IoT Service Based on JointCloud Blockchain: The Case Study of Smart Traveling

Weili Chen*, Mingjie Ma*, Yongjian Ye*, Zibin Zheng† and Yuren Zhou*
*School of Data and Computer Science
†School of Data and Computer Science, National Engineering Research Center of Digital Life
Sun Yat-sen University, Guangzhou, China
Email: {chenwli9, mamj3, yeyj7}@mail2.sysu.edu.cn, {zhzibin, zhouyuren}@mail.sysu.edu.cn

***Abstract*—With the advancements in Internet technologies and Wireless Sensor Networks (WSN), a new era of the Internet of Things (IoT) is being realized. IoT produces a lot of information which can be used to improve the efficiency of our daily lives and provides advanced services in a wide range of application domains. However, the privacy and the data fusing problems remain major challenges, mainly due to the massive scale and distributed nature of IoT networks and the amount of data collected from IoT increasing at an exponential rate. Thus, a privacy-protected and inter-cloud data fusing platform is needed to the demand for data mining and analytic activities in IoT. In this paper, we propose such a platform based on JointCloud Blockchain and study a novel case of smart traveling based on the proposed platform.**

I. Introduction

Ubiquitous sensing enabled by Wireless Sensor Network (WSN) technologies makes the Internet of Things (IoT) one of the most important technologies of this century. The IoT, connecting physical world and digitalized world, has the potential to change the world as the Internet did [1]. It has received extensive attention among industries and researchers since it was officially published in 2005 [2]. It has been widely used in medical [3], transportation [4], logistics [5] and many other fields. It is predicted that 50 billion devices will be connected to the Internet by 2020 [6]. However, it still suffers many problems and challenges in the following aspects:

- *The efficiency and generality of the IoT architecture*. Although many IoT architectures have been proposed, these architectures are typically aimed at a single specific situation, which often cannot guarantee the efficiency and quality of services.
- *Mass data processing in IoT*. IoT will produce massive amounts of data every day. Determining how to store, process and analyze these data is a challenge.
- *Data security issues*. Because sensors are ubiquitous, many private data can be collected and used to construct digital people (i.e., all various digital information belong to a person), revealing private behavior and lifestyles. Thus, data security issue is one of the most important problems in the application of IoT technology.
- *The difficulty in IoT deployment*. As a result of the strong heterogeneous characteristic of each part, the deployment of IoT has always been extremely challenging.
- *Communication problem in IoT*. Due to the distributed structure of IoT, different parts of IoT need to establish effective communications, in order to ensure the smooth flow of information.

To solve these problems, Service Oriented Architecture (SOA), which can achieve interoperability between heterogeneous devices in a multitude of ways [7], was regarded as a promising solution [8]. However, SOA cannot fulfill the increasing demands of IoT. Thus, new service framework is needed to fulfill the needs from handling the data from billions of devices and improving the efficiency of IoT usage to maximizing the role of IoT. Internet of Things service (IoT service) is proposed. Unlike traditional service which is often heavy-weighted and relies on powerful data centers and computing platforms, IoT service is mainly based on the distributed deployment of the devices.

IoT service has different definitions and different classifications. In a recent paper [9], a complete definition of IoT Service is given as follows:

> *A dynamic end to end information network seamlessly linking physical and cyberspace by which data from objects are connected, interacting and processed to enable people, objects, and systems turning data into useful information and valued services to users.*

Many platforms for IoT service have been proposed such as Baidu and Amazon. However, these platforms are essentially centralized, resulting in privacy leakage concerns. Furthermore, with the proliferation of IoT, many other technologies, such as data mining, machine learning, real-time response and assistant decision-making policy will integrate with and improve IoT service. Thus, it may be more economical to implement IoT service framework by deeply integrated multi-source cloud services based on collaboration among cloud service entities, which is the aim of JointCloud Computing (JCC) [10]. As for the privacy leakage concerns, it is solved by the blockchain technology (i.e., JointCloud Blockchain), which is an underpinning technology for the JointCloud computing [10].

This paper makes the following contributions. First, we provide a simple literature survey on IoT Service models,

which help us to design model on JointCloud. Second, we summarize the IoT Service challenges as data privacy and data fusion. Then, we propose to implement IoT Service based on JointCloud, as it helps to protect the privacy and data fusion. Finally, an imaginary case of smart traveling is studied. Though the proposed solution for the IoT service still remains in the concept stage, we believe this is a meaningful first step.

The remainder of the paper is organized as follows. In Section II, we introduce two important IoT service models. The challenges on IoT service are discussed in Section III. The proposed IoT service platform based on JCC is discussed in Section IV after introducing the Baidu and Amazon IoT service platforms. An application of smart traveling based on JCC is presented in Section V and the paper concludes in Section VI.

II. IoT Service Model

With the development of IoT, various equipment will be connected to the Internet in real time. Determining how to collect data and use these collected data to provide services is an important question. This problem is essentially identical to the problem of IoT service model. In this section, we provide a short survey on IoT service model. According to our survey, the IoT service model contains five parts as shown in Fig. 1. Roughly speaking, the IoT service model contains three tiers. The first tier is the equipment management tier. The second tier is the core of IoT service model. It provides services for various applications in the third tier facilitated by the network which connects equipment.

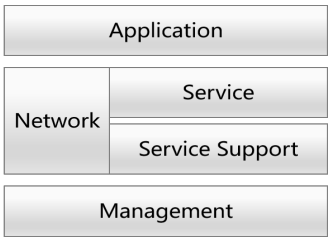

Fig. 1. The Structure of IoT Service Model

Many studies have revolved around the model of IoT service and many achievements have been made. The following subsections introduce two important IoT service models.

A. SOA for IoT

In the initial research process, SOA was seen as the service solution to IoT. SOA is a design framework for the construction of information systems by "combination of service" [11]. There are a number of studies on SOA.

Guinard *et al*. [12] gave a comprehensive account of SOA issues related to the IoT and discussed the problems on network discovery of the embedded device, real-world service discovery, process evaluation and other issues. With the new research progress, many researchers begin to improve the SOA model based on traditional SOA problems to enhance the availability of the model.

Through the study of traditional SOA problems, Zhang *et al*. [13] proposed an event-driven SOA (EDSOA) and also discussed the creation, execution, and coordination of the IoT service, proposing an information-centric session mechanism. This study fills in the gap that distributed logic cannot provide powerful expression to describe business logic in SOA.

Similarly, in [14], Zhu *et al*. designed a PT-based model (PT stands for physical things), and evaluated the model based on an example of emergency rescue. The two have obvious differences in structure. Zhang *et al.* [13] used a three-layer structure, in which, the recipient and provider of the service are separated by the service environment. In this way, the security of the underlying resources is ensured and the efficiency of the service is improved. While the model in [14] adds feedback to the service and dynamically adjusts the service.

From the different perspectives of IoT, some models about SOA have been put forward, in [7], from the perspective of functionalities, a four-layer SOA of IoT service was proposed, namely sensing layer, networking layer, service layer and the interface layer. Compared with the five-layer model in [15], the four-layer one listed the service separately as a layer, highlighting the importance of service.

B. Semantic Model for Service

The semantic model is *a new kind of data models, which adds new data structure and data processing primitives on the basis of the relational model to express complex structures and rich semantics* [16].

The semantic modeling of the IoT service has become a fundamental problem in solving the interoperability in distributed and heterogeneous environment. Therefore, the research of the semantic model of IoT service has also received extensive attention from both academia and industry.

Wang *et al.* [17] thought that most of the current studies on IoT service are mainly focused on the modeling of equipment and resources, while little attention was paid to the access and use of things to generate information. They, therefore, proposed a design that can give a comprehensive description of ontology in the field of knowledge representation, and discussed how to use it to achieve such tasks as service discovery.

Semantic service matching process is to provide a more advanced service-oriented functions of the basic structure, such as IoT in the service recommendation, combination and provision. In order to overcome the semantic synonymy in the semantic service description, Cassar *et al.* [18] proposed a hybrid semantic service matching method, which has obvious advantages in improving semantic service matching accuracy and normalizing discounted cumulative gain (NDCGn) measurement values. In order to enhance IoT service capabilities, Kim *et al.* [19] proposed a service semantic ontology model that is user-centric, and establish the WoO (Web of Objects) platform to provide users with the dynamic IoT service.

III. Challenges on IoT Service

This section depicts two important challenges in IoT service and the possible solution.

A. Data Privacy and Security

With the development of the Internet, security issues have been widely concerned. For the users of IoT service, the first thing to note is security. Based on interconnected cheap sensors, a lot of information about our environment can be collected at a much higher granularity. These detailed information can be used in a wide range of application domains including smart city services and autonomous driverless cars. However, as sensors are ubiquitous, many private data can be collected and used to construct digital people, revealing private behavior and lifestyles. Thus it is one of the most important problems in the application of IoT technology. IoT service security issues include data security, privacy protection and so on. It is now one of the most important issues in the IoT service. Many security issues are identified. Generally, the main problems include:

- *Terminal security*. As for users, the underlying structure of IoT service is blocked. However, there are risks of illegal intrusion in device access, operation, control. Once broken, the IoT service collapse. Thus, the security of the terminal device is very important and is the responsibility of the service providers.
- *Data transmission security*. The Data collected from devices needs to be transmitted to the data center through the Internet or other mediums. Unsafe transmission protocols or models can cause data to be stolen or lost, resulting in the disclosure of user information.
- *Data process security*. Because the massive IoT data are usually stored in the data center. It is very convenient to reveal human behavior by using data mining and machine learning technologies. This is useful for personalized services, but it is also at the risk of tracing specific people.
- *Management security*. IoT service is a highly scalable service. Determining how to expand the service effectively under the existing situation and guarantee the security is also a challenge when the user groups become larger.

Traditional security policy is usually heavy and has a good effect on centralized deployment [20]. However, it cannot effectively maintain the security of IoT service because of the distributed and heterogeneous nature of it. Therefore, it is necessary to investigate new security protection mechanism for IoT service. Many frameworks can be found in the literature. Ning *et al.* [21] proposed a protection mechanism that includes secure data access, privacy-preserving data sharing, and secure access authority transfer. On the basis of typical system and network security technology, a systemic approach to the IoT service security was put forward in [22]. Alam *et al.* [23] proposed a layered IoT architecture, aiming at the security access problems of the IoT service and the interoperability of security attributes among different management domains. To solve the problem of security heterogeneity of wired sensors and wireless sensors in IoT service of multimedia applications, Zhou *et al.* [24] came up with a security architecture. In [25], Abie *et al.* proposed a security framework based on risk adaptability, which is used to solve the security of electronic medical field networking service issues. And Savola *et al.* [26] proposed a high-level adaptive security management mechanism based on security metrics to the problem.

Another notable trend to solve the security problem in IoT service is the adopting of blockchain technology [27]. Blockchain, the underpinning technology of Bitcoin, is considered a disruptive technology that is going to change many industries. It is considered as a promising way to solve the security issues in IoT service system as it is essentially distributed and users are anonymous in it [28].

B. Data Fusion

The amount of data collected from IoT increasing at an exponential rate due to the massive scale and distributed nature of IoT networks. It is natural that these data are stored in data centers or clouds. To provide high-quality services in the IoT era, data fusion is inevitable. Data fusion is the process of integrating multiple data sources to produce more consistent, accurate, and useful information than that provided by any individual data source [29]. However, data is considered as the oil of the digital era. So it is very important to construct a platform which can be used to facilitate data fusion among clouds. Many data exchanges can be found nowadays. However, a centralized data exchange have many weaknesses. For example, the data privacy problem and whether the exchange is trustworthy when disputes occur between participants are big concerns for participants in the data exchange.

Data exchange is a possible way for some applications, but it may be inconvenient for applications based on real-time data. Thus, a uniform platform, which supports contracts for participants and these contracts are automatically effective or invalid according to the predefined clauses, is needed. Take companies of autonomous driverless cars, for example, it is necessary for the companies to make a contract with certain organizations to provide real-time map service and traffic navigation. Furthermore, it is obligated for the companies to provide insurance contracts during the passages on the cars. The company may do all the things by itself, but a more effective way is to buy professional services from other companies.

C. Solution Based on JonitCloud

To solve the aforementioned two challenges, JCC is one of the best choices. JCC is a new generation of cloud computing model which facilitates developers to customize cloud services by the way of software definition and towards the borderless cloud services and resource sharing [10]. It will implement a JointCloud Collaboration Environment (JCCE) which serves as a uniform platform among clouds. As can be seen from Fig. 2, the JCCE is partitioned into four parts. The underlying part is a blockchain [30] that recording all transactions among clouds. We call the underpinning blockchain as JonitCloud Blockchain (JCB). Based on JCB, there are three distributed functional modules: transaction, community and supervision. As in a distributed environment, all the functions are realized by *smart contracts* [31].

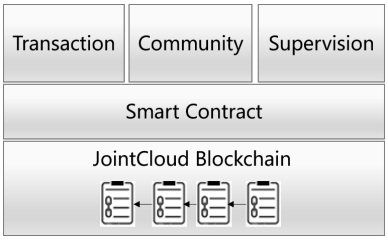

Fig. 2. JointCloud Collaboration Environment (JCCE)

A smart contract is a computer protocol intended to facilitate, verify, or enforce the negotiation or performance of a contract. Smart contracts were first proposed by Nick Szabo in 1996 [32]. Based on blockchain technology, smart contracts can be applied to many industries to make automatic and smart businesses.

By using JCCE, the aforementioned challenges are easy to be solved. Because data privacy is naturally protected due to transactions are stored in JCB and JCCE functions as a decentralized exchange which facilitates resources integration among clouds. All trades and supervisions are done through smart contracts. It helps data fusion among clouds in a trustworthy and impartial environment.

IV. Architectures of IoT Service

IoT service needs not only to dispose of massive real-time and heterogeneous data, but also to support different complex applications for different purposes. Thus, a reasonable platform is necessary for the IoT service. This section first introduces two typical platforms that are based on single clouds. Then, the architecture of IoT service platform based on JCC is proposed.

A. Baidu IoT Platform

Tiangong[1] is an intelligent IoT platform based on Baidu cloud. It provides access to material, material management, rules engine, timing database, machine learning, MapReduce and a series of IoT core products and services based on the integration of big data and artificial intelligence technology. They can help developers quickly move from the device side to the server side to efficiently construct a variety of networking applications.

Tiangong provides a complete solution for the users in industrial manufacturing, energy, retail O2O, car networking, logistics and other industries. The basic architecture of the platform is shown in Fig. 3.

The platform provides a series of IoT services like IoT Parser, IoT Device and Rule Engine, and the details are as follows:

- IoT Parser, through which users can analyze and calculate data in various devices in the cloud, as a result, data traffic will be greatly saved and equipment costs will be reduced. Parsing data in the cloud allows users to adapt parsing rules at any time to suit business changes. Using the cloud's powerful computing capabilities, unlimited data storage capabilities and a rich variety of data analysis programs can help enterprises core business more stable and efficient operation, and stimulate more integration and innovation.
- IoT Device, which provides one station type of equipment management services covering the entire lifecycle of equipment, including the level of equipment management, monitoring, remote control, firmware upgrades and maintenance, and other scenes.
- Rule Engine, helps users to deal with equipment message flexibly. Users can set the message processing rules by the rule engine, and take corresponding measures to carry out monitoring and processing equipment for the specified message, such as pushing to the mobile phone APP. Users can also seamlessly forward device messages to sequential databases, relational databases, and object stores.

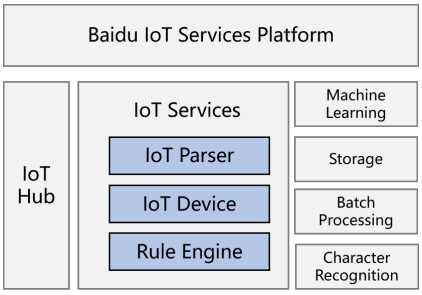

Fig. 3. Baidu IoT Service Platform

In terms of security, Baidu provides two-way verification of equipment and the platform based on TLS (Transport Layer Security) security transmission [33]. Besides, Baidu has also made special security protection for its data processing center. Baidu IoT service platform has provided complete intensive services for many companies including Dengyun and Proud. At present, the main business of Baidu IoT service platform mainly focuses on China.

B. Amazon AWS IoT Platform

Compared to Baidu, Amazon AWS IoT service platform[2] was created earlier, covering a wider range. The platform supports billions of devices, processes massive information and delivers information securely to AWS terminals and other devices. It helps build applications for the IoT, manage infrastructure and analyze data based on integrating with Amazon Lambda, Kinesis, and machine learning services. It has a similar platform structure with Baidu.

Like Baidu, Amazon AWS IoT service platform is also based on their own cloud. AWS has a great advantage that no other platforms has, because it has the largest could platform in the world. Thus it can provide a wider range of services to a larger number of people. However, based on a single cloud makes they all have the same anxious from users.

[1]https://cloud.baidu.com/solution/iot/index.html/

[2]https://aws.amazon.com/cn/iot-platform/

C. IoT Services Structure Based on JCC

The aforementioned two IoT service platforms are based on a single cloud. It may be enough for some applications. However, inter-cloud resource integration will be more economical and convenient for constructing complex applications. Thus, IoT may provide higher services based on JointCloud– clouds which implement JCCE. Figure 4 exhibits the framework for IoT service based on JCC. Roughly, the framework can be portioned into three tiers. The first tier is composed of various sensors which connect to different clouds. The second tier is the clouds joined together by the JCCE. The third tier is the service tier. It provides personalized service to every user and application based on the JCC.

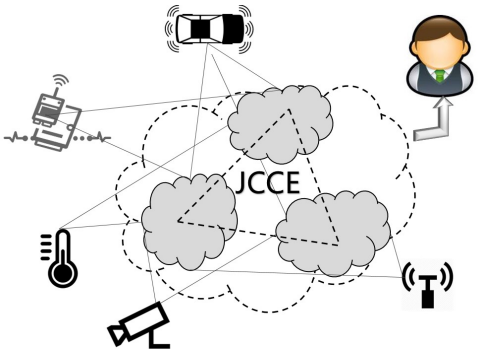

Fig. 4. JCCE IoT Service Platform

The proposed framework based on JCC has many advantages as compared with frameworks based on a single cloud. First of all, the collected sensor data are stored in a private cloud, which mitigated concerns of data security. Next, when it implemented the JCCE, the private cloud can provide IoT service to other clouds or users for more profits if wants. Finally, the trades are automatically executed in the trusted JCCE and all transactions are records in the JCB. There is no risk of user privacy disclose and prejudice.

V. Case Study

This section depicts an IoT service scenario for smart traveling based on JCC. As can be seen from Fig. 5, these are three clouds collaborated together to support the smart traveling based on autonomous driverless car service. *A* is a cloud-focused on providing insurance service for all kinds of vehicles. It stores many historical and real-time data of objects insured. Based on these data, the clouds automatically compute and generate insurance contracts for customers. As the insurance cloud implemented JCCE, the insurance contracts can be implemented as smart contracts and provided to the distributed community of JCCE for users to select. We call these contracts smart insurance contracts.

Cloud *B* is a professional map service company. Furthermore, it provides real-time navigation and path planning by traffic flow monitoring through ubiquitous surveillance cameras. These cameras may be owned or rented from other organizations. Similar to Cloud *A*, it provides these services through JCCE and smart contracts.

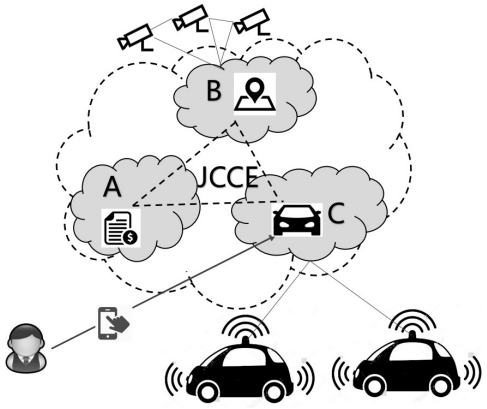

Fig. 5. Smart Traveling Service Based IoT

Cloud *C* is a company operating autonomous driverless cars. The strength of this company is precisely controlling the autonomous driverless car by the data collected from the running cars. It develops an application which helps passengers rent a driverless car through a smartphone.

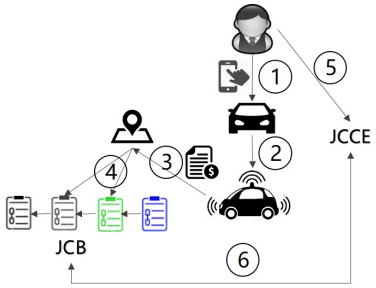

Fig. 6. Procedure of Smart Traveling

Figure 5 describes a new kind of traveling based on IoT service. We call it as *"smart traveling "*, as many aspects of traveling are controlled by smart contracts. Figure 6 shows the procedure of smart traveling. (1) The passenger submits a traveling request through the application on the smartphone to the company of driverless cars. The submitted information include some necessary data such as start position (automatic positioning or manually fill in), destination and the start time; (2) The company receives the order and sends the most suitable car to the start position before start time; (3) The car sends transactions to sign smart contracts with map service and insurance company; (4) The map service smart contract analyze real-time traffic flow to provides real-time navigation service and the key path information will be stored in the JCB; (5) After the traveling , the fees are deducted from the passenger's account and the passenger can score the service; (6) The score will be store in JCB to computing the reputation of the company. Furthermore, if the passenger is not satisfied with the service, he or she can invoke the verdict procedure. The supervision smart contract in the JCCE will call historical data stored in JCB to make an impartial verdict.

VI. Conclusion

IoT technology is going to impact every aspect of our daily lives based on IoT service. However, challenges still abound. The major challenges are data security and data fusing. A possible solution to these problems is building IoT service platforms. However, existed IoT service platforms are based on single cloud, which still has the concerns of privacy disclose and difficult to fusing data. In this paper, we propose to build IoT service based on JCC. The concerns about data security and data fusing can greatly relieve as it provides a trusted environment for resources exchange among clouds and a blockchain to record all these transactions. We analyze a typical application based on JCC. We envision that IoT service based on JCC has a great potential to change our daily lives.

Acknowledgment

The work described in this paper was supported by the National Key Research and Development Program (2016YFB1000101), the National Natural Science Foundation of China (61722214, 61472338), the Program for Guangdong Introducing Innovative and Enterpreneurial Teams (2016ZT06D211), and the Pearl River S&T Nova Program of Guangzhou (201710010046). Zibin Zheng is the corresponding author.

References

[1] K. Ashton, "That internet of things thing," *RFiD Journal*, vol. 22, no. 7, pp. 97–114, 2009.

[2] I. Strategy, "policy unit (spu)," *ITU Internet Reports*, 2005.

[3] F. Hu, D. Xie, and S. Shen, "On the application of the internet of things in the field of medical and health care," in *Proceeding of the Internal conference on IEEE Cyber, Physical and Social Computing*. IEEE, 2013, pp. 2053–2058.

[4] A. Zanella, N. Bui, A. Castellani, L. Vangelista, and M. Zorzi, "Internet of things for smart cities," *IEEE Internet of Things journal*, vol. 1, no. 1, pp. 22–32, 2014.

[5] T. Qu, M. Thürer, J. Wang, Z. Wang, H. Fu, C. Li, and G. Q. Huang, "System dynamics analysis for an internet-of-things-enabled production logistics system," *International Journal of Production Research*, vol. 55, no. 9, pp. 2622–2649, 2017.

[6] X. Jin, S. Chun, J. Jung, and K.-H. Lee, "Iot service selection based on physical service model and absolute dominance relationship," in *Proceedings of the 7th International Conference on Service-Oriented Computing and Applications (SOCA)*. IEEE, 2014, pp. 65–72.

[7] L. Da Xu, W. He, and S. Li, "Internet of things in industries: A survey," *IEEE Transactions on industrial informatics*, vol. 10, no. 4, pp. 2233–2243, 2014.

[8] S. Karnouskos, D. Savio, P. Spiess, D. Guinard, V. Trifa, and O. Baecker, "Real-world service interaction with enterprise systems in dynamic manufacturing environments," in *Artificial Intelligence Techniques for Networked Manufacturing Enterprises Management*. Springer, 2010, pp. 423–457.

[9] X. Shang, R. Zhang, X. Zhu, and Q. Zhou, "Design theory, modelling and the application for the internet of things service," *Enterprise Information Systems*, vol. 10, no. 3, pp. 249–267, 2016.

[10] H. Wang, P. Shi, and Y. Zhang, "Jointcloud: A cross-cloud cooperation architecture for integrated internet service customization," in *Proceedings of the 37th International Conference on Distributed Computing Systems (ICDCS)*. IEEE, 2017, pp. 1846–1855.

[11] N. Komoda, "Service oriented architecture (soa) in industrial systems," in *Proceedings of the 4th International Conference on Industrial Informatics*. IEEE, 2006, pp. 1–5.

[12] D. Guinard, V. Trifa, S. Karnouskos, P. Spiess, and D. Savio, "Interacting with the soa-based internet of things: Discovery, query, selection, and on-demand provisioning of web services," *IEEE transactions on Services Computing*, vol. 3, no. 3, pp. 223–235, 2010.

[13] Y. Zhang, L. Duan, and J. L. Chen, "Event-driven soa for iot services," in *Proceedings of the 11th International Conference on Services Computing (SCC)*. IEEE, 2014, pp. 629–636.

[14] W. Zhu, G. Zhou, I.-L. Yen, and F. Bastani, "A pt-soa model for cps/iot services," in *Proceedings of the 22th International Conference on Web Services (ICWS)*. IEEE, 2015, pp. 647–654.

[15] C.-L. Zhong, Z. Zhu, and R.-G. Huang, "Study on the iot architecture and gateway technology," in *Proceedings of the 14th International Symposium on Distributed Computing and Applications for Business Engineering and Science (DCABES)*. IEEE, 2015, pp. 196–199.

[16] A. Borgida, R. J. Brachman, D. L. McGuinness, and L. A. Resnick, "CLASSIC: A structural data model for objects," in *Proceedings of the 1989 ACM SIGMOD International Conference on Management of Data*. ACM, 1989, pp. 58–67.

[17] W. Wang, S. De, R. Toenjes, E. Reetz, and K. Moessner, "A comprehensive ontology for knowledge representation in the internet of things," in *Proceedings of the 11th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*. IEEE, 2012, pp. 1793–1798.

[18] G. Cassar, P. Barnaghi, W. Wang, and K. Moessner, "A hybrid semantic matchmaker for iot services," in *Proceedings of the 2012 IEEE International Conference on Green Computing and Communications (GreenCom)*. IEEE, 2012, pp. 210–216.

[19] Y. Kim, S. Lee, and I. Chong, "Orchestration in distributed web-of-objects for creation of user-centered iot service capability," *Wireless personal communications*, vol. 78, no. 4, pp. 1965–1980, 2014.

[20] J. L. Greathouse, I. Wagner, D. A. Ramos, G. Bhatnagar, T. Austin, V. Bertacco, and S. Pettie, "Testudo: Heavyweight security analysis via statistical sampling," in *Proceedings of the 41th annual IEEE/ACM International Symposium on Microarchitecture*. IEEE Computer Society, 2008, pp. 117–128.

[21] H. Ning, H. Liu, and L. T. Yang, "Cyberentity security in the internet of things," *Computer*, vol. 46, no. 4, pp. 46–53, 2013.

[22] A. Riahi, Y. Challal, E. Natalizio, Z. Chtourou, and A. Bouabdallah, "A systemic approach for iot security," in *Proceedings of the 2013 International Conference on Distributed Computing in Sensor Systems (DCOSS)*. IEEE, 2013, pp. 351–355.

[23] S. Alam, M. M. Chowdhury, and J. Noll, "Interoperability of security-enabled internet of things," *Wireless Personal Communications*, vol. 61, no. 3, pp. 567–586, 2011.

[24] L. Zhou and H.-C. Chao, "Multimedia traffic security architecture for the internet of things," *IEEE Network*, vol. 25, no. 3, 2011.

[25] H. Abie and I. Balasingham, "Risk-based adaptive security for smart iot in ehealth," in *Proceedings of the 7th International Conference on Body Area Networks*. ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), 2012, pp. 269–275.

[26] R. M. Savola, H. Abie, and M. Sihvonen, "Towards metrics-driven adaptive security management in e-health iot applications," in *Proceedings of the 7th International Conference on Body Area Networks*. ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), 2012, pp. 276–281.

[27] A. Dorri, S. S. Kanhere, and R. Jurdak, "Blockchain in internet of things: Challenges and solutions," 2016.

[28] M. Conoscenti, A. Vetro, and J. C. D. Martin, "Blockchain for the internet of things: A systematic literature review," in *Proceedings of the 13th IEEE/ACS International Conference of Computer Systems and Applications*. IEEE, 2016, pp. 1–6.

[29] D. L. Hall and J. Llinas, "An introduction to multisensor data fusion," *Proceedings of the IEEE*, vol. 85, no. 1, pp. 6–23, 1997.

[30] M. Swan, *Blockchain: Blueprint for a new economy*. " O'Reilly Media, Inc.", 2015.

[31] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the internet of things," *IEEE Access*, vol. 4, pp. 2292–2303, 2016.

[32] N. Szabo, "Smart contracts: Building blocks for digital markets," Sep. 1996. [Online]. Available: http://www.fon.hum.uva.nl/

[33] T. Dierks, "The transport layer security (tls) protocol version 1.2," 2008. [Online]. Available: https://www.ietf.org/rfc/rfc5246.txt