CLOUD COMPUTING, BLOCKCHAIN, AND IOT: A BLESSING OR CURSE?

Rania El-Gazzar, University of South-Eastern Norway, Rania.El-gazzar@usn.no

Karen Stendal, University of South-Eastern Norway, Karen.Stendal@usn.no

Abstract

Cloud computing, blockchain, and Internet of Things have gained considerable attention from industry and academia. The focus was on the benefits of using such technologies to do more with less i.e. improve work routines and enhance resource usage, as well as reduce costs. However, when the interest in combining the three technologies surfaced, several challenges appeared due to the conflicting nature of these emerging technologies. These challenges cannot be ignored, as they span technical, organizational, business, and legal aspects of organizations. In this paper, we discuss those challenges through selected literature. We conclude the paper with implications for research.

Keywords: Blockchain, Internet of things, Cloud computing, Challenges, Benefits.

1 Introduction

The ever-evolving nature of information technology (IT), with various software and infrastructure technologies, mandates organizations to innovate and keep their information systems (IS) up to date. The fast growing IT developments trick organizations to focus on the enticing benefits of emerging technologies and overlook the challenges behind their adoption. Such situations happen due to the lack of clear sight and awareness of the nature of the emerging technologies i.e. cloud computing, blockchain, and Internet of things (IoT). These three emerging technologies gain considerable attention from academia and organizations from various industries and sectors (Khan & Salah, 2018; Schneider & Sunyaev, 2014; Underwood, 2016; Yli-Huumo, Ko, Choi, Park, & Smolander, 2016).

The value propositions of cloud computing, blockchain, and IoT lures organizations to use them for executing business processes in a different and better way. In other words, the three emerging technologies are perceived to enable organizations to do more with less i.e. less time and effort. However, each one of the three emerging technologies poses technical, economic, organizational, and legal challenges that would elongate or hinder its adoption if overlooked (Asatiani, 2015; Papadopoulou, Kolomvatsos, Panagidi, & Hadjiefthymiades, 2017; Yli-Huumo et al., 2016). These challenges can be triggered from various sources, such as the nature of each emerging technology is conflicting with existing legacy systems and the staff skills (Venters & Whitley, 2012), current legal framework (Vegh, 2018; Weir, Aßmuth, Whittington, & Duncan, 2017), type of organization (e.g., public or private) (Ølnes, Ubacht, & Janssen, 2017), and the nature of the other technologies when combining the three together (Samaniego & Deters, 2016).

Definitions of the three emerging technologies are still undergoing discussions; further, their characteristics of openness and innovativeness pose complexities and risks to organizations despite their architecture deployments are tailored to various types of organizations (Mell & Grance, 2011;

Underwood, 2016). Furthermore, the marketing messages make emerging technology solutions, such as cloud computing, blockchain, and IoT appear as miraculous solutions to all the problems in organizations, and their magic will happen between day and night. This tends to trap managers and IT specialists into the ever-existing misbelief in the magical power of IT (Markus & Benjamin, 1997). Additionally, the threats to cloud computing, blockchain, and IoT develop at a higher speed than the developments of these three technologies. Industry reports indicate that the three emerging technologies are not considered completely mature yet (Buntz, 2016; IBM Institute for Business Value, 2016; Schulze, 2019), and, yet, serious security problems around them appear in the news headlines everyday (Bradbury, 2019; Chandhok, 2019; Spadafora, 2019). The adoption of cloud computing, blockchain, IoT, or combination of the three has its benefits and challenges for organizations at the technical, economic, organizational, and legal levels.

The aim of this paper is to synthesize those benefits and challenges and their triggering sources. Through our narrative review, we aim to contribute to the debate concerning benefits and challenges brought to organizations by each of the three emerging technologies and their combination. Therefore, our research question (RQ) is:

What are the benefits and challenges that cloud computing, blockchain, and IoT bring to organizations?

Narrative reviews are of great value for examining important and controversial topics, report on the current state of knowledge, and directing a further development in a domain area (King & He, 2005; Templier & Paré, 2015). In narrative reviews, researchers *"make judgments that support their own background, understanding, or established point-of-view"* (King & He, 2005, p. 667). Common characteristics of narrative reviews are that the researchers are free to select relevant papers to review and categorize research characteristics (King & He, 2005; Templier & Paré, 2015). There is no standard method to explicitly explain how the reviewed papers are search, selected, and synthesized in narrative reviews (Templier & Paré, 2015).

The paper is organized as follows: Section 2 provides a background on each of the three emerging technologies covering definitions, characteristics, deployment forms, benefits, challenges, and readiness assessment methods. Section 3 provides an overview of the differences and similarities between the three emerging technologies, as well as the benefits and challenges of combining them. In Section 4, we provide our interpretations and discuss the benefits and challenges by revisiting our RQ, then; we conclude the paper with implications for research and academia.

2 Background

To understand the benefits and challenges of each emerging technology, we provide an overview on the nature, definition, characteristics, and value proposition of each in the following sub-sections.

2.1 Cloud Computing

Cloud computing emerged as a successor of IT outsourcing model that has been around since the 1960s and took various forms of arrangements (Lacity, Khan, Yan, & Willcocks, 2010). The underlying computing technologies for cloud computing are virtualization and distributed computing technologies, such as clusters and grid computing (B. Armbrust et al., 2010; M. Armbrust et al., 2009; Buyya, Yeo, Venugopal, Broberg, & Brandic, 2009). Utility computing concept gave rise to the pay-per-use pricing model for using the shared IT resources in cloud computing environment (Bhargava & Sundaresan, 2004; Su, Akkiraju, Nayak, & Goodwin, 2009).

Buyya et al. (2009, p. 601) defined cloud computing as a type of parallel and distributed system consisting of a collection of inter-connected and virtualized computers that are dynamically provisioned and presented as one or more unified computing resource(s) based on service-level agreements established through negotiation between the service provider and consumers. Cloud computing model is more than dynamically provisioned IT resources; it provides ubiquitous on-demand access to those resources. Mell and Grance (2011, p. 2) defined cloud computing as a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

The shared environment of cloud computing model enables multi-tenancy by allowing multiple users to access a pool of virtual IT resources (i.e., infrastructure, development environments, and software) using computers, mobile phones, and tablets whenever needed without interacting with the cloud service provider (Mell & Grance, 2011). The location of the IT resources is only visible at the level of country, state, or data center, but not at the server level (Mell & Grance, 2011). The IT resources are adjusted to the demand and released automatically, as well as their usage is monitored, optimized, and controlled automatically (Mell & Grance, 2011). Cloud service models include, but not limited to, Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). These services can be deployed as public, private, or combination to serve a wide range of users with particular interests, such as governments, businesses, and individuals (Mell & Grance, 2011; Venters & Whitley, 2012).

The value proposition of cloud computing services is that organizations can lower their IT capital expenditures (i.e., hardware and software) and IT operating costs (i.e., administration and maintenance) by paying only for their use of on-demand IT resources (Garrison, Kim, & Wakefield, 2012). In cloud computing scenario, those IT capital expenses and operating costs shifted from the business and individual consumer to the cloud provider. Additionally, cloud computing model shifts the need for skilled IT personnel to maintain and secure the hardware and software from the consumer side, especially small and medium businesses, to the cloud provider side (Venters & Whitley, 2012). Therefore, businesses are able to dedicate their resources to core business activities instead of maintaining IT, which makes cloud computing "an IT-related strategy for competitive advantage" (Garrison et al., 2012). However, this does not apply to large businesses and governments, as they afford implementing their private cloud and acquire the necessary skills to maintain it (Venters & Whitley, 2012).

Although the shared IT environment of cloud computing model is the source of its innovativeness (Su et al., 2009), it is also the source of vulnerability (Coppolino, D'Antonio, Mazzeo, & Romano, 2017; Duncan, 2019). The shared IT environment of cloud computing model is enabled by the hypervisor component that is:

"The software layer that lies between virtual machines and the physical hardware, in charge of abstracting the underlying architecture. It is a fundamental part to guarantee the cloud multi-tenancy feature. It allocates physical resources to the guest Virtual Machines (VMs), such as main memory, CPU and peripherals. In terms of security, hypervisors should be considered as the most important layer to protect in the cloud stack, because they have the highest privilege and thus any command can be run from this space. Attackers can achieve full control of any resource of the host system if they alter or compromise the hypervisor (whose original goal was ensuring VMs isolation)." (Coppolino et al., 2017, p. 129)

The hypervisor is vulnerable to attacks from the employees of the consumer organization through the VMs created for them, external attackers through the network of the cloud infrastructure, or employees of the cloud provider who are responsible for maintaining the hypervisor (Coppolino et al., 2017). This can cause variety of attacks, such as Distributed Denial of Service (DDoS) attack, malware injection, spoofing, and sniffing attacks (Coppolino et al., 2017) that are still happening despite there are commercial solutions to address them (Suß, Freimuth, Aßmuth, Weir, & Duncan, 2019). Despite the cloud computing market being well-established the organizational concerns remain (Schulze, 2019). These concerns can be categorized into technical related to cloud computing model, organizational, economic, and environmental (Kauffman, Ma, & Yu, 2012).

Technical concerns stem from the immaturity of cloud computing model itself where data loss and leakage are reported as the top concerns (Schulze, 2019). Furthermore, unauthorized access and misuse of access controls, and insecure interfaces are perceived as top security vulnerabilities (Schulze, 2019). Economic concerns by consumer organizations relate to the maturity of cloud market; this includes standards, transparency, reputation, and financial stability of the cloud provider (Kauffman et al., 2012). It has been argued in the literature that cloud market is immature and volatile compared to the IT outsourcing market (Schneider & Sunyaev, 2014). The invisibility of cloud infrastructure is identified as a key concern for organizations and can be costly when addressing their legal compliance (Schulze, 2019). The hidden operational costs, time, and resources required to address interoperability issues are of considerable concern and mainly depend on the process maturity of the cloud provider (Durkee, 2010; Kauffman et al., 2012; Koehler, Anandasivam, & Dan, 2010). The hidden costs may be incurred due to poor selection of cloud services, bandwidth charges, etc. (Durkee, 2010).

The literature reported that the uncertain legal conditions are one of the environmental peculiarities of cloud computing (Schneider & Sunyaev, 2014). Environmental concerns fall into two directions; one is the speed that the legal frameworks develop to regulate the adoption of cloud computing, and the other is that compliance poses a challenge to consumer organizations (Kauffman et al., 2012; Schneider & Sunyaev, 2014). The trans-border legal conflicts between the USA and Europe have existed before the implementation of General Data Protection Regulation (GDPR) (Altorbaq, Blix, & Sorman, 2017; Seddon & Currie, 2013) and increased after the GDPR implementation (Duncan, 2018; Duncan & Zhao, 2019).

After the GDPR, the legal concerns regarding cloud computing include the right for the data subjects to give consent on have their data processed (i.e., collecting, storing, analyzing, altering, and deleting) in a lawful and transparent manner. Due to the exact location of the data not being visible (Mell & Grance, 2011; Schulze, 2019) and cloud service providers, which are the data processors, rely on third-party cloud providers for storing data (El-Gazzar, Hustad, & Olsen, 2016) the compliance with GDPR becomes a challenge (Duncan, 2019; Gobeo, Fowler, & Buchanan, 2018). The cloud shared environment, which is enabled by the hypervisor, is vulnerable to the “cloud forensic problem” (Duncan, 2018). This forensic problem happens when the attacker gains access to the hypervisor and escalate privileges to be able to modify or delete data stored on the cloud and the log trail to clean up the traces of their actions on the stored data (Duncan, 2018, 2019; Duncan & Zhao, 2019). This cloud forensic problem makes it difficult to comply with GDPR since the breach action traces are deleted; thus, the cloud service provider will not be able to have immediate oversight whether a breach happened or not and which records have been affected (Duncan & Zhao, 2019). Consequently, the cloud service provider will not be able to report the breach in a short time to the data controller, so that the data controller can notify the supervisory authority within 72 hours according to GDPR requirements (Duncan, 2019).

Organizational concerns regarding cloud computing include size of the organization, type of organization, IT capabilities, strategic focus of organizations, experience in changing work policies and operational routines smoothly (Kauffman et al., 2012; Schneider & Sunyaev, 2014). The skills of IT personnel become more focused on cloud service integration and negotiation of service level agreements (SLAs) (Abdelmaboud, Jawawi, Ghani, Elsafi, & Kitchenham, 2015; Garrison et al., 2012; Schneider & Sunyaev, 2014). Regarding service integration, a recent report indicates that misconfiguration is among the top concerns by consumer organizations (Schulze, 2019).

2.2 Blockchain

Blockchain has gained a considerable attention to understand its benefits for various domain areas (Avital, King, Beck, Rossi, & Teigland, 2016; Underwood, 2016). Blockchain is argued to have a significant impact on the business model of organizations, both cutting costs and offering efficiency, while adding other costs and risks (Morkunas, Paschen, & Boon, 2019). Blockchain is known as distributed ledger technology, where users add transactions by means of creating a block with assigned cryptographic hash, timestamp, and transaction data (Ølnes et al., 2017; Swan, 2015; Underwood, 2016). Each block created is sent to each participant in the blockchain to be verified through the proof-of-work consensus mechanism. Further, the block is chained to other blocks that are stored in the distributed ledger and shared with the participants on their computers in a transparent manner (Swan, 2015; Underwood, 2016). The distributed ledger is decentralized and not owned or controlled by a central trusted authority, and the consensus mechanism, or validation of transactions, is decentralized as well (Ølnes et al., 2017; Swan, 2015; Underwood, 2016).

Blockchain builds on peer-to-peer networks, cryptographic methods, and distributed systems (Johansen, 2018; Ølnes et al., 2017; Swan, 2015). Blockchain models are known as public permissionless and private permissioned (Underwood, 2016). Public permissionless blockchain is open to anyone to join, not controlled by a central authority, and ensures user anonymity (Walsh et al., 2016). The validation of transactions is decentralized in private permissioned blockchain (Rückeshäuser, 2017). Private permissioned blockchain is limited to predefined trusted users with known identity, and a central authority controls it (Hans, Zuber, Rizk, & Steinmetz, 2017; Walsh et al., 2016). Therefore, the validation of transactions is centralized in private permissioned blockchain (Rückeshäuser, 2017).

The value proposition of blockchain resides in its transparency and decentralization (Alexopoulos, Charalabidis, Androutsopoulou, Loutsaris, & Lachana, 2019; Johansen, 2018). Decentralization reduces the need for a central authority to eliminate its dominant control and avoid having a single point of failure (Al-megren et al., 2018; Alexopoulos et al., 2019; Johansen, 2018). Every user node in the blockchain has a copy of the data; therefore, there is no single point of failure (Johansen, 2018; Mosakheil, 2018) as it is the case of the hypervisor in cloud environment (Coppolino et al., 2017; Neumann, 2014; A. Singh & Chatterjee, 2017). The decentralized validation of transactions using consensus mechanism helps reducing corruption (Risius & Spohrer, 2017). Additionally, the goal of blockchain is to cut out the transaction costs through automated logic of transaction contracts and validation routines based on predefined rules (Beck & Müller-Bloch, 2017). The fact that blockchain is immutable makes it attractive to organizations to ensure the integrity of the data and ensure traceability of the history of the transactions, especially public permissionless blockchain that is more open and growing in nodes, which makes it hard to alter the data (Mosakheil, 2018).

The source of innovation in blockchain is in its decentralization, automation, and consensus mechanism (Beck & Müller-Bloch, 2017; Johansen, 2018; Risius & Spohrer, 2017). However, these sources of innovation are sources of technical and architecture vulnerabilities at the same time (Mosakheil, 2018). The consensus mechanism is prone to DDoS attack (Sayeed & Marco-Gisbert, 2019) and double-spending attack (i.e., 51% attack) that is likely to happen in private permissioned blockchain (Mosakheil, 2018). The openness and decentralization of public permissionless blockchain, being not controlled by a central authority, makes it prone to lack of control in address creation and flawed key generation threats (Mosakheil, 2018). Smart contracts are prone to program design flaws (Mosakheil, 2018).

Blockchain is still immature technology and undergoing experimentation stage despite organizations perceive the values it adds to their business (Angelis & Ribeiro da Silva, 2019; Deloitte, 2019). A recent industry report highlighted the top barriers to adoption of blockchain as perceived by organizations (Deloitte, 2019). These barriers are regulatory issues, implementation issues (i.e., replacing or integrating with legacy systems), security threat, uncertain return on investment, lack of skills and understanding, concern about sensitive information, the challenge of forming a consortia, lack of compelling applications, and the perception that it is unproven technology. The literature reported further scalability barrier (i.e., limited capacity to process transactions per second and many blocks are stored in each node in the blockchain network) (Al-megren et al., 2018; Alexopoulos et al., 2019). Other barriers are the legal applicability with GDPR regarding data subject rights, lack of standardized blockchain architectures, expensive specialized personnel, and the energy-consuming consensus mechanism (Al-megren et al., 2018; Alexopoulos et al., 2019; Morkunas et al., 2019).

The legal conflict that is commonly discussed in the literature is the records that are stored in the distributed ledger cannot be deleted, which is the opposite to the subject right to be forgotten under the GDPR (Herian, 2018; Ølnes et al., 2017). Even if there is a possibility for workaround to make blockchain GDPR-compliant (Farshid, Reitz, & Roßbach, 2019), it is not completely meeting the legal requirement for deleting the data when it is no longer needed. Hence, legal issues are number one barrier to the adoption of blockchain (Deloitte, 2019). Consequently, the current situation with blockchain is witnessing many pilots and experiments with blockchain (Morkunas et al., 2019), in addition to the difficulty to form consortia due to the challenge of dealing the shift in mindset and regulatory risk factors (Deloitte, 2019).

2.3 Internet of Things (IoT)

The term IoT was first introduced in 1999 by the MIT Auto-ID Labs, which is a research group specialized in networked Radio Frequency IDentification (RFID) and sensing technologies (Gubbi, Buyya, Marusic, & Palaniswami, 2013).

Gubbi et al. (2013, p. 1647) gave the IoT a rather broad definition as the *"interconnection of sensing and actuating devices providing the ability to share information across platforms through a unified framework, developing a common operating picture for enabling innovative applications. This is achieved by seamless ubiquitous sensing, data analytics and information representation with cloud computing as the unifying framework"*.

IoT enables Machine-to-Machine communication (M2M) and builds on real-time analytics, pervasive computing, machine learning and embedded devices (Atzori, Iera, & Morabito, 2017; Gubbi et al., 2013). The core elements of IoT as stated by Gubbi et al. (2013) are the hardware components (i.e., sensors, actuators and embedded communication devices), storage and computing resources to perform data analytics, and visualization and interpretation tools that can be accessed on different platforms and used by different applications. The design challenges of IoT are (Papadopoulou et al., 2017): (1) the heterogeneity of the devices made by different manufacturers has consequences on the connection between those devices. (2) lack of standards to address the different formats of annotating the data and devices. (3) the ecosystem of IoT lacks specific roles for stakeholders to create new relationships in new industrial sectors (i.e., industrial consortia).

IoT is positioned behind blockchain in the hype cycle for emerging technologies and it is in the stage of experimentation (Panetta, 2018). The value proposition of IoT for organizations and nations is that it increases productivity, improves quality of life, enables process automation, provides context-specific applications, enables real-time generation of rich data, etc. (Papadopoulou et al., 2017). However, there are major issues that affect the realization of those values (Buntz, 2016; Papadopoulou et al., 2017); these include privacy, security attacks, interoperability as a result of device heterogeneity, high cost of implementation, inadequate infrastructure, technological immaturity in storing and processing massive amount of data, and inadequate regulatory frameworks. Additionally, it became a trend in cyberattacks after the DYN attack in October 2016 (Shim et al., 2018), which was the largest attack of its kind in history. The attack involved 100,000 malicious endpoints overwhelming the DYN's Internet domain name system (DNS) infrastructure with a distributed denial of service attack (DDoS). Furthermore, the source of innovation in IoT is the M2M communication and real-time analytics (Atzori, Iera, & Morabito, 2010; Gubbi et al., 2013). However, it is still a source of security vulnerability, as there are still security problems with M2M communication (Tuna et al., 2017) and resource efficiency and scalability problems (Atzori et al., 2010).

CC is the infrastructure technology for IoT that enables storing and processing the vast amount of data generated from different devices (Atzori et al., 2017). This takes the legal issues regarding GDPR to a higher level of complexity given the issues with IoT. This includes storing and processing data collected by devices from different manufacturers, not directly by the infrastructure providers providers (Atzori et al., 2017; Shim et al., 2018). Additionally, those devices have storage utilities embedded by the manufacturers (Atzori et al., 2017). Furthermore, the use of big data analytics means that the devices collect a massive amount of data, which raises concerns about the subject right to give a consent on the data collected (Pham, 2019).

3 Putting All Together

After presenting the key benefits and challenges of each individual technology, we review the benefits and challenges of combining these technologies in the following sub-sections.

3.1 Cloud Computing and Blockchain

The security problems in cloud computing environment we discussed earlier are claimed to be resolved by blockchain technology (Park & Park, 2017; Zhao & Duncan, 2018). Blockchain technology can address the known cloud forensic problem inherent in the hypervisor vulnerabilities, where the attacker can delete all traces of an attack from the cloud environment (Liang et al., 2017; Tosh et al., 2017). Using Blockchain technology, any transactions data are stored and are difficult to delete due to the consensus mechanism of blockchain, especially the public permissionless blockchain (Zhao & Duncan, 2018). Therefore, all actions conducted in the cloud environment are recorded; thus, cloud providers can spend less time in discovering the attacks and comply with GDPR by being able to notify the supervisory authority within 72 hours (Zhao & Duncan, 2018). This blockchain solution requires distributing the blockchain ledgers over several locations and cloud instances. Thus, it becomes difficult for the attacker to tamper with the transactions data, because the larger the number of blockchain nodes the difficult to alter the data (Makhdoom, Abolhasan, Abbas, & Ni, 2019; Zhao & Duncan, 2018). This blockchain solution to the security and legal issues in the cloud forensic problem comes with a price. Having blockchain ledgers distributed at a wide-scale increases performance costs i.e. more latency problems (Zhao & Duncan, 2018).

Key management and cryptography are not strong in cloud computing, as the cloud virtual environment can be compromised and its instances can be controlled with escalated privileges (Coppolino et al., 2017). This problem can be resolved through consensus and cryptographic mechanisms provided by blockchain to allow for secure identity management, authentication, validation of user authentication (Bendiab, Kolokotronis, Shiaeles, & Boucherkha, 2018; Park & Park, 2017), as well as authorization to access and use cloud services and charging for cloud usage through smart contracts (Nayak, Narendra, Shukla, & Kempf, 2018).

3.2 Cloud Computing and IoT

The relationship between cloud computing and IoT is bidirectional, in terms of benefits and challenges they bring to each other. The challenges and benefits of cloud-based IoT encompass security vulnerabilities, legal and privacy issues, and performance (Makhdoom et al., 2019). IoT increases the cloud forensic problem due to IoT devices have limited memory capacity and can be exploited by the attackers to access the cloud's virtual environment and gain access to sensitive data (Duncan & Zhao, 2019). This makes it difficult to discover and trace any breaches (Duncan & Zhao, 2019). Therefore, the cloud service providers would face a major challenge in complying with GDPR, as they will need to spend longer time to discover the breach and notify the supervisory authority (Duncan & Zhao, 2019). Furthermore, through IoT devices, an attacker can launch a DDoS attack and exhaust the cloud servers, causing performance issues to the cloud environment (Duncan & Zhao, 2019). The fact that IoT devices energy-constraints and may be unreachable by the RFID reader is a challenge that can be addressed by cloud computing virtual environment (Atzori et al., 2017). Cloud computing can be a beneficial alternative to enable creating virtual instances of the physical IoT devices in so-called cloud of things, Sensing and Actuation as a Service (SAaaS), or Thing as a Service (TaaS) (Atzori et al., 2017).

The limited memory storage and processing power of IoT devices can benefit from the scalable storage and computing resources in the cloud environment (Makhdoom et al., 2019). However, cloud cannot guarantee the immutability of the data being stored due to the hypervisor vulnerability (Makhdoom et al., 2019). The scalable computing power of cloud servers provides a better data analytics feature for the real-time data sent from the heterogeneous IoT devices (Makhdoom et al., 2019). Though, at a certain point the IoT requirements for high availability, real-time data delivery, scalability, security, and resilience will pose a major challenge for the cloud environment (Makhdoom et al., 2019). The increase of IoT devices connected to the cloud infrastructure may cause latency due to distant locations of IoT devices and the processing of massive data received from them (Yousefpour et al., 2019). Additionally, IoT can pose a major challenge for the cloud environment, as the likelihood of DDoS attacks, data breaches, manipulations to the data or the virtual machines becomes higher (Khan & Salah, 2018). IoT shares the same issues with cloud computing regarding authentication and authorization, but for things and not people or organizations i.e. unique identification of IoT devices (Khan & Salah, 2018). The cloud insecure interfaces pose a further security challenge for accessing IoT services (Khan & Salah, 2018).

3.3 Blockchain and IoT

Blockchain is computationally expensive and typically consumes massive network resources due to its consensus mechanism, which may not be an ideal infrastructure technology for IoT and pose latency and scalability issues (Dorri, Kanhere, & Jurdak, 2017). However, security and privacy issues in IoT can be resolved by blockchain through its the peer-to-peer decentralized architecture as well as cryptographic security and immutability benefits (i.e., distributed ledger, authentication, and anonymity and possibly pseudonymity because of the hashing) (CMS LAW, 2019; Lyons, Courcelas, & Timsit, 2018; Makhdoom et al., 2019). Security benefits brought to IoT by blockchain include strong cryptographic mechanisms to manage the identity of things, as well as secure communication between things and provide effective authentication and authorization using smart contracts (Khan & Salah, 2018; Makhdoom et al., 2019). However, blockchain can transform its majority attack (i.e., 51% attack), where the trusted node that controls 51% of the computing resources becomes the attacker's node causing data manipulation to happen (Makhdoom et al., 2019). Consequently, the security of IoT is at risk, in terms of data integrity and availability.

3.4 Cloud Computing, Blockchain, and IoT

Combining the three technologies resolves the issues in each technology for the other through so-called fog computing (Makhdoom et al., 2019). Fog computing emerged as a heirachical technology to facilitate the connection between the cloud and IoT devices by enabling computing, storage, networking, and data management on network nodes within the neighbourhood of IoT devices (Yousefpour et al., 2019). The cloud-to-IoT connection is enabled by edge computing, which is a decentralized peer-to-peer (P2P) network (Yousefpour et al., 2019). The P2P network addresses reliability issues related to Internet connectivity between IoT devices and the cloud; each node in the P2P network is called fog node (Makhdoom et al., 2019). Edge computing is placed between the IoT devices and the cloud infrastructure, and it provides small data centers within the fog nodes or cloudlets (Yousefpour et al., 2019). These small data centers bring network, computing and storage resources closer to the IoT devices (Makhdoom et al., 2019). However, fog nodes have, yet, vulnerabilities related to insecure communication, authentication, privacy and data integrity (Yousefpour et al., 2019). Furthermore, those fog nodes have limited computational resources but low latency.

To solve the authentication and privacy issues in fog computing, blockchain can be beneficial in managing identity management through smart contracts (Ahmad, Abdul Razak, Kannan, Yusof, & Muhamad Amin, 2018). Blockchain benefits extend to recording fog resource transactions, service provisioning and ensure data integrity through smart contracts as well (Ali, Wang, Bhuiyan, & Jiang, 2018; Sharma, Chen, & Park, 2018; Yousefpour et al., 2019). However, it has been a challenge whether the blockchain deployment is better hosted on the cloud or the fog, as blockchain consumes numerous computation resources (Samaniego & Deters, 2016; Sharma et al., 2018; S. Singh, Ra, Meng, Kaur, & Cho, 2019). Fog nodes have limited computational resources, but low latency in collecting and process IoT data, while the cloud infrastructure provides scalable resources, but higher latency (Samaniego & Deters, 2016).

4 Discussion, Conclusion, and Implications

In this paper, we provided a narrative review that commenced with the definition and characteristics of cloud computing, blockchain, and IoT. We reviewed the benefits and challenges that these three emerging technologies bring to organizations; each technology had a value proposition for organizations to offer benefits with the promise for doing things in a better manner, but also brought challenges to organizations (See summary in Table 1). Then, we reviewed four combinations of the three technologies to identify whether the challenges and benefits of combining two or the three technologies would generate more problems or solve problems in each technology (See summary in Table 2). Thus, we revisit our research question:

What are the benefits and challenges that cloud computing, blockchain, and IoT bring to organizations?

To answer our question at the level of each technology, we find the benefits and challenges from each technology stem from their innovative characteristics as per Table 1. These characteristics are the shared IT environment in the case of cloud computing, consensus mechanism in the case of blockchain, and the IoT devices that collect and generate real-time massive data. The benefits from cloud computing are mainly related to efficiency in operating the business. The benefits from blockchain put more emphasis on security. The benefits from IoT are more related to effectiveness in using rich data for increasing productivity and quality of life goals. However, the challenges brought by blockchain and IoT are more complex than cloud computing, as their market is not well-established as cloud computing. We find that blockchain and IoT are less mature than cloud computing; there are still uncertainties about investing in blockchain and IoT due to their immaturity, higher implementation costs, and lack of industrial consortia. This opens the opportunity for researchers to empirically question: *what are the challenges that hinder the wide establishment of industrial consortia for blockchain and IoT?* This can be related to the unresolved technical challenges from blockchain and IoT i.e. security, performance, scalability, and energy consumption as per Table 1. The security vulnerability in the hypervisor of the cloud shared environment has been, and is still, existing challenge (Coppolino et al., 2017) that is likely to raise a legal challenge concerning the inability to conduct audit trails and notify the supervisory authority of a breach within 72 hours (Duncan, 2019). This implies the need for more experiments on these technical challenges involving researchers and industry practitioners.

	Cloud computing	Blockchain	Internet of Things
Innovative Characteristics	-Shared environment of scalable virtual IT resources enabled by the hypervisor -Centralized architecture -Geographically distributed -Utilized on-demand -Paid per use -Automatically provisioned -Various service models (SaaS, PaaS, IaaS, etc.) -Deployed as public or private or combination	-Decentralized P2P architecture (no single point of failure) - Distributed ledger -Relies on cryptographic methods -Immutability of transaction data records - Transparency - Decentralized/centralized consensus mechanism to validate blocks of transactions -Deployed as public permissionless or private permissioned (managed by central authority) -Automated logic of transaction contract and validation routines	-M2M communication architecture based on pervasive computing -Embedded devices -Real-time analytics -Machine learning
Benefits	-Reduced IT capital expenditures -Outsourcing IT skills -More focus on core business activities	-Reduced transaction costs -Reduced corruption -Ensured data privacy and integrity -Ensured traceability of transactions	-Increased productivity -Improved quality of life -Context-specific applications -Generation of rich real-time data
Challenges	-*Technical:* security vulnerabilities in the hypervisor (single point of failure) and cloud forensic problem. -*Legal:* GDPR compliance issues related location of data and traceability of attacks -*Economic:* hidden costs related to addressing compliance and interoperability issues, poor service selection, bandwidth charges -*Organizational:* related to the size and type of organization, shift from in-house skills to service integration (misconfiguration can happen) and service level negotiation	-*Technical:* Security issues (decentralized consensus mechanism is prone DDoS attack and centralized consensus mechanism is prone to 51% attack). Lack of standards. Implementation issues. Unproven technology. Scalability issues. Program design flaws. Key generation flaws. Energy consumption by consensus mechanism. -*Legal:* compliance issues related to the immutability in contrast with the right to be forgotten under GDPR -*Organizational:* related to investment uncertainties. Expensive skilled personnel -*Business:* lack of formed consortia	-*Technical:* connection issues du to heterogeneity of devices. Interoperability issues due to lack of standards. Vulnerability to DDoS attacks. Device limitations (connection, authentication and data integrity issues). Scalability issues in the long run due to the massive real-time data generated. -*Economic:* high implementation costs -*Legal:* inadequate legal frameworks. Complex legal issues regarding processing data and the right to give consent under GDPR -*Business:* lack of formed consortia

Table 1. Overview of benefits and challenges from each emerging technology.

The legal challenges brought by each of the three emerging technologies are as dominant as the technical challenges, and they stem from the innovative characteristics of each technology. These challenges are not, yet, resolved. Such challenges expensive for organizations whether in the case of compliance or non-compliance with GDPR. Previous comprehensive literature reviews on the three technologies focused mainly on technical and organizational challenges (Atzori et al., 2010, 2017; Gubbi et al., 2013; Makhdoom et al., 2019; Schneider & Sunyaev, 2014; Upreti, Asatiani, & Malo, 2016). Legal aspects regarding the three technologies deserve further review and empirical research efforts. This provides opportunities for research to contribute to identifying the areas of conflict/harmony in the three emerging technologies with the legal requirements and data subject rights under GDPR.

Furthermore, the uncertainties around investing in blockchain and IoT can be related to many organizations do not have the competence to decide whether they need blockchain or not (Wüst & Gervais, 2018), or that they need to shift their view of IoT as a general technology wave to become more critical and identify relevant use cases (Hung, 2017). These concerns provide opportunities for further empirical research. Additionally, future research could question, *what are the good or bad use cases, especially for blockchain and IoT?* There have been failure cases of blockchain projects with no impact due to the misalignment of business needs with the technical capabilities of blockchain (ICTworks, 2018; Vota, 2018). In this regard, organizations need to ask more questions when adopting any of the three emerging technologies than just how they work, such as why these technologies and what they can do compared to previous situation (ICTworks, 2018).

There are even more challenges arising from combining cloud computing, blockchain, and IoT (Samaniego & Deters, 2016; Uriarte & De Nicola, 2018) that need to be addressed by future research. When combining two or three technologies, further patterns emerged as per Table 2. The benefits from each technology may address the challenges inherent in the other. For example, the immutability of transaction data of blockchain solves the cloud forensic problem and, consequently, solves its compliance issues. On the other hand, the challenges from one technology increases the challenges from the other. For example, the security limitations of IoT devices increase the severity of the cloud forensic problem, which complicates its compliance with GDPR. Thus, the legal issues deserve further examination regarding the adoption of one or more of the three technologies we addressed in this paper, especially regarding GDPR. Performance issues are dominant in the four combinations of the three technologies and research is, yet, needed in this area (Khan & Salah, 2018; Makhdoom et al., 2019; Samaniego & Deters, 2016).

Cloud computing (CC) and blockchain (BC	**BC and IoT**
(+)	(+)
-BC can, through its immutability, address the CC forensic problem and the compliance issues related to the forensic problem	-BC can address authentication and data privacy and integrity in IoT through its immutability and its cryptographic and key management mechanism
-BC can, through its consensus and cryptographic mechanisms, address the vulnerabilities inherent in the hypervisor to protect is from being controlled by the attacker	
(-)	(-)
BC can bring performance costs and latency problems to CC environment	-BC is a resource-consuming technology and not an ideal infrastructure for IoT
	-BC can bring 51% attack to IoT platform, threatening data integrity and availability

CC and IoT	**CC, BC, and IoT**
(+) -CC can address IoT device limitations by providing scalable storage and processing resources to IoT devices to process the rich real-time data received from the IoT devices - CC can also address IoT device limitations by enable creating virtual instances of IoT devices -CC insecure interfaces pose a security challenge for accessing IoT services (-) -IoT increases the CC forensic problem due to IoT devices that can be exploited by the attackers to access the CC environment, complicating the compliance issues for CC -IoT can bring more advanced DDoS attacks causing performance issues to the CC environment -Increasing IoT devices and real-time data generated by them can challenge the scalability of CC -CC cannot guarantee addressing authentication and data integrity issues in IoT	(+) -CC provides infrastructure for IoT platform -BC can secure the authentications of IoT devices and the communication between the IoT devices and CC (-) -CC-to-IoT communication is unreliable, and it is enabled by fog nodes in the middle -BC is resource consuming and hosing it on CC or the fog nodes poses performance challenges

Table 2. Overview of benefits (+) and challenges (-) that each technology brings to the other.

The identified benefits and challenges from combining the three technologies provide implications for further empirical examination of the implementation mix of the three technologies with focus on three issues; these are security, compliance, and performance. Combining the three technologies to address one issue (e.g., security) comes at the expense of the performance or compliance (Duncan & Zhao, 2019; S. Singh et al., 2019). Organizations need to understand the escalated challenges from combining the three technologies and assess whether they are ready for the implementation mix, as perceiving the benefits of IT innovations is not enough for the IT-enabled transformation of organizations (Markus & Benjamin, 1997). Further research needs to look into the development of frameworks to assess how ready is an organization to implement more than one IT solution from emerging technologies and address the consequent challenges from the combinations we discussed in our paper. Additionally, lessons learned from early adopters of each or combination of the three technologies are worthy to report on from practitioners and not only put focus on the benefits. Further research needs to identify good and bad use cases regarding the implementation of solutions combining cloud computing, blockchain, and/or IoT, as the potential risks are higher for such complex implementations (Gill et al., 2019; Mittal, Kuder, & Hans, 2019).

This paper has methodological and empirical limitations due to its nature as a narrative review (Templier & Paré, 2015). We did not have an explicit methodology for our review; we reviewed selected papers to convey our point-of-view in trying to synthesize the benefits and challenges from the three emerging technologies at the level of each individual technology and comparative pairings. Future systematic literature reviews with similar focus will be provide substantial contributions to knowledge. We did not rely on empirical data for our paper; however, we built the synthesis of benefits and challenges from the three technologies based on selected empirical and review articles, and suggested future research agenda accordingly.

References

Abdelmaboud, A., Jawawi, D. N. A., Ghani, I., Elsafi, A., & Kitchenham, B. (2015). Quality of service approaches in cloud computing: A systematic mapping study. *Journal of Systems and Software*, *101*, 159–179.

Ahmad, N. M., Abdul Razak, S. F., Kannan, S., Yusof, I., & Muhamad Amin, A. H. (2018). Improving Identity Management of Cloud-Based IoT Applications Using Blockchain. In *Proceedings of the 2018 International Conference on Intelligent and Advanced System (ICIAS)*.

Al-megren, S., Alsalamah, S., Altoaimy, L., Alsalamah, H., Soltanisehat, L., Almutairi, E., & Pentland, A. (2018). Blockchain Use Cases in Digital Sectors : A Review of the Literature. In *Proceedings of the 2018 IEEE Conference on Internet of Things, Green Computing and Communications, Cyber, Physical and Social Computing, Smart Data, Blockchain, Computer and Information Technology, Congress on Cybermatics*.

Alexopoulos, C., Charalabidis, Y., Androutsopoulou, A., Loutsaris, M. A., & Lachana, Z. (2019). Benefits and Obstacles of Blockchain Applications in e-Government. In *Proceedings of the 52nd Hawaii International Conference on System Sciences*.

Ali, S., Wang, G., Bhuiyan, M. Z. A., & Jiang, H. (2018). Secure data provenance in cloud-centric internet of things via blockchain smart contracts. In *Proceedings of SmartWorld/UIC/ATC/ScalCom/CBDCom/IoP/SCI 2018*.

Altorbaq, A., Blix, F., & Sorman, S. (2017). Data Subject Rights in the Cloud: A Grounded Study on Data Protection Assurance in the Light of GDPR. In *2017 12th International Conference for Internet Technology and Secured Transactions (ICITST 2017)*.

Angelis, J., & Ribeiro da Silva, E. (2019). Blockchain Adoption: A Value Driver Perspective. *Business Horizons*, *62*(3), 307–314.

Armbrust, B., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A., Lee, G., … Rabkin, A. (2010). A View of Cloud Computing. *Communications of The ACM*, *53*(2), 50–58.

Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A., … Zaharia, M. (2009). Above the Clouds : A Berkeley View of Cloud Computing.

Asatiani, A. (2015). Why Cloud? - A Review of Cloud Adoption Determinants in Organizations. In *the 23rd European Conference on Information Systems*.

Atzori, L., Iera, A., & Morabito, G. (2010). The Internet of Things: A survey. *Computer Networks*, *54*(15), 2787–2805.

Atzori, L., Iera, A., & Morabito, G. (2017). Understanding the Internet of Things: Definition, Potentials, and Societal Role of a Fast Evolving Paradigm. *Ad Hoc Networks*, *56*, 122–140.

Avital, M., King, J. L., Beck, R., Rossi, M., & Teigland, R. (2016). Jumping on the Blockchain Bandwagon: Lessons of the Past and Outlook to the Future. In *Proceedings of the 37th International Conference on Information Systems*.

Beck, R., & Müller-Bloch, C. (2017). Blockchain as Radical Innovation: A Framework for Engaging with Distributed Ledgers. In *Proceedings of the 50th Hawaii International Conference on System Sciences*.

Bendiab, K., Kolokotronis, N., Shiaeles, S., & Boucherkha, S. (2018). WiP: A Novel Blockchain-Based Trust Model for Cloud Identity Management. In *Proceedings of DASC/PiCom/DataCom/CyberSciTech*.

Bhargava, H. K., & Sundaresan, S. (2004). Computing as Utility: Managing and Pricing Commitment , Availability , Bid Auctions Through Contingent. *Journal of Management Information Systems*, *21*(2), 201–227.

Bradbury, D. (2019). Cloud computing Giant PCM Hacked. Retrieved August 22, 2019, from https://nakedsecurity.sophos.com/2019/07/01/cloud-computing-giant-pcm-hacked/

Buntz, B. (2016). Top 10 Barriers for Adoption of the Internet of Things. Retrieved August 22, 2019, from https://www.iotworldtoday.com/2016/04/20/top-10-reasons-people-aren-t-embracing-iot/

Buyya, R., Yeo, C. S., Venugopal, S., Broberg, J., & Brandic, I. (2009). Cloud Computing and Emerging IT Platforms: Vision, Hype, and Reality for Delivering Computing as the 5th Utility. *Future Generation Computer Systems*, *25*(6), 599–616.

Chandhok, A. (2019). Top Five Blockchain Security Issues in 2019 — LedgerOps. Retrieved August 22, 2019, from https://ledgerops.com/blog/2019/03/28/top-five-blockchain-security-issues-in-2019

CMS LAW. (2019). *The Tension Between GDPR and the Rise of Blockchain Technologies*.

Coppolino, L., D'Antonio, S., Mazzeo, G., & Romano, L. (2017). Cloud Security: Emerging Threats and Current Solutions. *Computers and Electrical Engineering, 59*(2017), 126–140.

Deloitte. (2019). *Deloitte's 2019 Global Blockchain Survey: Blockchain Gets Down to Business. Deloitte*.

Dorri, A., Kanhere, S. S., & Jurdak, R. (2017). Towards an Optimized BlockChain for IoT. In *Proceedings of the Second International Conference on Internet-of-Things Design and Implementation (IoTDI '17)*.

Duncan, B. (2018). Can EU general Data Protection Regulation Compliance be Achieved when Using Cloud Computing? In *Proceedings of the Ninth International Conference on Cloud Computing, GRIDs, and Virtualisation (CLOUD COMPUTING 2018)*.

Duncan, B. (2019). EU General Data Protection Regulation Compliance Challenges for Cloud Users. In *Proceedings of the Tenth International Conference on Cloud Computing, GRIDs, and Virtualization (CLOUD COMPUTING 2019)*.

Duncan, B., & Zhao, Y. (2019). Cloud Compliance Risks. In *The Tenth International Conference on Cloud Computing, GRIDs, and Virtualization (CLOUD COMPUTING 2019)*.

Durkee, D. (2010). Why Cloud Computing Will Never Be Free. *Communications of the ACM*, *53*(5), 62–69.

El-Gazzar, R., Hustad, E., & Olsen, D. H. (2016). Understanding cloud computing adoption issues: A Delphi study approach. *Journal of Systems and Software*, *118*, 64–84.

Farshid, S., Reitz, A., & Roßbach, P. (2019). Design of a Forgetting Blockchain: A Possible Way to Accomplish GDPR Compatibility. In *Proceedings of the 52nd Hawaii International Conference on System Sciences*.

Garrison, G., Kim, S., & Wakefield, R. L. (2012). Success Factors for Deploying Cloud Computing. *Communications of the ACM*, *55*(9), 62–68.

Gill, S. S., Tuli, S., Xu, M., Singh, I., Singh, K. V., Lindsay, D., … Garraghan, P. (2019). Transformative Effects of IoT, Blockchain and Artificial Intelligence on Cloud Computing: Evolution, Vision, Trends and Open Challenges. *Internet of Things*, *8*, 100118.

Gobeo, A., Fowler, C., & Buchanan, W. (2018). *GDPR and Cyber Security for Business Information Systems*.

Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems*, *29*(7), 1645–1660. https://doi.org/10.1016/j.future.2013.01.010

Hans, R., Zuber, H., Rizk, A., & Steinmetz, R. (2017). Blockchain and Smart Contracts: Disruptive Technologies for the Insurance Market. In *Proceedings of Twenty-third Americas Conference on Information Systems (AMCIS 2017)*.

Herian, R. (2018). Regulating Disruption: Blockchain, GDPR, and Questions of Data Sovereignty. *Journal of Internet Law*, *22*(2), 8–16.

Hung, M. (2017). *Leading the IoT: Gartner Insights on How to Lead in a Connected World*. Retrieved from https://www.gartner.com/imagesrv/books/iot/iotEbook_digital.pdf

IBM Institute for Business Value. (2016). *Healthcare Rallies for Blockchains*.

ICTworks. (2018). Four Lessons Learned Launching Blockchain Financial Services for NGOs - ICTworks. Retrieved from https://www.ictworks.org/lessons-learned-blockchain-financial-services/#.Xah5VOgzZaQ

Johansen, S. K. (2018). A Comprehensive Literature Review on the Blockchain Technology as an Technological Enabler for Innovation. Department of Information Systems, Mannheim University. Retrieved from https://www.researchgate.net/publication/312592741

Kauffman, R. J., Ma, D., & Yu, M. (2012). A Metrics Suite for Firm-Level Cloud Computing Adoption Readiness. In *Proceedings of the 11th International Conference Grid Economics and Business Models (GECON 2014)*. Springer, Cham.

Khan, M. A., & Salah, K. (2018). IoT Security: Review, Blockchain Solutions, and Open Challenges. *Future Generation Computer Systems*, *82*(2018), 395–411.

King, W. R., & He, J. (2005). Understanding the Role and Methods of Meta- Analysis in IS Research. *Communications of the Association of Information Systems*, *16*(1), 665–686.

Koehler, P., Anandasivam, A., & Dan, M. A. (2010). Cloud Services from a Consumer Perspective. In *AMCIS 2010 Proceedings*.

Lacity, M. C., Khan, S., Yan, A., & Willcocks, L. P. (2010). A Review of the IT Outsourcing Empirical Literature and Future Research Directions. *Journal of Information Technology*, *25*(4), 395–433.

Liang, X., Shetty, S., Tosh, D., Kamhoua, C., Kwiat, K., & Njilla, L. (2017). ProvChain: A Blockchain-Based Data Provenance Architecture in Cloud Environment with Enhanced Privacy and Availability. In *Proceedings of the 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing*.

Lyons, T., Courcelas, L., & Timsit, K. (2018). *Blockchain and the GDPR: A Thematic Report by the European Union Blockchain Observatory and Forum*. Retrieved from https://www.eublockchainforum.eu/sites/default/files/reports/20181016_report_gdpr.pdf

Makhdoom, I., Abolhasan, M., Abbas, H., & Ni, W. (2019). Blockchain's Adoption in IoT: The Challenges, and a Way Forward. *Journal of Network and Computer Applications*, *125*(2019), 251–279.

Markus, M. L., & Benjamin, R. I. (1997). The Magic Bullet Theory in IT-Enabled Transformation. *Sloan Management Review*, *38*, 55–68.

Mell, P., & Grance, T. (2011). The NIST Definition of Cloud Computing: Recommendations of the National Institute of Standards and Technology.

Mittal, N., Kuder, D., & Hans, S. (2019). *Tech Trends 2019: Beyond the Digital Frontier*. Retrieved from https://www2.deloitte.com/content/dam/Deloitte/br/Documents/technology/DI_TechTrends2019.pdf

Morkunas, V. J., Paschen, J., & Boon, E. (2019). How Blockchain Technologies Impact your Business Model. *Business Horizons*, *62*(3), 295–306.

Mosakheil, J. H. (2018). *Security Threats Classification in Blockchains*. *Culminating Projects in Information Assurance*. Retrieved from https://repository.stcloudstate.edu/msia_etds/48

Nayak, S., Narendra, N. C., Shukla, A., & Kempf, J. (2018). Saranyu: Using Smart Contracts and Blockchain for Cloud Tenant Management. In *Proceedings of the 2018 IEEE 11th International Conference on Cloud Computing (CLOUD).*

Neumann, P. G. (2014). Risks and Myths of Cloud Computing and Cloud Storage. *Communications of the ACM*, *57*(10), 25–27.

Ølnes, S., Ubacht, J., & Janssen, M. (2017). Blockchain in Government: Benefits and Implications of Distributed Ledger Technology for Information Sharing. *Government Information Quarterly*, *34*(3), 355–364.

Panetta, K. (2018). 5 Trends Emerge in the Gartner Hype Cycle for Emerging Technologies, 2018 - Smarter With Gartner. Retrieved from https://www.gartner.com/smarterwithgartner/5-trends-emerge-in-gartner-hype-cycle-for-emerging-technologies-2018/

Papadopoulou, P., Kolomvatsos, K., Panagidi, K., & Hadjiefthymiades, S. (2017). Investigating The Business Potential Of Internet Of Things. In *MCIS 2017 Proceedings*.

Park, J. H., & Park, J. H. (2017). Blockchain Security in Cloud Computing: Use Cases, Challenges, and Solutions. *Symmetry*, *9*(8), 1–13.

Pham, P. L. (2019). The Applicability of the GDPR to the Internet of Things. *Journal of Data Protection & Privacy*, *2*(3), 254–263.

Risius, M., & Spohrer, K. (2017). A Blockchain Research Framework. *Business & Information Systems Engineering*, *59*(6), 385–409.

Rückeshäuser, N. (2017). Do We Really Want Blockchain-Based Accounting? Decentralized Consensus as Enabler of Management Override of Internal Controls. In *Proceedings of the 13th International Conference on Wirtschaftsinformatik*.

Samaniego, M., & Deters, R. (2016). Blockchain as a Service for IoT. In *Proceedings of the 2016 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*.

Sayeed, S., & Marco-Gisbert, H. (2019). Assessing Blockchain Consensus and Security Mechanisms Against the 51% Attack. *Applied Sciences*, *9*(9), 1–17.

Schneider, S., & Sunyaev, A. (2014). Determinant Factors of Cloud-Sourcing Decisions: Reflecting on the IT Outsourcing Literature in the Era of Cloud Computing. *Journal of Information Technology*, *31*(1), 1–31.

Schulze, H. (2019). *Cloud Security Report*. Retrieved from https://www.isc2.org/-/media/ISC2/Landing-Pages/2019-Cloud-Security-Report-ISC2.ashx?la=en&hash=06133FF277FCCFF720FC8B96DF505CA66A7CE565

Seddon, J. J. M., & Currie, W. L. (2013). Cloud Computing and Trans-Border Health Data: Unpacking U.S. and EU Healthcare Regulation and Compliance. *Health Policy and Technology*, *2*(4), 229–241.

Sharma, P. K., Chen, M. Y., & Park, J. H. (2018). A Software Defined Fog Node Based Distributed Blockchain Cloud Architecture for IoT. *IEEE Access*, *6*(2018), 115–124.

Shim, J. P., Avital, M., Sheng, O., Sorensen, C., Dennis, A. R., Rossi, M., & French, A. M. (2018). Internet of Things: Opportunities and Challenges to Business, Society, and IS Research. In *Proceedings of the 38th International Conference on Information Systems*.

Singh, A., & Chatterjee, K. (2017). Cloud security issues and challenges: A survey. *Journal of Network and Computer Applications*, *79*, 88–115.

Singh, S., Ra, I. H., Meng, W., Kaur, M., & Cho, G. H. (2019). SH-BlockCC: A secure and efficient Internet of Things Smart Home Architecture Based on Cloud Computing and Blockchain Technology. *International Journal of Distributed Sensor Networks*, *15*(4), 1–18. https://doi.org/10.1177/1550147719844159

Spadafora, A. (2019). IoT Attacks are the "New Normal." Retrieved August 22, 2019, from https://www.techradar.com/news/iot-attacks-are-the-new-normal

Su, N., Akkiraju, R., Nayak, N., & Goodwin, R. (2009). Shared Services Transformation : Conceptualization and Valuation from the Perspective of Real Options. *Decision Sciences*, *40*(3), 381–402.

Suß, F., Freimuth, M., Aßmuth, A., Weir, G. R. S., & Duncan, B. (2019). Cloud Security and Security Challenges Revisited. In *Proceedings of the Tenth International Conference on Cloud Computing, GRIDs, and Virtualization (CLOUD COMPUTING 2019)*.

Swan, M. (2015). *Blockchain: Blueprint for a New Economy* (First Edit). O'Reilly Media.

Templier, M., & Paré, G. (2015). A Framework for Guiding and Evaluating Literature Reviews. *Communications of the Association for Information Systems*, *37*(1), 112–137.

Tosh, D., Shetty, S., Tosh, D. K., Liang, X., Kamhoua, C. A., Kwiat, K. A., & Njilla, L. (2017). Security Implications of Blockchain Cloud with Analysis of Block Withholding Attack. In *Proceedings of the 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing*.

Tuna, G., Kogias, D. G., Gungor, V. C., Gezer, C., Taşkın, E., & Ayday, E. (2017). A Survey on Information Security Threats and Solutions for Machine to Machine (M2M) Communications. *Journal of Parallel and Distributed Computing*, *109*, 142–154.

Underwood, S. (2016). Blockchain Beyond Bitcoin. *Communications of the ACM*, *59*(11), 15–17.

Upreti, B. R., Asatiani, A., & Malo, P. (2016). To Reach the Clouds: Application of Topic Models to the Meta-review on Cloud Computing Literature. In *the 49th Hawaii International Conference on System Sciences (HICSS)*.

Uriarte, R. B., & De Nicola, R. (2018). Blockchain-Based Decentralized Cloud/Fog Solutions: Challenges, Opportunities, and Standards. *IEEE Communications Standards Magazine*, *2*(3), 22–28.

Vegh, L. (2018). A Survey of Privacy and Security Issues for the Internet of Things in the GDPR Era. In *Proceedings of the 2018 International Conference on Communications (COMM)*.

Venters, W., & Whitley, E. a. (2012). A Critical Review of Cloud Computing: Researching Desires and Realities. *Journal of Information Technology*, *27*(3), 179–197.

Vota, W. (2018). Blockchain Use Case Failure: 43 Projects and Zero Impact Found. Retrieved October 17, 2019, from https://www.ictworks.org/blockchain-impact-failure/#.Xah4g-gzZaQ

Walsh, C., O'Reilly, P., Gleasure, R., Feller, J., Li, S., & Cristoforo, J. (2016). New Kid on the Block: A Strategic Archetypes Approach to Understanding the Blockchain. In *Proceedings of the Thirty Seventh International Conference on Information Systems*.

Weir, G., Aßmuth, A., Whittington, M., & Duncan, B. (2017). Cloud Accounting Systems, the Audit Trail, Forensics and the EU GDPR: How Hard Can It Be? In *Proceedings of the British Accounting and Finance Association: Scottish Area Group Annual Conference*.

Wüst, K., & Gervais, A. (2018). Do you Need a Blockchain? In *Proceedings of the 2018 Crypto Valley Conference on Blockchain Technology (CVCBT)* (pp. 45–54).

Yli-Huumo, J., Ko, D., Choi, S., Park, S., & Smolander, K. (2016). Where Is Current Research on Blockchain Technology?-A Systematic Review. *PloS One*, *11*(10), 1–27.

Yousefpour, A., Fung, C., Nguyen, T., Kadiyala, K., Jalali, F., Niakanlahiji, A., … Jue, J. P. (2019). All One Needs to Know about Fog Computing and Related Edge Computing Paradigms: A Complete Survey. *Journal of Systems Architecture*, *98*(2019), 289–330.

Zhao, Y., & Duncan, B. (2018). Could Block Chain Technology Help Resolve the Cloud Forensic Problem?. In *Proceedings of Cloud Computing*.