Securely Driving IoT by Integrating AIOps and Blockchain

Alexandru Cristian GHEORGHIȚĂ[1,2], Ionuț PETRE[1,3]
[1]National Institute for Research and Development in Informatics – ICI Bucharest
[2]Politehnica University of Bucharest
[3]"Lucian Blaga" University of Sibiu
alexandru.gheorghita@rotld.ro, ionut.petre@rotld.ro

Abstract: The IoT networks are growing more complex each year. With this growth comes the cost of managing and monitoring all the devices present inside the network and the rise of concern regarding the security and privacy that can be ensured. This challenge can be overcomed by making use of the latest technologies available, AIOps and Blockchain. We will explore these technologies, how they are being successfully used on Cloud systems and how they can be molded to drive more complex networks such as the IoT.

Keywords: AIOps, IoT, blockchain, secure IoT

INTRODUCTION

In recent years, we have witnessed the transformation of the Internet of Things (IoT) from a concept to reality and to a major priority for many companies. More and more IoT devices are integrated in network infrastructures to collect more data and create new or improved experiences for the end-users. IoT has been defined as "a global infrastructure for the information society, enabling advanced services by interconnecting physical and virtual things based on existing and evolving interoperable information and communication technologies" *[Internet of Things Global Standards Initiative, 2015]*. In the light of technological innovations, the impact of intelligently leveraged data is now globally recognized and accepted. The innovations in IT have impact on some of the world's biggest challenges – improving healthcare and education, handle climate changes, proper use of natural resources, data privacy, quality of life – will depend on effectively understanding and acting on data *[Splunk, 2020]*.

Smart devices connect in manufacturing, industrial settings, production lines, travel, health systems, vehicles and transport systems, offices and homes. Even though the Covid-19 pandemic had impacted IoT heavily, it is predicted that global spending on the IoT will have a back to double-digit growth and rebound is expected to happen both in the mid and long-term. According to International Data Corporation, the IoT spending growth was 8.2% year over year to $742 billion in 2020 down from 14.9% growth forecast in November 2019, but it is expected that global IoT spending will return to double-digit growth rates in 2021. The predictions estimate that by 2025 there will be 55.9 billion connected devices, with about three

Fig. 1: *Connected world [source: Badhok, 2020]*

quarters of them connected to an IoT platform. Moreover, the data from connected IoT devices will reach a stunning value of 79.4 Zettabytes by 2025, six times higher than the volume of data generated in 2019, which is 13.6 Zettabytes.

When a new device is connected to the Internet, it can send and/or receive information. In IoT, a smart device can gather data, receive data and act based on that data or it can do both of them. IoT grew primarily due to the widespread use of sensors that can collect data from their environment and send it – such as sensors for air quality, temperature, light, traffic, motion etc. Now sensors are everywhere and most times we do not think about them. A smartphone is more than a phone with internet connection, it is a device packed with sensors (GPS, camera etc.) but it is way more than just a collection of sensors.

IoT will need new methods for addressing key challenges in security and reliability, focusing on the ability of the system to prevent itself from failing by continuously introspecting its own state and take decisions without human intervention *[Boncea, 2016]*.

Aggregating Big Data, Machine Learning, Analytics and Automation is increasingly, even widely, recognized amongst IT leaders as having enough potential to transform monitoring and event management and drive significant benefits across IT Operations processes *[Brink, 2019]*. In the digital society, ensuring system reliability and reducing workload on IT teams can be a key factor for economic success. Members of these teams can be assigned for developments or other tasks rather than manual monitoring.

In the past decade, the term *digital society* has been widely used to describe the society, but innovations appear faster and on a wider range than ever before. Therefore, we can state that the digital society is continuously transforming. A major part of these IT transformations was generated by the DevOps methodologies, Cloud Computing and by the large interest of the market in adopting technological developments. We are witnessing changes in the technological areas, from centralized IT towards external apps and development teams, from classic development to a fast-forward Agile innovation, development and deployment, a broad adoption of machine agents, IoT devices, web services, etc. The bundle of new technologies and devices are raising challenges for organizations as their service management strategies and tools are often not prepared to handle new infrastructure development.

Artificial Intelligence for IT operations – AIOps is the ITOps paradigm shift required to handle these digital transformation issues. It refers to multi-layered technology platforms that automate and enhance IT operations through analytics and machine learning *[Paskin, 2020]*. As presented in ***Figure 2***, AIOps encloses three different IT concepts:

- Engage – IT service management – the activities carried out by an organisation to design, plan, operate and control informational services towards their clients.
- Observe – IT monitoring – gather metrics about the operations performed in an IT environment (both hardware and software), such as CPU usage, application response times, API usage stats, memory loads etc. The goal is to ensure the availability and proper functioning of IT equipment.
- Act – Automation – automate tasks by routing workflows with or without human intervention.

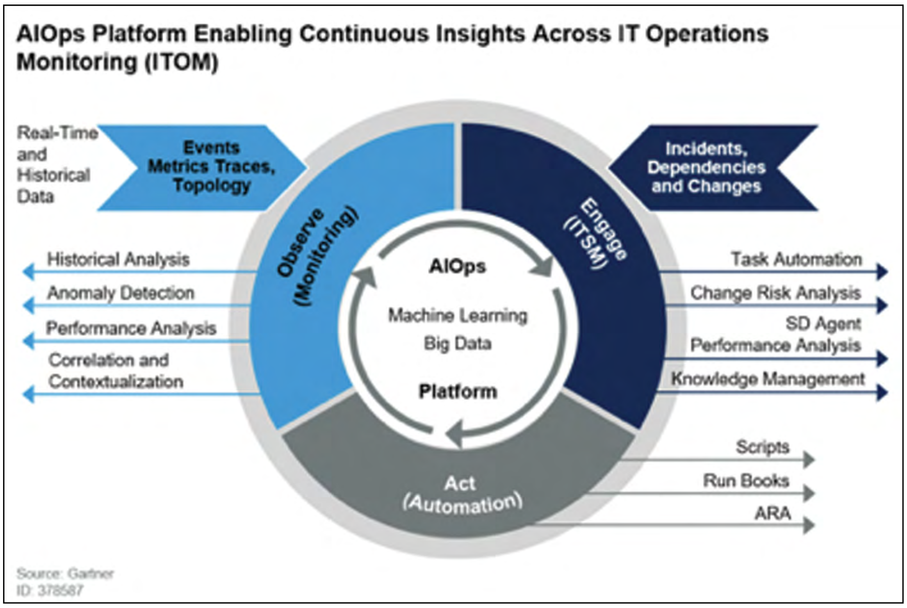

Fig. 2: *AIOps Platform Enabling continuous insights across IT operations [source: Gartner, 2019]*

Increase accuracy by continuously learning with the goal of solving issues before reaching to end-users.

An AIOps platform combines big data with machine learning or AI; it collects data and metrics from IT operations with the goal to detect issues automatically and react to those issues in real-time, while it still provides historical analytics.

AIOps revolves around two main concepts: Big Data and Machine learning. It requires a move away from isolated IT data towards aggregation of observational data (such as data from monitoring systems, variety of sensors, job logs, etc.) and engagement data (ticketing systems, incident and event recording) inside a big data platform. AIOps then implements a comprehensive analytics and ML strategy against the combined IT data *[Paskin, 2020]*.

AIOPS AND CLOUD INFRASTRUCTURES

To better understand how AIOps can improve the management of large IoT infrastructures, we must look at how this technology is currently being used in large cloud infrastructures.

Cloud computing is now a ubiquitous and mature technology. According to (IDG, 2020) 92% of an organization's IT environment is present in some way in the cloud and with more than 55% of these organizations using multiple such public clouds.

To maintain such complex systems, a large team of IT specialists must constantly check large amounts of logs and statistics to detect service outages caused by failing software or hardware. This task is difficult and costly, and it can at most recover the lost data or restore the normal functioning of the systems if there are enough specialists available at the time of the incident. Each year a company loses 1.55 million dollars because of service downtime and more than 14 hours of productivity loss *[ERS, 2018]*.

AIOps solutions for Cloud infrastructure promise to lower the costs and downtime of services by understanding the functioning of these large systems and providing DevOps personnel a more understandable view across the vast amount of data that is being produced each second.

Common types of failures in Cloud infrastructures

Storage

The storage allows data to be persisted over time and in a cloud infrastructure setup it can be accessed globally by each computing node in the system. Cloud storage systems are made up of virtual machines that emulate physical servers allowing for homogenous storage solutions to be provided.

Failures on this layer could be prevented by monitoring and analyzing each component's health. This task involves gathering all the logs and metrics produced by each node and identifying potential malfunctioning behavior. The resulting amount of data is too large to be analyzed by IT specialists, making it hard to detect potential problems.

Network

Cloud networking tends to be more complex than traditional enterprise network layouts. A public cloud such as AWS or Azure can be made up of more than 50.000+ servers that run in physical containers while private clouds use considerably less servers but still must interface with the traditional enterprise design. The traditional approach to enterprise networking involves a lot of equipment from different providers that can lack in homogeneity which makes it more difficult to monitor, manage and recover from a failure.

Cloud systems use virtualized appliances that run over physical containers emulating the same type of network devices. This system makes it easy to deploy, manage and scale the network whenever there is a need without any physical intervention from the IT specialists. Another benefit of having virtualized appliances is the ease of configuration when creating a network from scratch and the homogeneity of logs that are produced over time. This allows for a more consolidated data set of logs that could provide valuable information when a failure occurs.

Security

The cloud computing security concerns are not different from traditional computing. The machines that compose the cloud system can still be vulnerable if they are not properly maintained and updated. As more companies are migrating their infrastructure into the cloud, they are bringing along many of the risks that plague the traditional enterprise systems. Poorly written applications or deficient implementations of security policies are some of the causes that born security issues. While analyzing the top threats of cloud computing, the most occurred security issues are as follows *[Enisa, 2009, Mather, 2009]*:

- Abuse and Unallowed Use of Cloud Computing;
- Insecure Application Programming Interfaces;
- Malicious Insiders;
- Shared Technology Vulnerabilities;
- Data Loss and Leakage
- Account, Service and Traffic Hijacking;
- Unknown Risk Profile.

All the above-mentioned threats can be translated into metrics that can be used to identify and analyze potential vulnerabilities that can endanger the system and its valuable data.

Traditional infrastructure monitoring tools

Traditional enterprise infrastructure IT specialists rely on a multitude of tools to collect and analyze the data produced by appliances and applications. Most of the tools collect the metrics, they compare them with some pre-defined thresholds and if the values are above these thresholds, the system starts to alert the assigned IT specialists. What these systems lack is the possibility to foresee and prevent failures before they actually happening.

We will explore some of the most popular monitor solutions on the market.

Datadog

It features integrations with most popular cloud infrastructure providers, it provides extensive dashboards for monitoring different metrics (hardware, software and financial)

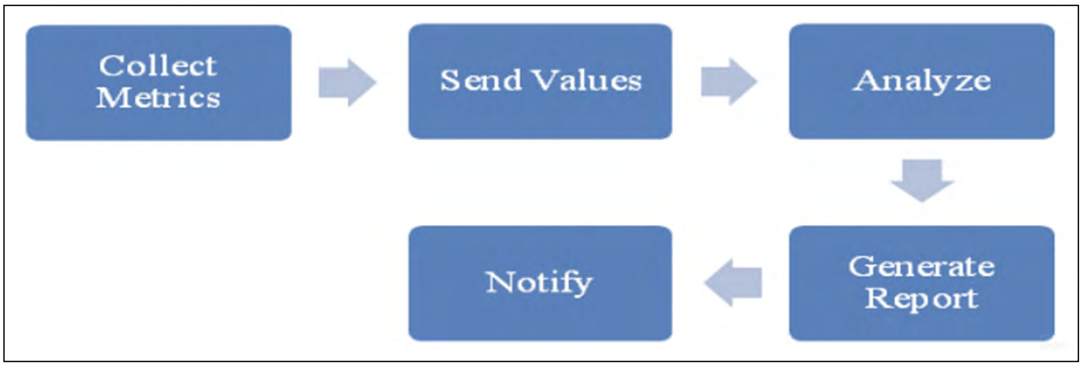

Fig. 3: Fault Monitoring Process

and it offers a public SDK with which one can develop custom integrations for specific applications. The downside of using this system is the need of special training of the personnel and it stores large amounts of data that can be hard to process.

Nagios

Nagios is one of the veteran platforms that dates from 2002 making it one of the more popular choices among IT specialists. It offers monitoring and alerting services for servers, switches, applications and services. When something goes wrong with any of the monitored system it alerts the system administrators and it also alerts when the system is back on-line and fully functioning.

The issue with Nagios is that it only alerts when some thresholds are being passed. There is no dashboard where data can be analyzed in order to form predictions about future failures.

AIOps Cloud infrastructure solutions

Although the traditional monitoring systems are providing valuable data to the IT specialists to analyze, practice has shown that most of the time the focus is shifted towards the wrong metrics leading the specialist on false paths regarding the origin of the failure. This happens mainly because of the large data sets that need to be filtered and analyzed manually and because of the many different appliances and software that are found inside a cloud infrastructure.

By deploying an AIOps monitoring tool the data generated by the cloud subsystems are automatically interpreted resulting in a more concise view of the problem and a more targeted and fast response from the IT specialists. This is accomplished by employing machine learning algorithms *[StackOverFlow, 2019]* on the logs produced by all the software/appliances available in the cloud allowing for long-term patterns to be created that in turn will create a broader view of the incidence of failures.

Although AIOps is a rather new concept, several companies are already starting to offer services for cloud infrastructures.

Watson AIOps

IBM Watson AIOps *[IBM, 2020]* combines deep learning and comprehension of natural language to compare organized and unstructured data in real time throughout toolchain operations to reveal concealed knowledge and help more easily locate root causes. Watson AIOps feeds feedback and suggestions directly into the workflows of the team to speed event response by eliminating the need for multiple dashboards.

Splunk

Splunk solution *[Splunk – AIOps, 2020]* is based on data that has been gathered in time from different IT infrastructures to better create a ML (machine learning) model. Splunk can ingest nearly any kind of data, like logs, metrics, text, wire, API, and even social media derived, just to name a few, and from nearly any tool and system. After gathering all this disparate data into one single silo, an AI will start to make correlations that could result in useful predictions regarding the systems health and general functioning state.

Moogsoft AIOps

Moogsoft AIOps *[Moogsoft, 2020]* solution offers integration to most cloud infrastructure systems, thus unifying all the heterogeneous data into a more manageable homogeneous data set available under a single dashboard. This leads to a better monitoring and recovery from a potential failure.

AIOps for IoT infrastructures

Traditional IoT incidents monitoring

Generally, IoT networks are comprised of thousands of sensors and devices that can generate streaming data which can be analyzed in a specialized data center. It is not unusual for one of these sensors to break down and when this happens, the gateway to which the sensor is connected, starts to send signals to the data center about the failing sensor. Usually the generated alerts are processed by a human or an automated service that will dispatch an on-site team to fix the broken sensor. This system is slow and laborious when the sensors are in especially remote locations and it doesn't offer any prediction model that would allow the IT specialists to foresee this type of incidents.

Another approach would be to analyze all the logs that are being produced by the sensors and by applying statistical models one can start to visualize vulnerable spots inside the network and take appropriate actions. The process involves extensive data sets that need to be processed in order to obtain an understandable status quo which can delay decision making resulting in a slow and costly operation.

Using AIOps in IoT environment

Analyzing and using extensive data to produce viable predictions can grow resilience and overall availability of the network. Interchanging the human factor with specialized AI can considerably speed up the interpretation of logs and events that are constantly produced by the IoT network. AIOps can also provide more focused and solutions to incidents and can also form up the appropriate IT specialists team that should carry out the repairs.

One other important aspect that IoT networks can benefit from AIOps solutions is the ability to create predictions for each sensor and establish a more concise maintenance plan in order to prevent future failures that in turn will result in an overall cost saving for the network provider.

OMG (Object Management Group) is a non-profit organization known for developing industry standards, especially in the area of data interchange, that already created a special Artificial Intelligence Platform Task Force (AIPTF) that will look into standardizing data and communication inside large networks. This will benefit further AIOps since it will allow for a more homogenous data that will be easier to create AI models from.

Although AIOps and IoT integration is at its infancy, judging by the constant growing of IoT networks and rapid appearance of smart cities, AIOps and IoT represents the perfect synergy.

BLOCKCHAIN IN IOT

Blockchain is a technology based on the concept that digital information should be distributed but not replicated. Blockchain is a set of data records that is not backward-altered, but permanently increased with new records. The data chain is distributed throughout the Internet ecosystem and there is no device meaning that has the complete chain. Instead, each node that has a copy of the chain. The chain cannot be modified; past records are not altered – new records add to the chain after being validated by nodes.

A blockchain consists of two types of elements *[Banafa, 2016]*:

- Transactions – which are the actions created by the participants.
- Blocks – record the transactions and ensure that those records are in the correct sequence and have not been tampered with. Blocks also record a timestamp when the transactions were added.

When a new transaction is added to the chain, the transaction is validated by all the participating nodes by applying an algorithm, defined by the Blockchain system. Then the nodes will “vote” whether the transaction is valid or not – as in most votes, the majority decides. A set of approved transactions constitute in a block that is transmitted to every node in the network. The new block also contains the hash of the previous block, acting as a unique fingerprint, so the chain previous blocks of the chain cannot be altered. Unlike encryption algorithms, hash functions cannot be decrypted. Even minute input differences result in a completely different hash. The encryption level is so strong that brute force attacks would require multiple attempts and still might find a completely different input value *[Madumidha, 2018]*.

A study conducted by Stack Overflow on 60k developers, shows that approximately 55% consider Blockchain useful outside what is best known for, crypto currency.

With each new scenario that is introduced in IoT systems the probability of having more devices or new connection between devices is increased. In a centralized system, these can lead to frequent hurdles, as each device will try to communicate with the core servers. Therefore, in growing large-scale IoT systems the centralized approach may not be effective,

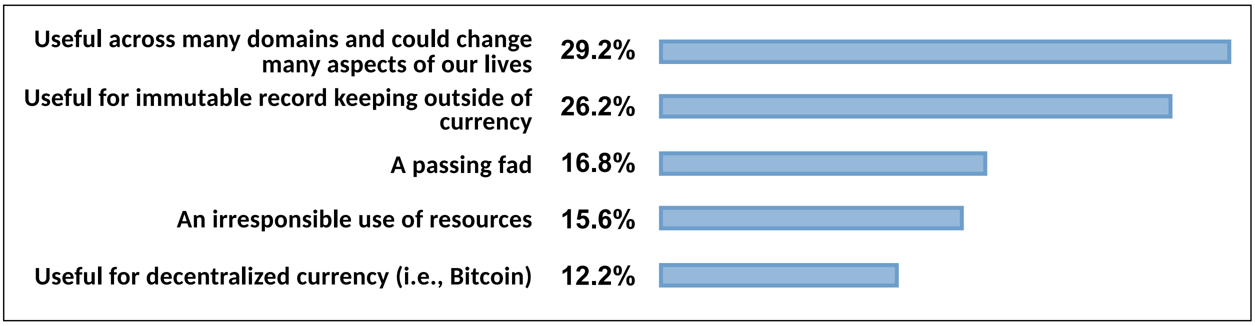

Fig. 4: *Developers opinion on Blockchain [source:StackOverFlow, 2019]*

as the new scenarios will need better, higher connectivity to keep the data and actions reliable.

In a centralized IoT system, the data exchange is performed only through the central server, raising security and privacy issues (such as device spoofing, false authentication, intrusions in data sharing). To address such security and privacy concerns, Blockchain can be introduced in the IoT system, the central server concept can be replaced by distributed nodes *[Kumar, 2018].*

Blockchain can enable true autonomous smart devices that can exchange data, without the need of a centralized broker, due to the nodes in the blockchain network that can check the validity of the transaction without relying on a centralized authority *[Banafa, 2016]*. The data flow process in IoT with Blockchain technology is different from what happens in a "classic" IoT system. In an IoT system with Blockchain, the data flow is from sensors-network-router-internet-distributed blockchain-analytics-user *[Kumar, 2018].*

But Integrating blockchain into IoT service architecture may come with flaws and shortcomings, such as *[Boncea, 2019]*:

- *Scalability* – There are fears relating to the size of Blockchain ledger that might lead to centralization as it's grown over time and might require some centralized record management;
- *Processing power and time* – high values required to encrypt all transaction data generated by the blockchain-based IoT ecosystem. This process is exhaustive given the fact that IoT ecosystems diverse and comprise heterogenous devices in terms of computing capabilities;
- *Storage* – its architecture implies that all its nodes are required to store the ledger. But as the chain grows, the ledger will increase in size.

These issues arise mostly from Blockchain's main advantage – decentralization. Blockchain falls in the CAP theorem, introduced by Eric Brewer in 1998, which states that any distributed system cannot simultaneously have consistency, availability and partition tolerance.

In Blockchain, consistency is sacrificed in favor of availability and partition tolerance. Consistency (C) on the blockchain is not achieved simultaneously with Partition tolerance (P) and Availability (A), but it is achieved over time. This is known as eventual consistency and it is reached due to validation from multiple nodes over time. A solution to this problem, described by *[Boncea et al., 2019]*, is to split the main blockchain into regional sub-blocks that will unburden the limited-resource IoT devices but still maintain the system's consistency. Regional separation would not impact consistency in an IoT environment because of the large number of devices that would have to validate new entries in the blockchain.

SMART CONTRACTS

An important technology that rose from inside the blockchain ecosystem and that could prove to be especially useful for the IoT environment. They emulate regular legal contracts with the difference being that they live inside the blockchain, are formed between virtual entities rather than actual persons and are fully automated. A smart contract is basically a small program (several lines of code long) that can be executed inside a specialized blockchain when a predetermined condition is met. In the IoT paradigm the condition could be shaped in a form of tax for one to be able to access a device's services. This method guarantees that both involved actor's interests are fulfilled and by being an automated system it allows for a faster interaction between the providers of services and the consumers.

CONCLUSIONS

The IoT ecosystem never stops to challenge the research community with its sheer complexity and constant challenges. It is more than apparent that it will continue to grow and include many more diverse areas of interest, from automated, intelligent, agriculture to smart cities, from better ecological monitoring to a more personal approach in health monitoring, all these sensors and devices will continue to grow in numbers. With this growth, there are also challenges that arise: monitoring and management, security and privacy, fast interaction with the system and widespread availability.

By combining AIOps and Blockchain technology it makes it easier to manage, monitor and guarantee a level of privacy that a consumer would expect to find. Companies such as Mongoose are already making steps into providing AIOps solutions for the IoT environment and blockchain systems like Ethereum act as a foundation of trust for the many interactions that are born inside this complex environment.

REFERENCE LIST

Badhok, V. (2020). A complete web world.

Banafa, A. (2016). Securing the Internet of Things (IoT) with Blockchain

Brink, M. (2019). Gartner Market Guide for AIOps Platforms, AIOps Blog. https://www.bmc.com/blogs/gartner-aiops-market-guide/ (retrieved in September 2020)

Boncea R., Bacivarov, I. (2016). A System Architecture for Monitoring the Reliability of IoT. In: Proceedings of the 15th International Conference on Quality and Dependability, pp. 143–150.8

Boncea, R., Petre. I., Vevera, V. (2019). Building trust among things in omniscient Internet using Blockchain Technology, Romanian Cyber Security Journal, Vol.1, No.1

ENISA (2009). Cloud Computing: Information Assurance Framework.

ERS (2018). The Costs of IT Downtime & Other Computer Downtime Statistics. https://ers.ie/it-downtime-the-numbers/ (retrieved in October 2020)

Gartner (2019). Market Guide for AIOps Platforms

IBM (2020). AIOps from IBM. https://www.ibm.com/watson/aiops (retrieved in September 2020)

IDG (2020). IDG Cloud Computing Study. https://resources.idg.com/download/2020-cloud-computing-executive-summary-rl (retrieved in September 2020)

Internet of Things Global Standards Initiative. (2015). ITU.

Kumar, N.M., Mallick, P.K. (2018). Blockchain technology for security issues and challenges in IoT. International Conference on Computational Intelligence and Data Science (ICCIDS 2018)

Levin, Anna & Garion, Shelly & Kolodner, Hillel & Lorenz, Dean & Barabash, Katherine & Kugler, Mike & McShane, Niall. (2020). AIOps for a Cloud Object Storage Service.

Madumidha, S., SivaRanjani. P, Siddarth, R., Santhosh. (2018). Blockchain Security for Internet of Things: A Literature Survey. Tenth National Conference on Computing, Communications and Information Systems, Coimbatore

Mather, T., Kumaraswamy, S., Latif, S.(2009). Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance. O'Reilly Media, Inc., Sebastopol

Moogsoft (2020). Moogsoft AIOps. https://www.moogsoft.com/aiops-platform/

Paskin, S. (2020). AIOps in 2020. https://www.bmc.com/blogs/what-is-aiops/ (retrieved in September 2020)

Splunk (2020). The 5 Forces Building the Next Data Wave. https://www.splunk.com/pdfs/ebooks/the-five-forces-building-the-next-data-wave.pdf (retrieved in September 2020)

Splunk – AIOps. (2020). AIOps: Artificial Intelligence for IT Operations. https://www.splunk.com/en_us/artificial-intelligence-aiops.html

StackOverFlow (2019). Developer Survey Results.
https://insights.stackoverflow.com/survey/2019#blockchain-in-the-real-world (retrieved in September 2020)