Generating and delivering cognitive algorithms that can be executed by DTs in order to convert knowledge into wisdom
- Managing permissions and maintaining the operation of permitted BCs

Blockchains

In the proposed model, DTs are assumed to be capable of attaching to a variety of BCs: permitted BCs from a manufacturer (e.g., Manufacturer-X from Fig. 2), public BCs (e.g., Manufacturer-Y from Fig. 2), and permitted or public BCs from third parties (e.g., third party from Fig. 2). The manufacturer, depending on its strategy, may decide to employ one of the following BC approaches:

- Maintaining/using a single (p-)BC (permitted or public BC) for all services
- Maintaining/using separate (p-)BCs for a variety of services
- Making use of side or child chain structures

Besides getting appliance-specific services from BCs, DTs may also benefit from the aforementioned public BCs for generic services such as storage and processing power. Last but not least, we envision that Blockchain 3.0 with better scalability, interoperability, and better fit to IoT is adopted in the model.

Use Cases

Our model promises a wide range of use cases by ensuring the following features for appliance owners:

- Absolute control over appliances by liberating their DTs from the manufacturers' clouds and offering edge-near placement and management of DTs
- 40–60 percent improved storage, processing power, total energy consumption, and average latency compared to centralized cloud models [14]
- More scalable (by a factor of the average number of devices connected to an SH gateway) as well as privacy and security preserving participation of appliances in the SIoT ecosystem via BCs
- Easier integration of cognitive algorithms and big data reduction methods (70–90 percent potential decrease in data volume in circulation) into DTs and more efficient execution of these algorithms on local and smaller datasets [15]
- Faster DT-appliance interaction without suffering from network latency during the appliance management and execution phases of cognitive algorithms
- Increased intelligence of offline and autonomous operations
- Improved extendibility and application diversity by making use of the progressive BC technology
- Reduced cloud processing, storage, and network costs

Selling Appliance Data

One of the possible use cases that can run on the proposed model is selling the appliance's data anonymously in a privacy preserving way to the manufacturer or third-party data aggregators, as illustrated in Fig. 4. While selling the data:

- The purchaser can verify appliance-twin coupling (shell-1).
- Micropayment channels and contract details can be defined (shell-2).
- The owner can define the restrictions, permissions, and access privileges (shell-3).
- Both parties can ensure compatibility, accurate data translation, and representation (shell-4).

Manufacturers, on the other hand, can also come up with various business models based on the proposed architecture. For example, a manufacturer can make micropayments with its proprietary crypto-currency and offer the opportunity to buy services or products with this crypto-currency. A very fitting example of third-party data aggregators can be Dbrain BC, which enables sharing of training datasets to crowdworkers and data scientists to develop artificial intelligence applications.

Purchasing Microservices

The owner can purchase some applications for the DTs of appliances. An example application is predictive maintenance on a DT using a social network of DTs.

Usage-Based Pricing

Usage-based pricing (home appliance as a service) can also be enabled within this model. A service dealer can retain ownership (Shell-3) of the DT, and hand over the appliance and its usage rights to another user through a smart contract for both parties on Shell-2.

Conclusion

In this study, we present a novel architecture of DTs of home appliances that are placed at the fog layer and interfaced to other twins and the cloud via BCs. In fact, to overcome the limitations of cloud systems and address the challenges posed by social and cognitive IoT applications on home appliances, we make use of three key enablers: DTs, fog computing, and BC. Secure twin-appliance coupling, avoidance of digital figments, enabling absolute ownership rights, and liberalization of DTs are specified as the key requirements. In the architecture, DTs are structured in layers, and linkage of each layer to appliances, appliance owners, digital wallets, and manufacturers is secured by BCs. We elaborate on sample applications such as selling appliance data, purchasing microservices, and usage-based pricing that can run on this architecture.

Acknowledgments

The authors would like to thank the Scientific and Technological Research Council of Turkey (TUBITAK) for their financial support and Dr. Sebastian Berning for his initiative on this work.

References

[1] H. Yang, H. Lee, and H. Zo, "User Acceptance of Smart Home Services: An Extension of the Theory of Planned Behavior," *Ind. Mgmt. Data Sys.*, vol. 117, no. 1, Feb. 2017, pp. 68–89.

[2] L. Atzori, A. Iera, and G. Morabito, "SIoT: Giving a Social Structure to the Internet of Things," *IEEE Commun. Lett.*, vol. 15, no. 11, Nov. 2011, pp. 1193–95.

[3] Q. Wu *et al.*, "Cognitive Internet of Things: A New Paradigm Beyond Connection," *IEEE Internet of Things J.*, vol. 1, no. 2, Mar. 2014, pp. 129–43.

[4] M. Nitti *et al.*, "The Virtual Object as a Major Element of the Internet of Things: A Survey," *IEEE Commun. Surveys & Tutorials*, vol. 18, no. 2, 2nd qtr. 2016, pp. 1228–40.

[5] Z. U. Shamszaman and M. I. Ali, "Towards a Smart Society Through Semantic Virtual-Object Enabled Real-Time Management Framework in the Social Internet of Things," *IEEE Internet of Things J.*, vol. 5, no. 4, Aug. 2018, pp. 2572–79.

[6] D. Kelaidonis *et al.*, "Virtualization and Cognitive Management of Real World Objects in the Internet of Things," *Proc. IEEE Int'l. Conf. Green Comp. and Commun.*, 2012, pp. 187–94.

[7] K. Yeow *et al.*, "Decentralized Consensus for Edge-Centric Internet of Things: A Review, Taxonomy, and Research Issues," *IEEE Access*, vol. 6, no. 7, Dec. 2017, pp. 1513–24.

[8] M. Samaniego and R. Deters, "Internet of Smart Things — IoST: Using Blockchain and CLIPS to Make Things Autonomous," *Proc. IEEE Int. Conf. Cog. Comp.*, 2017, pp. 9–16.

[9] R. L. Ackoff, "From Data to Wisdom," *J. Appl. Sys. Anal.*, vol. 16, no. 1, Jan. 1989, pp. 3–9.

[10] K. M. Alam and A. El Saddik, "C2PS: A Digital Twin Architecture Reference Model for the Cloud-Based Cyber-Physical Systems," *IEEE Access*, vol. 5, Jan. 2017, pp. 2050–62.

[11] T. Hardjono and N. Smith, "Cloud-Based Commissioning of Constrained Devices Using Permitted Blockchains," *Proc. ACM Int'l. Wksp. IoT Privacy Trust Security*, 2016, pp. 29–36.

[12] C. Machado and A. A. Medeiros Frohlich, "IoT Data Integrity Verification for Cyber-Physical Systems Using Blockchain," *Proc. IEEE Int'l. Symp. Real-Time Distrib. Comp.*, vol. 277, no. 12, 2018, pp. 83–90.

[13] O. Novo, "Blockchain Meets IoT: An Architecture for Scalable Access Management in IoT," *IEEE Internet of Things J.*, vol. 5, no. 2, Apr. 2018, pp. 1184–95.

[14] A. Muthanna *et al.*, "Secure and Reliable IoT Networks Using Fog Computing with Software- Defined Networking and Blockchain," *MDPI J. Sens. Actuator Net.*, vol. 8, no. 1, Feb. 2019.

[15] M. H. ur Rehman *et al.*, "Big Data Reduction Methods: A Survey," *Data Sci. Eng.*, vol. 1, no. 4, Dec. 2016, pp. 265–84.

Biographies

Cankal Altun (caltun@etu.edu.tr) is currently with Robert Bosch Power Tools GmbH, Leinfelden-Echterdingen, Stuttgart, and is a Ph.D. candidate in the Department of Electrical and Electronics Engineering, TOBB University of Economics and Technology, Ankara, Turkey. His current research interests are IoT, blockchain, security and privacy in consumer electronics, social and cognitive IoT, embedded systems, and smart grid.

Bulent Tavli (btavli@etu.edu.tr) is a professor in the Department of Electrical and Electronics Engineering, TOBB University of Economics and Technology. His current research areas are IoT, wireless communications, networking, optimization, embedded systems, information security and privacy, and smart grid.

Halim Yanikomeroglu [F] (halim@sce.carleton.ca) is a full professor in the Department of Systems and Computer Engineering at Carleton University, Ottawa, Canada. His research interests cover many aspects of 5G/5G+ wireless networks. His collaborative research with industry has resulted in 34 granted patents. He is a Fellow of the Engineering Institute of Canada and the Canadian Academy of Engineering, and he is a Distinguished Speaker for IEEE Communications Society and IEEE Vehicular Technology Society.