Incorporating Permanent Audit Trails for Corporates

Bob Duncan
Business School
University of Aberdeen
King's College, Aberdeen, UK
and
Arcada University of Applied Sciences
Jan-Magnus Janssons plats 1, 00550 Helsinki, Finland
Email:robert.duncan@abdn.ac.uk

Magnus Westerlund
and John Wickström
Department of Business Management and Analytics
Arcada University of Applied Sciences
Jan-Magnus Janssons plats 1, 00550 Helsinki, Finland
Email:magnus.westerlund@arcada.fi, wickstjo@arcada.fi

***Abstract*—All corporate businesses are under constant attack. There is no doubt that the adoption of a multitude of cheap Internet of Things devices have proved to be a great enabler of the vastly expanded potential for data collection to run systems, processes, and machines more effectively. Unfortunately, their very cheapness often means that security is not appropriately considered during design, and that the incorporation of such devices can introduce a new route in to corporate systems for attackers. The audit trail is often the single most important target for attackers to allow them to cover their tracks and remain hidden in the system for a long duration. Therefore, we must ensure we take extra precautions to properly secure this important record in a cryptographically secured immutable database, for without it, we have no means to forensically discover who has perpetrated attacks, nor how they penetrated our systems. In this paper, we explore a method of securely collecting and storing this information in an immutable database. We approach this using blockchain based smart contracts, which has the added advantage of allowing us to take a distributed approach, which also fits well with modern corporate computing infrastructures. We find that this approach can allow us to retain the relevant audit trails deemed necessary to meet corporate security goals and compliance requirements.**

***Keywords*—blockchain, IoT, smart contracts, security, audit trails**

I. Introduction

The introduction of Internet of Things (IoT) devices presents a serious challenge for keeping corporate systems secure. In 2020 in the UK alone, the Government Cyber Security Breaches Survey [1] noted that almost half of all businesses suffered a breach during the previous year. In the case of large corporates, the rate of breaches was 75%. As corporate systems become ever larger and more complex, the challenge of securing them can increase exponentially. Vulnerabilities are numerous, although often well understood. However, the one area where most corporate failures lie is in the widespread inability of corporate system users to be able to retain the audit trail of key transactions processed within these highly complex information infrastructures. This is not a new problem and has been with us for a very long time.

In traditional highly centralised corporate systems, which generally used a tight firewall around all corporate IT assets within the boundaries of the organisation, attackers were still able to get in. With ever expanding corporate needs, systems have also grown and transitioned away from a centralised IT model to a more distributed approach, partly due to multiple site locations within a country, followed by multiple site locations across both other countries and indeed continents, the challenge has only intensified.

Once an attacker had successfully penetrated the system, the audit trail was often their first target, to ensure they could remove all trace of their incursion. By altering the audit trail, attackers can remove their traces so that their activities are not recognized, and their identity and localisation remains hidden, and their continued presence is guaranteed [2]. With a highly distributed network, the goal of the attacker will still be the same. The only difference will be in the exponential increase in opportunity to gain entry into a system that may struggle to maintain either physical or logical integrity.

During the past couple of decades, corporate IT systems have expanded in complexity and capability beyond all comprehension. The addition of powerful, yet cheap, IoT devices has had an impact on corporate systems and as a result may demand new forensic methods [3]. While this has allowed corporates to achieve greater cost savings, IoT gateways have opened up considerable avenues of potential access to corporate systems. Meanwhile, the appetite of attackers has merely continued to expand relentlessly year on year [4].

In this paper, we outline how we propose to tackle this serious problem with a very robust approach to resolving these difficult challenges. In Section II, we provide some background, discussing the motivation for this work, in Section III, we discuss the practical requirements for an audit trail storage solution. In Section IV, we discuss why we elected to use blockchain smart contracts to provide robust security of the audit trail records. In Section V, we outline how smart contracts can be used to deliver a persistent audit trail for corporate systems that addresses the particular weaknesses of adding IoT systems to the corporate IT systems portfolio. In Section VI, we consider how adoption of the Zero Trust approach might fit with our proposed system elements. In Section VII, we discuss our conclusions and consider future improvements and developments of this system.

 ISBN: 978-1-61208-845-7

II. Background

Traditional monolithic information systems are challenging to keep secure and to retain a complete audit trail of events. When such complexities as cloud computing, IoT and distributed systems are added, the challenge grows exponentially. Duncan and Whittington [5] have written about the challenges of dealing with the proper audit of cloud systems, stressing the need to maintain a proper audit trail in these systems, and about weaknesses arising through poor configuration of database systems [6]. They proposed addressing this through the use of an immutable database to record a secure audit trail and system logging for cloud applications [7].

In this paper, we opted to avoid using traditional databases due to their mutability and subsequent unworthiness of storing something as invaluable as audit trail data. Traditional databases can be very simple to operate, store and analyse data, yet are notoriously difficult to prevent the data being modified by either internal authorized users such as administrators or by external attackers that have breached the network barrier. It is certainly the case that many early relational database management systems offered the provision of an immutable database option. The downside was that they were unable to offer the benefits of rapid searching through the use of indexed fields, thus rendering them too difficult to handle after a volume of transactions had built up. While it is certainly true that advances have since been made in more modern database systems, and the capabilities of No-SQL databases have opened up unstructured searching, nevertheless, weaknesses still remain once subject to attack.

Westerlund et al., [2] started development of a blockchain based solution for companies who wished to ensure the addition of a highly secure IoT network. Subsequent work has led to the development of a robust mechanism for a complete IoT system that can protect audit trails through the use of smart contracts as an immutable storage platform (see Subsection II-C).

A. The Audit Trail

Duncan and Whittington [8] note the huge wealth of experience accountants bring to financial systems, which have traditionally been subject to constant attack from both external and internal sources. While cash remains a highly attractive target, attackers have long realised that data often provides easier pickings. This arises because cash systems are often exceptionally well protected compared to data which can also have a significant value to an attacker.

The Oxford English Dictionary (OED) defines audit as: Audit — OED ([9]: “To make an official systematic examination of (accounts), so as to ascertain their accuracy”). This is a process (in accounting) that requires outsiders who are deemed to be both objective and expert to form their own opinion of what is being audited and to then publicly state their confidence (or otherwise) in the reliability of what they have investigated. Auditing is not straightforward or easy and a common view is that the main purpose of audit is the statutory requirement to audit financial statements. There are a further two areas in which we could find audit useful. First, IT systems audit will often be carried out in addition to financial audit, with one common weakness being that the IT system is often treated as a “black box” system, meaning too much trust may be placed in the system. IT systems audit is not mandatory, meaning many opportunities to spot weaknesses can be ignored, leaving potentially gaping security holes in systems. Second, audits are often used, as a means of assuring legislators and regulators that the legislation and regulations are being complied with. As these are often not mandatory, they tend to be carried out infrequently due to their highly sensitive nature, thus they may be contingent on a relationship between the auditor and the audited, again potentially leaving weaknesses unaddressed. However, there is a wealth of history and experience available in the accounting world that we can learn from, and in particular with our approach to improving the security of systems.

Turning to the audit trail, the OED [9] has the following two useful definitions of an audit trail: “(a) Accounting: a means of verifying the detailed transactions underlying any item in an accounting record; (b) Computing: a record of the computing processes that have been applied to a particular set of source data, showing each stage of processing and allowing the original data to be reconstituted; a record of the transactions to which a database or a file has been subjected”. Thus, we can see that there is not a unified perception between the two disciplines of exactly what an audit trail is. Thus, if we accept that we can choose our own requirements to suit our purposes, we can leverage the vast wealth of audit skills and experience from the accounting world to create an accounting record that helps us adapt, improve, and satisfy our computing requirements.

In the accounting world, the audit trail provides additional information to help ensure the veracity of transactions such that in the event of a serious breach, it is possible to reconstruct what took place following examination by a forensic accountant. For our purposes, we can theoretically leverage these skills to apply this technique to any kind of data, together with verification of whatever useful information we may be seeking to retain.

Whenever a new technological area is developed, a big challenge is that it is usually difficult to find people who have the appropriate skillset — since there is a requirement for people who have both competence in audit as well as expertise in the new discipline [10]. Nevertheless, for forensic accounting purposes, a tailored audit trail that can be captured and kept fully intact, can provide copious ammunition to a forensic scientist who is called upon to investigate the aftermath of a security breach. Thus, by ensuring our audit trail provides the key evidence we require, we can significantly improve our ability to fight back against the attackers.

B. Motivation

There are a great many businesses who will only ever pay lip service to proper security [4], taking the view ‘It will never happen to us’ or ‘We are not big enough to be of interest

to attackers'. Since all business systems are under constant attack, regardless of size or annual revenue, a business should always err on the side of caution and prepare for one or more of their systems to be breached. Once that happens, there can be significant consequences. There will be the disruption of official investigations, which can drag on for months, even years, often resulting in punitive fines. The disruption of a serious breach can have a significant impact on day-to-day business, often leading to huge loss of revenue, huge reputational damage, loss of confidence in the business from customers and suppliers, as well as from stock markets, which can have a serious adverse impact on share prices. The one constant in most large breach situations is that it never ends well.

A big motivator happens on the first day of a serious breach when an attacker has taken over the systems of the business. Many companies are completely unprepared for an event such as this. At the very least, there may be significant disruption to business activities, with the extent of this depending on the nature and extent of the attack. This can turn out to be such a serious outcome that many firms have been put out of business, or caused major disruption, job losses or complete meltdowns. In the case of the EU General Data Protection Regulation (GDPR), companies have only 72 hours in which to report a breach to the regulator after detecting the event [11]. In the midst of such a panic, that would likely be far down the list of priorities, yet failure to do so would not be a valid excuse, adding to the resultant fine.

In addition, it is worth pointing out that legislators and regulators are getting ever tougher with companies who suffer major breaches, especially where they have been less than competent with their security practices. There are signs that throughout the globe, punishments are getting ever tougher, year on year. Just late last year, the Hamburg Commissioner for Data Protection and Freedom of Information fined H&M (Hennes & Mauritz) €35.3 million for data protection violations of employees' personal data. These violations only came to light when the data became accessible company wide following a misconfiguration error, following which the regulator became involved [12].

C. The IoT Secure Solution

A common challenge with distributed architectures based on cloud computing or IoT, lays in securing them. Traditionally, networks are separated into physical or logical distinct networks, but for distributed architectures we may also see overlay networks that implement certain structures on the network. These overlay networks may offer a more nuanced control over the network nodes that can include customized security protocols.

In a previous proposal, we have detailed such an approach for distributed security, whereby all entities, both actors and devices, authenticate themselves through smart contracts running on the Ethereum blockchain [13]. Further, smart contracts provide function authorization so that all entities conform to a push and pull agreement for all activities. Thus, a device owner can operate the device by executing a smart contract transaction, defined as a task, that the device listens to and then interprets into an action on the device.

This class of solutions can significantly improve the security of distributed systems as nodes can be made invisible to the network. By hardening nodes and denying any externally initiated connections to a node means that they become extremely hard to attack remotely. Although the approach still demands improvement, such as detailed event audit trails, we can foresee significant improvement for distributed systems that remain publicly hidden but whose utilization remains largely unchanged.

III. Practical Requirements for an Audit Trail Storage Solution

In this section, we discuss the requirements for an immutable, distributed, database that can hold the audit trail records in a trustworthy manner offering good redundancy. Users cannot modify or delete records from an immutable database [6] and even if the system is breached, the attacker should not be able to escalate credentials to take down the distributed database nodes [2]. Many of the early database management systems did have an immutable database option. However, there was no access to indexing, which made accessing records a slow task that would get incrementally slower the more records that were in the database. With no easy means to sort the records, analytical searches would not be an option. Without any cryptographical backing of the records, assuring the integrity of the records would also have been a difficult challenge to overcome.

The development of blockchain technology introduced novel methods of storing data in a distributed, immutable, and scalable database. Public blockchains, like Ethereum [15], provide an extremely robust mechanism to ensure the veracity of immutable transactions, albeit at a significant monetary cost, particularly for use cases such as ours. Due to this impracticality, we chose to deploy our own private blockchain by using the same toolkit that was used to create the Ethereum network.

While the Ethereum network is secure to a point of redundancy, its cryptocurrency is now so valuable that it actively attracts malicious users to explore and abuse exploits for monetary gain. The primary benefit of using a private blockchain is that it reduces the cost of operations to almost nothing, because the corporate owns the blockchain's cryptocurrency. Additionally, since the cryptocurrency's value is no-longer determined via supply and demand, attackers have significantly less to gain compared to the effort it takes to find and abuse potential vulnerabilities [14].

Database companies have slowly started proposing immutable storage systems like Amazon's Quantum Ledger Database (QLDB) [16]. This product was specifically designed for cloud applications and uses a cryptographically verifiable transaction log to ensure the integrity of transactional data, without the blockchain/smart contract transaction replication. However, since we are planning ahead to incorporate the Zero

Trust approach recommended by the NSA (see Section VI), we will not use any system based on proprietary code that is fully managed by the supplier. ImmuDB [17] has also developed a fast and cryptographically secure immutable database which can be used on conventional servers or deployed in cloud. It has arguably many improvements over the Amazon QLDB option by being open source, privately hosted, and significantly faster, but does, however, lack the built-in authorized processing of blockchain smart contracts.

IV. Why We Opted for Blockchain Technology

It is fair to say that all companies, no matter how large or small, will generally have similar incentives to ensure the completeness and veracity of their data systems. Since all companies are equally exposed to the potentially punitive levels of fines for failures to comply with the demands for increasingly tougher security and privacy requirements, all are likely to benefit from a robust approach.

In our view, the bar for corporate compliance is set to a high level so we must ensure that an exceptionally robust approach can be achieved. In addition to these stringent compliance requirements, corporate systems architectures have become so complex, that failure to secure even one small part of the system can have catastrophic consequences.

Thus, we need to ensure that every possible means should be deployed to provide an exceptionally robust method to safeguard these corporate systems. By utilizing blockchain smart contracts, we can deliver a high degree of security to all the varied and necessary audit trails, and ensure proper protection for all parts of today's highly complex systems.

It is often the case that we are faced with the task of adding huge new parts to existing complex systems, such as when we add a large IoT system to an existing corporate mega-system. There may already be some weaknesses present in many corporate systems and adding something like a large insecure IoT system brings far more risks to the equation.

It is obvious that SMEs will not have large resources at their disposal to ensure the highest security standards for their business data. Being small companies, they also have a lot to lose when anything goes wrong. In today's ever increasingly punitive jurisdictional environment, compliance failures lead to potentially massive fines, even for the minnows of the corporate world.

This paper will focus on the same approach as our IoT solution [13], which has proved to deliver the high security we sought. We can be selective about which audit trail data we seek to protect, since not every event in the main corporate systems will be critical. Naturally, all login events to access control systems will be critical to retain, as will events surrounding all financial transactions. There will be others, and the corporate can make up its own mind what needs to be secured.

While we accept that there will be a resource cost to this high security audit trail retention process, in the event of a breach, it is likely to provide more than ample reward. Currently, it is hugely challenging to understand how the attacker got in to the system and what they did once there, particularly since deleting the audit trail of their activities once in the system is their primary focus. This is why attackers are so difficult to catch.

V. How We Structured Our Approach

Having developed a working distributed security solution for IoT systems, we realised that it would be insufficient without proper attention to the main corporate system. Our current work addresses the core system into which a secure IoT system is added. The vast majority of current corporate systems are not fit for purpose as far as security is concerned. Simply bolting on a secure IoT solution still does nothing if the underlying corporate system is insecure. Thus, we were motivated to consider upcoming practices and methods to determine their potential weaknesses and to propose improved solutions.

Edge computing performs computing tasks physically close to target devices rather than on the cloud or centralised location. Edge computing offers huge potential to make it possible to apply different machine learning algorithms at the edge node. An edge computing architecture relies on pipelines crossing several security boundaries in the corporate system, but the collected data should remain on the edge node and thus privacy can be improved. Given the often distributed nature of today's large corporates, the ability to include edge computing would be a potential asset.

Machine Learning Operations (MLOps) has been proposed as a systematic software engineering method to automate and optimize AI for production [18]. MLOps looks to increase automation and improve machine learning quality in production while respecting business and regulatory requirements. It allows businesses to onboard machine learning to their operations by training, deploying, and maintaining machine learning pipelines, such as those employed for edge computing. MLOps is being proposed as an industry standard for handling operational machine learning tasks. Given that we do not intend for the audit trail data to be merely collected and safely stored, it is obvious to us that their provisions to allow for the performance of a variety of analytics on this data needs to be put in place [19], and we discuss this further in Section VII.

While we have looked at these new technologies, and are considering them for our future work, they are not specifically included in the work we have addressed in this paper. Thus, we set out to deliver an approach based on smart contracts for corporate systems that aim to utilize complex set-ups that are hard to secure with traditional physical or logical networking approaches, utilising our already proven approach to delivering robust security for IoT systems. Obviously, in this case, we would need to deliver the means to capture a variety of different audit trail data, to address whatever areas might be deemed necessary by the corporate.

Our software collects an extra copy of the data direct from every system log and audit trail source that we wish to secure and this is processed to the relevant smart contract. The

 ISBN: 978-1-61208-845-7

multiple nodes that process the smart contracts simultaneously process this data to ensure robust security. With a multiplicity of physical locations for the nodes, we can achieve robustness, redundancy and security. The data in the blockchain is immutable, ensuring permanent security. The blockchain consensus algorithm will ensure the data is validated thus allowing us to develop trust in the data.

In the event of an attack, authorised users can access the data from the smart contract, and can compare this against the data contained in the original system logs and audit trail files, which will highlight where the attacker has attempted to cover their tracks. The necessary forensic data can be passed to the relevant authorities.

The beauty of our approach is that no major system rewrite is required to ensure that full security and privacy can be achieved. Companies are usually reticent to abandon an existing expensive system after they have added a large IoT implementation to ensure security and privacy. Rather, our approach allows us to select every part of existing and new systems to be specifically secured, without the need for major change. Since the audit trail runs concurrently with the existing system, there will be minimal disruption to existing systems, yet additional levels of security and privacy will be added.

In our initial testing, our software works exactly as planned. Processing is carried out efficiently and we can select the data we wish to inspect at will. This data extraction facility makes investigation considerably less of a challenge. Our next stage will be to set up a test server to run an example system, in which we will generate a typical selection of data. We will then carry out a range of attacks on the system to test how well the system works. We will publish the results of this investigation in due course.

VI. How this can align with the NSA Zero Trust Approach

The National Security Agency (NSA) of the US recently recommended all government, military and contractors who work for these agencies to adopt a Zero Trust strategy [20]. The essence of this approach is to assume that ALL hardware, software and people in an organisation should be regarded as having Zero Trust. On this basis, corporates will not make any weak assumptions of trust with any part of the business architecture. This paradigm shift is a very sensible and a welcome recommendation to security, but most centralized systems would need to be rebuilt from the ground up in order to comply with the ruleset.

We believe there is strong merit in adopting this approach for all corporate systems. All too often, assumptions are made about the level of trust according to hardware, software and the people in an organisation, leading to too many weaknesses in security being allowed to arise. There is no doubt that adoption of this approach will require new ways of thinking. However, if a corporate starts by adopting our secure IoT system first, this will cause no disruption to the smooth running of the business, since our IoT solution already complies with the Zero Trust model. Adopting the securing of the audit trails in the manner we suggest in this paper, will further improve security with minimal disruption.

The next stage would be to introduce the Zero Trust strategy, again in a phased way in order to minimise disruption. Once this fundamental shift in approach has been successfully carried out, we would then be ready to incorporate the next phase. Earlier in this paper, we introduced the possibility of conducting analytics on the collected data. We can foresee the possibility of using such analytics on secure data to perform all manner of useful tasks to measure the veracity of data being produced and recorded, all of which could be tailored to every single part of the business architecture of the corporate. Again, these variations could be added as required, to minimise disruption to ongoing systems.

VII. Conclusion and Future Development

In conclusion, we have developed a high security audit trail system that can theoretically be applied to protect any part of a large corporate system, which works by protecting the forensic information contained in activity logs. Since these are a frequent target of attackers, the ability to retain these records will be transformative for corporates in their fight against cyber attacks. Having the ability to identify an attack more quickly, identify how the attack was perpetrated, how it was executed, and what data was exposed will be a huge improvement when reporting to regulators. By ensuring that this data is properly encrypted in the first place and that we can identify specifically which data was compromised, and whether it was properly encrypted, the impact on personally identifiable information will be minimal, as will the resultant fine.

Furthermore, there will be an evidential trail available for authorities to follow and pursue legally, opening up the possibility that for the first time, attention will be able to have a forensic focus directed onto the criminals who perpetrated these attacks. Nation states are taking these criminal activities ever more seriously, and it will be interesting to see how criminals like having the tables turned on them for a change. Equally, it will be useful for corporates to be able to mitigate the usual massive fines that are levied against them every time they suffer a data breach.

Looking ahead to future developments, we can see that the adoption of the Zero Trust approach will remove slack perceptions of the security of corporate systems and will ensure stronger corporate systems are developed and maintained. At the same time, the ability to ensure the addition of highly secure IoT systems will provide a massive boost to security, as will be the ability to retain complete audit trails for all important corporate systems.

However, the possibility to leverage this important data that we have been able to secure will open the possibility to develop some really important capabilities. Automated analysis of server logs could provide instant feedback of an attack in process. However, it might also be possible, by developing systems using machine learning, to provide assurance of the veracity and integrity of every single element of corporate systems on an ongoing basis. Every single device, software

 ISBN: 978-1-61208-845-7

system, server, and even the weakest link in the corporate business architecture, the people, could all be continuously monitored to ensure nothing untoward is happening.

REFERENCES

[1] HMG, "UK Cyber Security Breaches Report 2020," HMG, London, Tech. Rep., 2020. [Online]. Available: https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2020 [Last access: 21 March 2021]

[2] M. Westerlund, M. Neovius, and G. Pulkkis, "Providing Tamper-Resistant Audit Trails with Distributed Ledger based Solutions for Forensics of IoT Systems using Cloud Resources," *International Journal on Advances in Security Volume 11, Number 3 & 4, 2018, pp 288 - 300*, 2018.

[3] S. Zawoad and R. Hasan, "Faiot: Towards building a forensics aware eco system for the internet of things" *2015 IEEE International Conference on Services Computing*, pp. 279-284, 2015.

[4] Verizon, "Verizon Security Breach Report 2020," Tech. Rep., 2020. [Online]. Available: https://enterprise.verizon.com/en-gb/resources/reports/dbir/ [Last access: 21 March 2021]

[5] B. Duncan and M. Whittington, "The Complexities of Auditing and Securing Systems in the Cloud — is there a Solution and will the GDPR move it up the Corporate Agenda?" *International Journal on Advances in Security*, vol. 11, no. 3&4, pp. 232–242, 2018.

[6] B. Duncan and M. Whittington, "Creating an Immutable Database for Secure Cloud Audit Trail and System Logging," *International Journal on Advances in Security*, vol. 10, no. 3&4, pp. 1–12, 2017.

[7] B. Duncan and M. Whittington, "Enhancing Cloud Security and Privacy: The Power and the Weakness of the Audit Trail," in *Cloud Computing 2016: The Seventh International Conference on Cloud Computing, GRIDs, and Virtualization*, no. April. Rome: IEEE, 2016, pp. 125–130.

[8] B. Duncan and M. Whittington, "Enhancing Cloud Security and Privacy: The Cloud Audit Problem," in *Cloud Computing 2016: The Seventh International Conference on Cloud Computing, GRIDs, and Virtualization*. Rome: IEEE, 2016, pp. 119–124.

[19] K. Grahn, M. Westerlund, and G. Pulkkis, "Analytics for network security: A survey and taxonomy", *Information fusion for cyber-security analytics*, pp. 175–193, 2017, Springer.

[9] OED, "Oxford English Dictionary," 2021. [Online]. Available: http://www.oed.com [Last access: 21 March 2021]

[10] B. Duncan and M. Whittington, "Can Forensic Audit Help Address the Cloud Forensic Problem in Light of the Requirements of the Forthcoming European Union General Data Protection Regulation?" in *Cloud Computing 2018: The Ninth International Conference on Cloud Computing, GRIDs, and Virtualization*, no. February. Barcelona, Spain: IARIA, 2018, pp. 84–89.

[11] EU, "EU General Data Protection Regulation (GDPR)," 2017. [Online]. Available: http://www.eugdpr.org/ [Last access: 21 March 2021]

[12] H. Commissioner, D. P. of Information, and Freedom, "35.3 Million Euro Fine for Data Protection Violations in H&M's Service Center," p. 1, 2020. [Online]. Available: https://datenschutz-hamburg.de/assets/pdf/2020-10-01-press-release-h+m-fine.pdf [Last access: 21 March 2021]

[13] J. Wikström, M. Westerlund, and G. Pulkkis, "Smart Contract based Distributed IoT Security: A Protocol for Autonomous Device Management," in proceedings of *21st ACM/IEEE International Symposium on Cluster, Cloud and Grid Computing (CCGrid 2021) (forthcoming)*, Melbourne, Australia, 2021 pp 1 - 6.

[14] Y. Zhao and B. Duncan, "Could Block Chain Technology Help Resolve the Cloud Forensic Problem?" in *Cloud Computing 2018: The Ninth International Conference on Cloud Computing, GRIDs, and Virtualization*, no. February. Barcelona, Spain: IARIA, 2018, pp. 39–44.

[15] V. Buterin and Others, "Ethereum white paper," *GitHub repository*, vol. 1, pp. 22–23, 2013.

[16] Amazon, "Quantum Ledger Database," 2020. [Online]. Available: https://aws.amazon.com/qldb/ [Last access: 21 March 2021]

[17] Immudb, "immudb," 2020. [Online]. Available: https://www.codenotary.com/technologies/immudb/ [Last access: 21 March 2021]

[18] E. Raj, M. Westerlund, and L. Espinosa-Leal, "Reliable Fleet Analytics for Edge IoT Solutions", in *Cloud Computing 2020: The International Conference on Cloud Computing, GRIDs, and Virtualization*, pp 65 - 62 2020.

[20] N. S. Agency, "Embracing a zero trust security model," Tech. Rep., 2020. [Online]. Available: https://media.defense.gov/2021/Feb/25/2002588479/-1/-1/0/CSI_EMBRACING_ZT_SECURITY_MODEL_UOO115131-21.PDF [Last access: 21 March 2021]

 ISBN: 978-1-61208-845-7