Holistic Blockchain Approach to Foster Trust, Privacy and Security in IoT based Ambient Assisted Living Environment

Akpanakak Mkpa
School of Computing and Information Science
Anglia Ruskin University
Cambridge. UK
akpanakak.mkpa@pgr.anglia.ac.uk

Jeannette Chin
School *of Computing Sciences*
University of East Anglia
Norwich, UK
0000-0002-9398-5579

Adrian Winckles
School of Computing and Information Science
Anglia Ruskin University
Cambridge. UK

***Abstract*— The application of blockchains techniques in the Internet of Things (IoT) is gaining much attention with new solutions proposed in diverse areas of the IoT. Conventionally IoT systems are designed to follow the centralised paradigm where security and privacy control is vested on a "trusted" third-party. This design leaves the user at the mercy of a sovereign broker and in addition, susceptible to several attacks. The implicit trust and the inferred reliability of centralised systems have been challenged recently following several privacy violations and personal data breaches. Consequently, there is a call for more secure decentralised systems that allows for finer control of user privacy while providing secure communication. Propitiously, the blockchain holds much promise and may provide the necessary framework for the design of a secure IoT system that guarantees fine-grained user privacy in a trustless manner. In this paper, we propose a holistic blockchain-based decentralised model for Ambient Assisted Living (AAL) environment. The nodes in our proposed model utilize smart contracts to define interaction rules while working collaboratively to contribute storage and computing resources. Based on the blockchain technique, our proposed model promotes trustless interaction and enhanced user's privacy through the blockchain - Interplanetary File System (IPFS) alliance. The proposed model also addresses the shortfall of storage constraints exhibited in many IoT systems.**

Keywords—blockchain; Internet of Things; AAL; Trust and Privacy; Security; Smart Contracts; Ethereum Swarm, IPFS

I. INTRODUCTION

The Internet of Things (IoTis described as potentially amongst the most significant disruptive technologies of the 21st century, and it is believed to be the angular stone of the information and Communication Technology (ICT) market in the coming years [1]. In 2016, there were approximately 13.3 million IoT connections in the UK and this is expected to grow at a compound annual growth rate (CAGR) of approximately 36% to 155.7 million connections at the end of 2024 [2]. Similarly, Cisco forecasts 50 billion devices will be connected worldwide by 2020, with an average of about 16 IoT devices per person; a potential market in excess of $14 trillion [3]. A recent study shows that by 2025, the IoT will form an integral part of everyday things such as household, furniture, wearable health systems, food packaging, clothing, and paper documents [4] [5].

IoT allows the integration of tiny pervasive devices into our daily lives. This, in turn, enables the digital world to directly affect our physical space through sensing and automation. While this integration presents several opportunities for improved services, it also exposes us to threats and attacks that prevail in the digital space [6]. By way of an example is Ambient Assisted Living (AAL) environment - a technical system built to support the elderly and infirmed to improve their safety and enhance day-to-day living [7]. IoT in AAL environment utilizes intelligent devices in the homes of the elderly to continuously monitor and collect information; both system, and user data, and forward them to a centralised system for processing and analysis. The data gathered reveals patterns that can be used by healthcare professionals to assist with diagnosis or collaborative care or treatment of ailments[8]. It has been suggested that IoT plays a significant role in AAL for improving wellbeing, safety and healthcare of millions of elderly people worldwide due to the nature of its power of connectivity and sensing. Hence vital health statistics can be provided by constantly gathering data from the body and environment, which in turn helps longevity [9]. However, existing methods allow sensitive data to remain accessible to the "trusted" broker, hence, exposing users to various attack and privacy leaks. Consequently, systems built upon the implicit trust on third-parties (trustful systems) will fail to satisfy the privacy requirements of the post-Snowden and Cambridge Analytica era user. To this end, Implementation of IoT in privacy-sensitive areas such as AAL need to be modeled to encourage the trust the outputs of a system without trusting any actors within it [10] (trustless trust interaction). This will bolster user confidence and adoption of IoT in such areas.

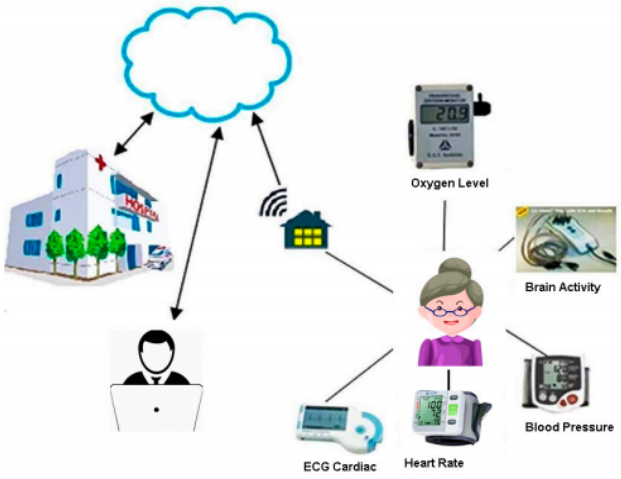

Figure 1. A simplified representation of the current implementation of IoT in AAL.

In this paper, we first present security and privacy challenges of AAL, explore existing implementations of AAL and discuss the drawbacks of these implementations. We then propose a holistic approach to address the drawbacks. We argue the use of blockchain, smart contracts, and IPFS will enable trustless trust transactions in the distributed AAL environment enhancing user's privacy and security. The rest of the paper is organized as follows: Section I and II explore the background information on IoT and AAL, identifying its opportunities and challenges. In Section III, we introduce the use of blockchain as a possible solution to the challenges of the IoT in Ambient Assisted Living environment and also investigate the pitfalls of using blockchain in AAL. To conclude this section, we present our proposed holistic model to address these problems. In Section IV we conclude the paper and set up our future work.

INTERNET OF THINGS AND AMBIENT ASSISTED LIVING

A. Background and Context

AAL is gaining significant attention as a result of the fast-growing demographic of the aging population. This puts a great burden on the traditional care infrastructure, thereby challenging the viability of conventional elderly care systems. According to [11] successful utilization of AAL in association with IoT technologies promises to greatly lower operational cost, facilitate collaborative care, and encourage the elderly to live independently. However, Security and user privacy protection remain a major challenge [12] to IoT-AAL integration (Fig 1). Information collected by IoT devices used therein are of interest to many players and present an attractive target to cybercriminals. For instance, a user's personal information can be sold to third parties where it will be analysed to reveal patterns that might affect the user's chances of fair treatment, especially in health insurance. Furthermore, users are becoming apprehensive about critical health data being tampered with or stored in untrusted servers, as disclosure or abuse of personal information can lead to property damage. This is as evidenced in the recent Edward Snowden and Cambridge Analytica Saga [13], which caused great mistrust in centralised processing of personal information, leading to an intensified call for fine-grained control of user privacy. This abuse of trust is cited as a principal reason for the drastic decline in the adoption of IoT technologies in recent times, especially in home automation and AAL. Consequently, research in AAL has intensified and many systems, methods, and prototypes have been developed to provide solutions to security and privacy concerns. Minnetti et al [14] presented smart hospitals system (SHS); an IoT-aware system which provides automatic patient and assets tracking in hospitals and care homes. Suntiamorntut et al [15] proposed an affordable system for private homes to assist the elderly to live independently. Other approaches such as Bodyguarding Heart [16] rely on wearable devices in combination with smartphones to monitor vital signs and other health information.

Although the implementations cited above provide a level of privacy through access control mechanism, users are still exposed to internal abuse or misuse of private information collected and managed by the broker. To this end, systems built upon the centralised brokered model will fail to guarantee the advocated level of privacy control and user autonomy that is required of future IoT and AAL implementations. As a result, implicit trust and the reliability of centralised systems has been recently challenged [17], therefore calling for more secure decentralised systems that allow for fine-grained control of user privacy. Summarily, the potential benefits of IoT/AAL cannot be fully utilized except new methodologies, approaches and techniques are developed to meet IoT requirements in terms of the trust, privacy, and security [18].

B. Opportunities and Challenges

Home automation is currently the slowest area of IoT penetration because consumers have failed to embrace the potentials of IoT for fear of privacy invasion [19]. Future IoT development will favor a scenario where users maintain fine-grained control over access to sensitive data collected and benefit from proceeds of analysis or the use of their personal data. This calls for a shift in the conventional approach to security in IoT to embrac new paradigms that radically lower the cost, allowing users to extract value for data exchange, promote privacy and autonomy, while also providing adequate security. It is succinct to say that the brokered model cannot effectively satisfy the call for fine-grained control of user privacy and trust requirement of the new IoT, we argue that new models built upon the Decentralised Ledger Technology (DLT) will provide a solution that satisfies the privacy demands of the post-Snowden era user. Such implementation must permit secure communication amongst peers, allowing trustless user-controlled interactions, development of micro-services, user autonomy and transparency at all times.

II. BLOCKCHAIN

A paper published by Satoshi Nakamoto in 2008 introduced the concept of Blockchain to enable entities to transact in a safe and secure manner without the need for a trusted third party [20]. Bitcoin; a first generation blockchain was developed principally for cryptocurrencies, but it lacked features necessary to facilitate solutions as desired in other sectors such as the IoT. However, Ethereum blockchain platform was later introduced by Vitalik Buterin in 2015 to facilitate touring completeness and rich-statefulness; a system feature that allows programs to be written to solve any reasonable computational problem assuming there are enough resources available [21]. The Blockchain has grown in recent years and has been adapted to provide solutions in different sectors of the economy such as energy [22], finance, intelligent transport systems legal, IoT, and healthcare [23].

Blockchain represents a new approach to service delivery, and start-ups are seeking new ways to incorporate its abilities to enable transactions between unreliable actors to be transparent, highly resistant and auditable. Put it simply; blockchain can be viewed as a ledger or database that maintains a continuously growing set of time-stamped transaction records, where each hashed block of transactions is chained and linked to the hash of the previous one [24][25]. Blockchain permits multiple nodes on a network to transact securely without relying on a trusted third party. Contrary to the brokered model which mandates users to trust the broker implicitly, a blockchain model relies on cryptographically verifiable systems rather than trust [26];

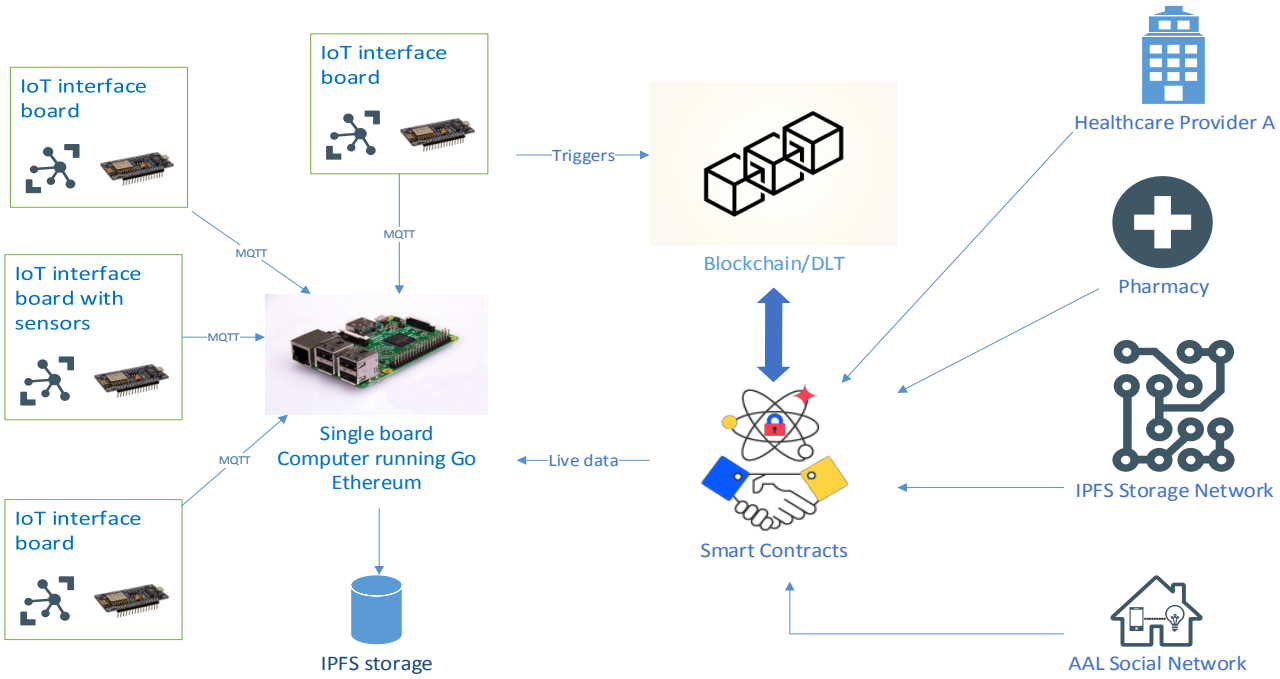

Figure 2. Diagrammatic representation of the proposed model.

each node maintains a local copy of a common ledger of transactions and trusts the cryptographic system to ensure that copies of the ledger within each node remain the same. This enables disparate parties to transact securely without the need to trust each other or a trusted third party, hence the basis of its efficiency in developing decentralised trustless systems. Despite the promise of blockchain to IoT and AAL, storage capacity remains a major challenge [27] in practice owing to the fact that Blockchain was originally designed to append tiny records of financial transactions to a ledger and lacks the capacity to store large data streams generated by pervasive devices used in IoT and AAL. The ledger grows continually as more blocks are created, putting more pressure on the resources, hence reducing its ability to scale considerably [28].

A. A collaborative holistic approach to AAL using Blockchain, Smart Contracts, IPFS decentralised storage, and Ethereum Swarm as a possible solution

We propose a collaborative holistic approach to address the storage problem in blockchain-based AAL environment using decentralised storage - the Interplanetary File System (IPFS) [29], together with Smart Contracts and Ethereum Blockchain (Fig 2). Ethereum is preferred in our implementation because of its Turing-complete capability. Other components of our proposed implementation are as described below:

IPFS is a p2p hypermedia protocol that combines the distributed hash table, an incentivized block exchange, and self-certifying namespace to coordinate a network of untrusted peers to cooperate in distributing files to each other [30]]. Built using the technology behind bit torrent, IPFS synthesizes the best ideas in distributed file systems built to date to connect all computing devices with the same system of files. IPFS provides a high throughput content-addressed block storage model that exhibits no single point of failure and best suited in an environment where nodes do not need to trust each other [29]. In addition, IPFS can handle big data with ease. It is well suited for hosting and distributing petabyte dataset, high-volume high definition on-demand and real-time media streaming, computing on large data across organizations, versioning, and linking of massive data sets and preventing accidental disappearance of important files.

Similarly, Swarm is an Ethereum decentralised content distribution and storage platform. It is used for storing Ethereum public records and Distributing Applications (Dapps) code. Ethereum Swarm is censorship resistant. Like blockchain, it has no single point of failure and supports a built-in incentive mechanism for participating peers who contribute storage and bandwidth resources to facilitate content distribution. Swarm is designed with a mechanism to ensure the availability of unpopular contents and scales easily. Smart Contracts are a set of executable functions and state variables that govern the interaction of nodes in a blockchain network. Smart contracts reside in the blockchain and are executed when transactions are addressed or sent to it. Smart contracts define input parameters that must be supplied by the interacting calls, which is used to manipulate the state of the contract based on the publicly available logic contained within the contract. Once compiled, smart contracts are uploaded to the blockchain which assigns a unique address to each smart contract. smart contracts can operate autonomously interacting with other smart contracts or devices in the blockchain.

In our proposed holistic model, an IoT-based AAL environment will consist of a network of interacting sensors such as motion sensors, fall detection sensors, environmental sensors, wearable devices, and smart appliances. These will collaborate to provide relevant data necessary for effective health monitoring of the occupant. Using machine learning and coded instructions, data collected will be intelligently analysed for triggers that may require response or

intervention of the healthcare team. In cases where the supplied data is large, the IPFS address and the hash of the trigger data will be stored in the blockchain, while the bulk data is stored in the distributed storage network of nodes that contribute storage facility for a reward (IPFS, Swarm) Content addressing will be used to properly index the files for access when needed. To access information stored in the blockchain and the distributed storage network, smart contracts will be employed to ensure user-controlled access to data. The smart contract will define which data is accessed by whom, based on the role and agreement with the data owner. This will also allow the user to trade data for value, thereby extracting some form of financial or concessional benefits from services rendered by companies using data generated by these devices. For instance, the user can extract value from health data generated by IoT-AAL devices for use in research, marketing or product development. Furthermore, any information of importance can be stored in the blockchain as defined by the user and other key players in the IoT-AAL ecosystem.

III. Conclusion and Future Work

Although IoT promises great cost reduction and enhancement to AAL and elderly care, there are many barriers that need to be overcome in order to gain user trust and improve the technology adoption rate. We propose a holistic model to address this problem. With the use of blockchain technique, smart contract, IPFS, and Swarm, our proposed holistic model enhance privacy and security [31] by using smart contracts which define rules for interaction with users and data as a means to empower user's control, thereby facilitating trustless transactions between nodes on the network. The storage constraints associated with blockchain in IoT is resolved by leveraging distributed scalable IPFS storage platform. The future work is to implement this proposed holistic model and conduct critical system and user evaluations to uncover challenges and optimize accordingly. We aim to use resource-constrained devices in our testing environment as shown in figure 2. Our first target users are elderly homes in the UK. Modifications will be made where necessary to adapt some associated platforms to meet the needs of AAL.

References

[1] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security, privacy and trust in Internet of Things: The road ahead," Comput. Networks, 2015.

[2] T. Winchcomb, S. Massey, and P. Beastall, "Review of latest developments in the Internet of Things," vol. 1636, no. 1636, pp. 1–143, 2017.

[3] Taylor Stuart, "10 Predictions for the Future of the Internet of Things," 2015. [Online]. Available: https://blogs.cisco.com/cle/10-predictions-for-the-future-of-the-internet-of-things. [Accessed: 15-Jan-2019].

[4] J Chin ; V Callaghan; S. B. Allouch; "The Internet of Things from Smart Environments Perspective", In press, Journal of Ambient Intelligence and Smart Environments, doi: 10.3233/AIS-180506

[5] X. Caron, R. Bosua, S. B. Maynard, and A. Ahmad, "The Internet of Things (IoT) and its impact on individual privacy: An Australian perspective," Comput. Law Secure. Rev., 2016.

[6] C. Pahl, N. EL Ioini, and S. Helmer, "A Decision Framework for Blockchain Platforms for IoT and Edge Computing," Proc. 3rd Int. Conf. Internet Things, Big Data Secur., no. March, pp. 105–113, 2018.

[7] A. Dohr, R. Modre-Osprian, M. Drobics, D. Hayn, and G. Schreier, "The internet of things for ambient assisted living," ITNG2010 - 7th Int. Conf. Inf. Technol. New Gener., pp. 804–809, 2010.

[8] J. Ko, C. Lu, M. B. Srivastava, J. A. Stankovic, A. Terzis, and M. Welsh, "Wireless sensor networks for healthcare," in Proceedings of the IEEE, 2010, vol. 98, no. 11, pp. 1947–1960.

[9] D. Metcalf, S. T. J. Milliard, M. Gomez, and M. Schwartz, "Wearables and the internet of things for health: Wearable, interconnected devices promise more efficient and comprehensive health care," IEEE Pulse, vol. 7, no. 5, pp. 35–39, 2016.

[10] P. Rothenpieler, C. Becker, and S. Fischer, "Privacy concerns in remote monitoring and social networking platform for assisted living," 2011.

[11] R. Fernandez Horcajada et al., "Final Report. A Study concerning a Market Observatory in the Ambient Assisted Living field," 2014.

[12] M. Memon, S. R. Wagner, C. F. Pedersen, F. H. Aysha Beevi, and F. O. Hansen, "Ambient Assisted Living healthcare frameworks, platforms, standards, and quality attributes," Sensors (Switzerland), vol. 14, no. 3, pp. 4312–4341, 2014.

[13] S. Landau and | Google, "Highlights from Making Sense of Snowden, Part II: What's Significant in the NSA Revelations."

[14] L. Catarinucci et al., "An IoT-Aware Architecture for Smart Healthcare Systems," IEEE Internet Things J., vol. 2, no. 6, pp. 515–526, 2015.

[15] W. Suntiamorntut, S. Charoenpanyasak, and J. Ruksachum, "An elderly assisted living system with wireless sensor networks," Proc 4th Jt. IFIP Wireless. Mob. Netw. Conf. WMNC 2011, pp. 1–6, 2011.

[16] Preventice Solutions, "Preventice - BodyGuardian Heart," 2015. [Online] [Accessed: 23-Jan-2019].

[17] W. Sun, Z. Cai, Y. Li, F. Liu, S. Fang, and G. Wang, "Security and Privacy in the Medical Internet of Things: A Review," Secur. Commun. Networks, vol. 2018, 2018.

[18] M. Abomhara, "Security and Privacy in the Internet of Things : Current Status and Open Issues," Priv. Secur. Mob. Syst. (PRISMS), 2014 Int. Conf., pp. 1–8, 2014.

[19] P. Brody and V. Pureswaran, "Device democracy: Saving the future of the Internet of Things IBM," IBM Glob. Bus. Serv. Exec. Rep., 2015.

[20] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008.

[21] J. Ray, "A Next-Generation Smart Contract and Decentralized Application Platform Introduction to Bitcoin and Existing Concepts History," 2019. [Online]. [Accessed: 10-Apr-2019].

[22] N. Z. Aitzhan and D. Svetinovic, "Security and Privacy in Decentralized Energy Trading Through Multi-Signatures, Blockchain and Anonymous Messaging Streams," IEEE Trans. Dependable Secure. Comput., vol. 15, no. 5, pp. 840–852, 2018.

[23] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, "MedRec: Using blockchain for medical data access and permission management," Proc. - 2016 2nd Int. Conf. Open Big Data, OBD 2016, pp. 25–30, 2016.

[24] A. M. Antonopoulos, Mastering Bitcoin, vol. 50, no. 4. 2014.

[25] M. Abomhara and G. M. Køien, "Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks," 2015.

[26] G. Zyskind, O. Nathan, and A. S. Pentland, "Decentralizing privacy: Using blockchain to protect personal data," in Proceedings - 2015 IEEE Security and Privacy Workshops, SPW 2015, 2015.

[27] A. Reyna, C. Martín, J. Chen, E. Soler, and M. Díaz, "On blockchain and its integration with IoT. Challenges and opportunities," Futur. Gener. Comput. Syst., vol. 88, no. 2018, pp. 173–190, 2018.

[28] B. Arshdeep and M. Vijay, Blockchain Applications. 2017.

[29] J. Benet, "IPFS - Content Addressed, Versioned, P2P File System," 2017.

[30] Y. Chen, H. Li, K. Li, and J. Zhang, "An improved P2P file system scheme based on IPSF and Blockchain," in 2017 IEEE International Conference on Big data, 2017

[31] K. Werbach, "Summary : Blockchain , The Rise of Trustless Trust ?," Public Policy Initiat., 2017.