Securing Self-organizing IoT Ecosystem: A Distributed Ledger Technology Approach

Ajayi Oluwashina Joseph-*IEEE Member, Joseph Raffety-IEEE Member, Philip Morrow-IEEE Member, Lin Zhiwei, Christopher Nugent-IEEE Member, Sally McClean-IEEE Member, and Gery Ducatel*

***Abstract*—The proliferation of the Internet of Things has seen it adopted to practically all aspects of life. There has been an increase in demand for more IoT devices which are manufactured by several companies. This has however left need to address vulnerabilities within and threats to these devices. In many cases, these vulnerabilities arise from manufacturer focus on functionality rather than security. Secure by design IoT devices are rare in the market today. Efforts to address this are being made by the IoT research community, however, more effort is required. Deficiencies of current efforts include accountability of devices and privacy of data generated across the IoT landscape. The aim of this Ph.D. research is to improve the security, privacy, veracity, and trust. The approach developed in this study will be based on non-repudiation of actions among self-organized IoT devices in an IoT Ecosystem by leveraging Distributed Ledger Technology (DLT). A proposed system architecture which relies on the Distributed Ledger Technology and its related features will enable services to be applied to the IoT landscape to achieve aspects of end to end IoT security. The initial progress to date is presented within this manuscript.**

***Keywords* – Accountability, Distributed Ledger Technology, Internet of Things, Blockchain, IoT security, Privacy, Threat, Veracity, vulnerabilities.**

I. INTRODUCTION

The Internet of Things(IoT) is a computing paradigm referred to as *"the Future Internet which can be seen as a dynamic global network infrastructure with self-configuring capabilities based on standard and interoperable communication protocols where physical and virtual "things" have identities, physical attributes, and virtual personalities and use intelligent interfaces, and are seamlessly integrated into the information network"* [1]. Additional works [2] have defined IoT as a phenomenon that involves objects which are connected to the internet, interact with each other and their physical environments while incorporating their identities, purposes, and communal resources. IoT devices and their associated services have the potential to directly augment daily life of individuals in several ways such as supporting patient management within healthcare, digitalization of businesses, and improvement in efficiency within business processes which will consequently increase the revenue of businesses if properly managed [3]. In addition to the impact on lives of individuals, an expanded paradigm called Industrial IoT has the potential to augment industrial processes such as optimizing production lines in a manner which increases efficiency, fault and resource predictions, and product planning [4].

British Telecom is acknowledged for supporting this project under the British Telecom Ireland Innovation Centre (BTIIC) at Ulster University.
O.J. Ajayi, J. Rafferty, P. Morrow, L. Zhiwei, C. Nugent, and S. McClean are with Ulster University, Jordanstown, Northern Ireland, BT37 0QB, UK (email: ajayi-o2@ulster.ac.uk, j.rafferty@ulster.ac.uk, pj.morrow@ulster.ac.uk, z.lin@ulster.ac.uk, cd.nugent@ulster.ac.uk, si.mcclean@ulster.ac.uk)
G. Ducatel is with British Telecom, Adastral Park, Martlesham, Ipswich (email: gery.ducatel@bt.com)

This is achieved by deploying sensors, and related internet-connected devices, to enable greater optimization of operations in industries such as providing predictive maintenance to reduce downtime through the data aggregated by these devices. Driven by the benefits to individuals and industry, it is projected that by 2025, the number of IoT devices will number over 100 billion and will contribute over $11 trillion to the global economy [5]. IoT devices do not exist in isolation. They interact with other IoT devices, computational services, end users, and objects to provide their functionality. Given the expected quantity of IoT devices, it is important for these devices to safely and reliably integrate themselves with their environment in order to reduce device management overhead and reduce human intervention [6]. These deficiencies are discussed in the following section.

The proposed project aims to investigate and develop a novel self-organization and management paradigm for IoT devices. This paradigm will ensure that data and resources are safely shared while considering the security, trust, and risk involved in the way they interact. This will lead to providing a better way of securing the IoT Ecosystem.

II. RELATED WORK

The existence of IoT has changed the level of human interaction with their environment. Human decisions can be informed by inputs from devices, machines, and processes. Connected devices can smartly communicate with each other to perform major operations without human intervention to make incisive decisions [7]. This decision might be to auto-provision a new device introduced into IoT Network and form part of the Ecosystem with the device performing a definite function.

IoT enables access to several services over the internet by individuals, government agencies, service providers, industrial customers and societies at large at any time and in any location. These interactions currently exist in several use cases across diverse human operations and functions. IoT solutions have been developed and deployed on a case by case basis [8].

A typical IoT Ecosystem could have heterogeneous devices with different features, capabilities, as well as functionalities. For example, imagine devices such as NEST thermostat, Amazon Alexa, Philip LIFX, and Apple Home kit working together in the same environment without independent device-based integration, we could say – "plug and play" functionalities. These devices and its network which are proprietary based are not suitable for business and lack self-organization.

Another major issue is the existence of diverse communication standards which each device has the liberty to choose from. Various existing wireless communication [9] were reviewed as shown in figure 1 below.

978-1-5386-4980-0/19/$31.00 ©2019 IEEE
978-1-5386-4980-0/19/$31.00 ©2019 IEEE

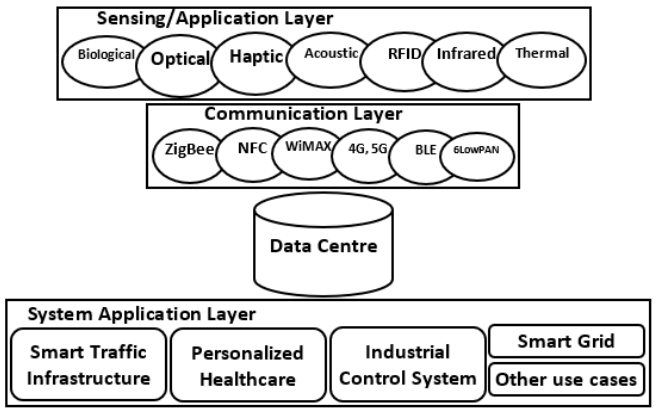

Fig. 1. Layered view of communication standards in IoT (adapted from [9]).

The figure showed some of the communication standards in use today which include but not limited to ZigBee, NFC, WiMAX, 4G, Bluetooth LE, 6LowPAN etc. These standards have several features which determine their selection in the production of diverse IoT devices. These features affect characteristics such as latency, range, throughput, the power consumption of the node, and security. As the IoT concept requires an increase in inter-communication and inter-operability of wireless communicating devices [10], it is important to consider various communicating standards which bring in diversities among devices that communication in an IoT ecosystem. Since these standards are not secure by design, finding a way to secure them becomes important.

So, it is important to consider these diversities, as well as the way they organize themselves in response to external factors or conditions, the level of agreement while interacting as well as the level of security that exist with a view to providing a secure way for their co-existence while protecting privacy of data generated by these devices.

A. Managing diversity within collective computing

Collective computing is a term describing scenarios where many computational devices collaborate and share resources with the aim of forming a solution for a single problem/many problems. The individual power of each machine is clustered to process computationally intensive tasks as may be required by pervasive devices and services [11]. The availability of a range of IoT devices has resulted in various implementations to address specific problems as determined by their design goals. This creates a scenario where an environment may adopt heterogeneous devices which each offer different capabilities [12]. Collective computing focuses on the amalgamation of pervasive and ubiquitous computing [13]. While systems are working towards autonomous operation, it is essential for them to be able to collaborate with each other to determine and incorporate capabilities provided by each device. There is usually a range of IoT devices in a typical ubiquitous setup [14] with various capabilities and functions, such as in smart environments by integrating devices within such environment. This heterogeneous nature is of vital importance while examining how such devices may co-exist and function in the ecosystem. Another important aspect is self-sufficiency [13] which is the ability of collective computing to perform an adequate function based on the resources available to it. This can be a situation where an IoT Ecosystem functions adequately and correctly irrespective of the situational circumstances and environmental conditions. Additionally, collective computing blurs differences between what is human and what are devices in order to provide a smooth working relationship [15]. Several accounts have shown that IoT devices existing in isolation has the tendency of reducing their effectiveness and further reduce the quality of the human-computation experience [16]. To build a stronger and effective community of varying devices, it is therefore important to manage these variations (called diversity) while building trust, confidentiality, and adequate risk awareness in the ecosystem and this will be one of the focuses of this research.

B. Self-organization within IoT solutions

As discussed in previous sections, many devices exist in an IoT ecosystem and there is a need for these devices to organize themselves for better productivity. Hence, self-organization enhances the interoperability of independent systems and should provide a basis for collective restructuring when subjected to different demands [17]. As seen in nature, a swarm of insects, herd of land animals, cells in an organism, and school of fish all display self-organization characteristics. So also, an array of artificial systems like the Internet of Things (IoT) related devices should exhibit, and leverage, self-organizing characteristics [18]. This enables the IoT system to perform the specific function it is designed to do while simultaneously providing a foundation to share resources in a manner which can support a variety of vertical use cases [19]. Self-organization will provide flexibility among autonomous IoT devices as they are expected to be part of many independent functional systems [20]. There are some scenarios [20] which are relevant to this project, one of which is a remote health monitoring system where sensors in a home measures temperature and humidity, alongside a heart monitor with these devices providing immediate logs to a cardiologist via the internet. Another scenario is that of sensors on solar panels communicating to a smart grid through a smart meter for energy efficiency. In these scenarios, there is the interplay of autonomous devices which can communicate and react according to their internal state. With self-organization, redundant devices can be securely introduced into the IoT Ecosystem to serve as failover in some unforeseen circumstances. This will re-task a device in a situation where one fails. This self-organizing feature will result in robustness and scalability of IoT use cases by increasing its functionalities, availability, and capacities [21]. IoT devices can collaborate to share resources as they organize themselves to enable energy efficiency, optimal system performance, redundant operation, quality of service (QoS), scalability, effective and responsive service delivery. This will also result in a reduction of demand for bandwidth and latency.

Due to these requirements, we must, therefore, research an approach that enables IoT devices to self-organize themselves within different use cases. This must be done, with some level of accountability incorporating adequate authentication checks and subsequent authorization in sharing their resources. Additionally, IoT devices should be held accountable for the resources and data they share. It is therefore important to

investigate how this could be achieved, for example, do they share resources safely, and in a non-repudiative manner so that each device can be accountable for their actions – even as they communicate. This will be an area of exploration for this research.

C. Planning and consensus within disparate IoT elements

Planning and consensus is a concept which differs self-organization mentioned above because before an organization can take place, there must be some sort of agreement between these devices and this is a function of how they interact in a heterogeneous setting [22]. While self-organizations investigate a whole network collaborating to achieve a goal, planning and consensus looked at the agreement at the heterogeneous device to device level [23]. Considering that a typical use case may consist of different types of IoT devices with each of them behaving differently over diverse communication networks to provide a service (or services) in an existing system or use case. The purpose of this is mainly to enhance the movement of data generated by these devices[23] [24]. Movement of data can be greatly enhanced or diminished based on the planning and consensus between elements in the IoT ecosystem. Several algorithms have been proposed by different researchers for distinct purposes. These algorithms do not follow a holistic approach to addressing security beyond interaction. Examples of these consensus algorithms are firefly[25], distributed containment control[26], forced bipartite[27], distributed flocking[28], constraint and projected[29], constant step-size gradient descent[30], proportional integral derivative and super twisting[31], uncertain linear[32], rate[33], and the ones based on swarm intelligence[34] among others. Each device senses things differently, for instance, a sensor might check for motion, some to measure temperature, while another humidity and they can exist in the same Wireless Sensor Network. For this network to exist and thrive, there are foundational requirements such as the following: Identification, Sensing, Communications, Computing, Services, and Semantics [35]. Identification and sensing involve obtaining data at the point of activity [36]. This usually includes identifying the object (virtual or physical) of interest. Communication is responsible for moving data from the sensing device typically to either the edge device or to the cloud, this is where communication technologies factor. Computing and services allow the aggregation of the data from different sources to support users and decision making. Semantics relates to making meaningful use of the data from the IoT elements such as an alarm going off in a scenario where a sensor detects smoke.

For this research, devices with a different level of complexity and computational resources will be explored alongside examining how data generated is transmitted through the communication medium, computed and storage as well as the possible resources and services they deliver across multiple use cases. Different existing scenarios will be studied, and a novel, simple and better unified consensus algorithm or method will be adopted in creating a co-existing and better means by which data is securely transferred between heterogeneous devices, i.e. the IoT elements.

D. Self-configured security within IoT Ecosystem

The proliferation and emergence of IoT devices have given rise to mass manufacturing of devices to meet up with the market demand and use cases. Attention is paid more to functionality as opposed to security [37]. In constrained IoT devices, it is common that lightweight security is used because of limited memory and processing capabilities. Communication protocols are also subject to compromise and can be a source of the attack to the IoT Network. Also, in some cases, fixes and updates are not automatically sent to devices [38], if they are still supported by the manufacturer at all. Additionally, these devices tend to be exposed to their environment, should they exist in a network which is mostly the case, they can become a point of attack in the IoT network [39]. Therefore IoT can provide functionality at the cost of increased vulnerability to malicious attacks or activities by an intruder [40]. These attacks include but are not limited to Denial of Service (DOS), Distributed Denial of Service (DDOS), Jamming, Spoofing, Intrusion, Malware, and eavesdropping[41]. Compounding this situation, the heterogeneous nature of IoT systems that may comprise hundreds of devices, which have diverse firmware images, Operating Systems (OS), and communication protocols which further complicating establishing security. For instance, if access is gained into a node within a Wireless Sensor Network, damage can be done to the whole network and as such the network will fail to achieve its aim at the detriment of the owner or the organization. Should the data from these sensors be reliant upon an actuator, a wrong decision or operation could then be performed. Hence, security becomes a challenge [42].

This study will, therefore, examine the existing security configuration within IoT Ecosystems, then attempt to proffer solutions to address these concerns which include vulnerabilities, privacy and other security domains as related to IoT devices, IoT OSs, protocols, connecting technologies, and their interoperability.

It could be noticed that each of the section reviewed above ends with some major issues that are of interest to this research. These are summarized in the section below in the form of research questions.

III. SUMMARY OF RESEARCH ISSUES

The following questions have emerged as targets for contribution to knowledge based on the initial investigations of several key research areas relevant to the study:

- Given the diversity of IoT devices, how is it possible to develop consensus within self-organizing systems to achieve a common goal?
- Given multiple use cases, can IoT solutions be harmonized and managed on a single platform?
- Is it possible to effectively manage varying IoT devices while building trust, confidentiality, and adequate risk awareness in the IoT ecosystem?
- Is it possible for IoT devices to share resources safely, and in a non-repudiative way so that each device can be accountable for their actions even as they communicate?
- How can security be maintained across IoT elements and ecosystems to protect privacy and safeguard them from vulnerabilities?

IV. AIM AND OBJECTIVES

The aim of this research is to improve the security, privacy, veracity, and trust based on non-repudiation of actions among self-organized IoT devices in an IoT Ecosystem.

This overall aim will be achieved through the following objectives:

- Identify and develop consensus algorithms which will manage self-organizing IoT ecosystems.
- Develop a prototype system to act as a testbed to be used throughout the project facilitating evaluation.
- Develop trust, confidentiality, and risk awareness models of IoT devices within an IoT Ecosystem.
- Develop a novel self-aware service that will maintain accountability of IoT devices within the Ecosystem.
- Develop a distributed system that will protect the privacy and secure IoT elements and ecosystems from vulnerabilities

V. PROPOSED RESEARCH APPROACH

Based on the research aim and objectives and identified research areas, the proposed system architecture is as shown in figure 2 below.

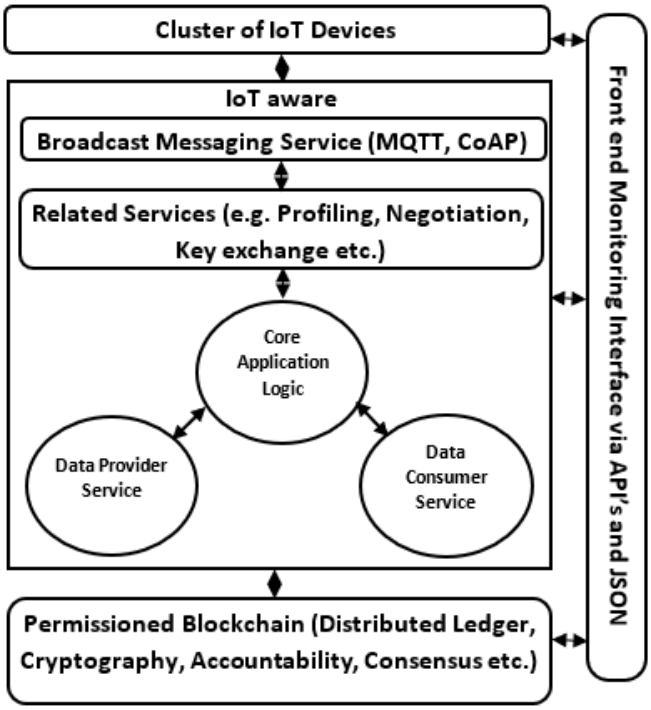

Fig. 2. Proposed System Architecture

This project leverage blockchain distributed ledger technology which provides inherent features such as immutability and, security. The core platform will be built to run both the data provider and consumer services which these connecting to the blockchain via respective API's. Other services that the IoT devices will interact with or consume can include broadcast messaging services which interact and handshake with various other services as shown.

VI. CONCLUSION

This research is still at its early stage. Therefore:

- The research issues aim and objectives will be the major focus of the research and will guide the work accordingly.
- Exploration of distributed ledger technology will occur to inform the implementation of the research by leveraging on its immutability, accountability, and other features.
- Concepts related to lightweight cryptography, encryption and decryption will be explored.
- An attempt will be made to create a novel aware service at the communication level of the IoT Ecosystem to provide end-to-end security.
- Detailed models, and architectures such as Risk Awareness Model, Implementation architectures will also emanate from this study.

REFERENCES

[1] H. Sundmaeker, P. Guillemin, P. Friess, and Sylvie Woelfflé, *Vision and Challenges for Realising the Internet of Things*, vol. 1, no. March. 2010.

[2] S. Singh, "Business Opportunities & Reference Architecture for E-commerce," *Int. Conf. Green Comput. Internet Things*, pp. 1577–1581, 2015.

[3] B. Al-Shargabi and O. Sabri, "Internet of Things: An exploration study of opportunities and challenges," *Proc. - 2017 Int. Conf. Eng. MIS, ICEMIS 2017*, vol. 2018–Janua, pp. 1–4, 2018.

[4] M. Aazam, S. Zeadally, and K. A. Harras, "Deploying Fog Computing in Industrial Internet of Things and Industry 4.0," *IEEE Trans. Ind. Informatics*, vol. 14, no. 10, pp. 4674–4682, 2018.

[5] S. Li, L. Da Xu, and S. Zhao, "The internet of things: a survey," *Inf. Syst. Front.*, vol. 17, no. 2, pp. 243–259, 2015.

[6] P. Maló, B. Almeida, and R. Melo, "Self-Organised Middleware Architecture for the Internet-of-Things," *IEEE Int. Conf. Green Comput. Commun. IEEE Internet Things IEEE Cyber, Phys. Soc. Comput.*, vol. 9, no. 2, pp. 445–451, 2013.

[7] D. Mendez, I. Papapanagiotou, and B. Yang, "Internet of Things : Survey on Security and Privacy," *IEEE Conf. Wirel. Sensors*, vol. 1, no. 2, pp. 1–16, 2017.

[8] Y. Chen, "Challenges & Opportunities in IoT," *IEEE Conf. Wirel. Sensors*, vol. 16, no. 12, pp. 383–388, 2012.

[9] A. Burg, A. Chattopadhyay, and K. Y. Lam, "Wireless communication and security issues for cyber- physical systems and the internet-of-things," *Proc. IEEE*, vol. 106, no. 1, pp. 30–60, 2018.

[10] R. Gunasagaran *et al.*, "Internet of things: Sensor to sensor communication," *2015 IEEE SENSORS - Proc.*, pp. 1–4, 2015.

[11] D. E. Boyle, M. E. Kiziroglou, P. D. Mitcheson, and E. M. Yeatman, "Energy Provision and Storage for Pervasive Computing," *IEEE Pervasive Comput.*, vol. 15, no. 4, pp. 28–35, 2016.

[12] Hui Lei, "Smarter pervasive computing," *2017 IEEE*

Int. Conf. Pervasive Comput. Commun., pp. 1–1, 2017.

[13] G. D. Abowd, "Beyond Weiser: From Ubiquitous to Collective Computing," *Computer (Long. Beach. Calif).*, vol. 49, no. 1, pp. 17–23, 2016.

[14] A. A. Mirani, M. S. Memon, N. M. Bhati, M. A. Soomro, and M. A. Rahu, "Taxonomy of Ubiquitous Computing: Applications and Challenges," *Int. Conf. Inf. Commun. Technol.*, pp. 202–208, 2017.

[15] A. Rajasekhar, N. Lynn, S. Das, and P. N. Suganthan, "Computing with the collective intelligence of honey bees – A survey," *Swarm Evol. Comput.*, vol. 32, pp. 25–48, 2017.

[16] I. Cavrak, I. Zagar, and A. Drazic, "Application models for ubiquitous systems with sporadic communication availability," *2017 40th Int. Conv. Inf. Commun. Technol. Electron. Microelectron. MIPRO 2017 - Proc.*, pp. 979–984, 2017.

[17] F. Oquendo, "Software Architecture of Self-Organizing Systems-of- Systems for the Internet-of-Things with SosADL," *IEEE 12th Syst. Syst. Eng. Conf.*, pp. 1–6, 2018.

[18] Y. Chuang, W. Yang, S. Lin, and T. Chiu, "Study and Implementation of the Smallest Closed-Area (SCA) Mechanism for Self-Organization Network Architectures in Smart Home Control Systems," *IEEE 17th Int. Symp. Consum. Electron.*, vol. 6, no. 13, pp. 79–80, 2013.

[19] W. Hu and H. Zhu, "A Methodology to Enable Self-organization in the Internet of Things Based on Negotiation Mechanism," *IEEE Int. Conf. Meas. Inf. Control*, vol. 2, no. 12, pp. 332–336, 2012.

[20] A. P. Athreya and P. Tague, "Network Self-Organization in the Internet of Things," *IEEE Int. Work. Internet-of-Things Netw. Control*, vol. 1, no. 13, pp. 25–33, 2013.

[21] B. Stefan, "Distributed Machine Learning with Self-organizing Mobile Agents for Earthquake Monitoring," *IEEE 1st Int. Work. Found. Self-Systems*, vol. 1, no. 16, pp. 126–132, 2016.

[22] S. S. Mathew, Y. Atif, and M. El-Barachi, "From the Internet of Things to the web of things-enabling by sensing as-A service," *Proc. 2016 12th Int. Conf. Innov. Inf. Technol. IIT 2016*, pp. 218–223, 2017.

[23] M. Nitti, V. Pilloni, G. Colistra, and L. Atzori, "The Virtual Object as a Major Element of the Internet of Things: A Survey," *IEEE Commun. Surv. Tutorials*, vol. 18, no. 2, pp. 1228–1240, 2016.

[24] S. K. Datta and C. Bonnet, "Securing datatweet IoT architecture elements," *2016 IEEE Int. Conf. Consum. Electron.*, no. i, pp. 1–3, 2016.

[25] C. Banerjee, S. Saxena, and I. Sharma, "Consensus achievement in multiagent system using adapted firefly algorithm," *Proc. 2014 2nd Int. Conf. "Emerging Technol. Trends Electron. Commun. Networking", ET2ECN 2014*, no. 3, pp. 1–4, 2015.

[26] Y. Cao, D. Stuart, W. Ren, and Z. Meng, "Distributed containment control for multiple autonomous vehicles with double-integrator dynamics: Algorithms and experiments," *IEEE Trans. Control Syst. Technol.*, vol. 19, no. 4, pp. 929–938, 2011.

[27] J. A. Guerrero and D. Olivares, "Forced Bipartite Consensus for Multi-Agent Systems," *IECON 2018 - 44th Annu. Conf. IEEE Ind. Electron. Soc.*, vol. 1, pp. 2335–2340, 2018.

[28] R. Olfati-Saberras, "Flocking for multi-agent dynamic systems: algorithms and theory," *IEEE Trans. Automat. Contr.*, vol. 51, no. 3, pp. 401–420, 2006.

[29] A. Ozdaglar, P. A. Parrilo, and A. Nedic, "Constrained Consensus and Optimization in Multi-Agent Networks," *IEEE Trans. Automat. Contr.*, vol. 55, no. 4, pp. 922–938, 2010.

[30] B. V. Philip, T. Alpcan, J. Jin, and M. Palaniswami, "Distributed Real-Time IoT for Autonomous Vehicles," *IEEE Trans. Ind. Informatics*, vol. 15, no. 2, pp. 1131–1140, 2018.

[31] E. G. Rojo-Rodriguez, E. J. Ollervides, J. G. Rodriguez, E. S. Espinoza, P. Zambrano-Robledo, and O. Garcia, "Implementation of a super twisting controller for distributed formation flight of multi-agent systems based on consensus algorithms," *2017 Int. Conf. Unmanned Aircr. Syst. ICUAS 2017*, pp. 1101–1107, 2017.

[32] M. Siami, S. Bolouki, B. Bamieh, and N. Motee, "Centrality measures in linear consensus networks with structured network uncertainties," *IEEE Trans. Control Netw. Syst.*, vol. 5, no. 3, pp. 924–934, 2018.

[33] F. Z. Zhang and H. Y. Yang, "Intelligent autonomous agents on fuzzy system," *Proc. - Int. Conf. Comput. Sci. Softw. Eng. CSSE 2008*, vol. 1, pp. 540–543, 2008.

[34] E. Bonabeau and G. Theraulaz, "Swarm Smarts," *Sci. Am. Inc.*, pp. 72–79, 2000.

[35] D. Navani, S. Jain, and M. S. Nehra, "The internet of things (IoT): A study of architectural elements," *Proc. - 13th Int. Conf. Signal-Image Technol. Internet-Based Syst. SITIS 2017*, vol. 2018–Janua, pp. 473–478, 2018.

[36] J. Voas, "Building blocks of the internet of things," *Proc. - 2016 IEEE Symp. Serv. Syst. Eng. SOSE 2016*, pp. 1–2, 2016.

[37] W. Zhou, Y. Zhang, and P. Liu, "The Effect of IoT New Features on Security and Privacy : New Threats , Existing Solutions , and Challenges Yet to Be Solved," *IEEE Internet Things J.*, pp. 1–11, 2018.

[38] D. Minoli, K. Sohraby, and B. Occhiogrosso, "IoT Security (IoTSec) Mechanisms for e-Health and Ambient Assisted Living Applications," *Proc. - 2017 IEEE 2nd Int. Conf. Connect. Heal. Appl. Syst. Eng. Technol. CHASE 2017*, pp. 13–18, 2017.

[39] S. Ray, T. Hoque, A. Basak, and S. Bhunia, "The Power Play : Security-Energy Trade-offs in the IoT Regime," *IEEE 34th Int. Conf. Comput. Des.*, vol. 2, no. 16, pp. 690–693, 2016.

[40] W. Wang, L. Yang, Q. Zhang, and T. Jiang, "Securing On-Body IoT Devices By Exploiting Creeping Wave Propagation," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 4, pp. 696–703, 2018.

[41] L. Xiao, X. Wan, X. Lu, Y. Zhang, and D. Wu, "IoT Security Techniques Based on Machine Learning," *IEEE Signal Process. Mag.*, vol. 35, no. 5, pp. 41–49, 2018.

[42] B. Duncan, M. Whittington, and V. Chang, "Enterprise

security and privacy: Why adding IoT and big data makes it so much more difficult," *Proc. 2017 Int. Conf. Eng. Technol. ICET 2017*, vol. 2018–Janua, pp. 1–7, 2018.