# Securing the Internet of Things from the Bottom Up Using an Immutable Blockchain-Based Secure Forensic Trail

Bob Duncan
Computing Science
University of Aberdeen, UK
Email: bobduncan@abdn.ac.uk

***Abstract*—It has traditionally been the case that the Internet of Things represents the weak link in the corporate information system chain. While research has tried to improve the status quo, this has brought a new challenge to the table. Corporate systems, while generally much stronger than Internet of Things systems, are not, in themselves, totally secure. This is especially true of cloud-based systems. This major flaw arises because of the difficulty in safeguarding the forensic trail of corporate systems. The first thing the attacker does as soon as they have penetrated a corporate system, is to delete all the evidence of their entry from the forensic records of the corporate system, and there is usually very little to prevent this from happening. This is why it is such a challenge for authorities to trace attackers and bring them to account. The forensic trail is often the least protected part of corporate systems, but is arguably the most important from a compliance point of view. We show how it is possible to secure the forensic trail for corporate systems users who adopt these secure IoT approaches, by adopting the straightforward approach we suggest here to protect the forensic trail through the use of Blockchain. This will allow corporates to ensure the overall system can be secured, but more importantly, will provide a means to fight back against the attackers.**

***Keywords–Corporate Systems; Internet of Things; Immutable Forensic Trail; Blockchain; Distributed Ledger Technology.***

## I. INTRODUCTION

The Internet of Things (IoT), a term first coined by Kevin Ashton in 1999 [1] was one of those great inventions that everyone thought would be the next big thing. Until they were implemented, and suddenly, the realisation struck that nobody had really considered how security might be an issue. Since most 'things' were produced with minimal resources, so that they would be cheap to buy, this also meant there was little ability to process the information collected and carried onwards, let alone be able to deal with security. Like all new advances in computing over the decades, it never takes certain people long to figure out a way to abuse the new technology for their own malicious ends.

The applications could be limitless, offering huge potential for operating efficiencies. For example, in some industries, many Supervisory, Control and Data Acquisition (SCADA) systems have been implemented to allow the company to control industrial process over a wide geographical area. Many components are highly specialised, very expensive, and can often only be upgraded once a year when the whole operational facilities are shut down for their annual maintenance program. Many of these SCADA components are decades old, because they are ultra reliable, but very expensive to replace.

However, when some bright spark suggested adding IoT devices all over the area to provide readings, or carry out functions that require people to physically travel to each location, this was seen as a great way to save huge sums on payroll and travel costs. Until those other people figured out there was little to zero security on these cheap IoT devices, and suddenly, they had unprecedented and unlimited access to not only the entire SCADA system, but could often leverage that access into confidential corporate systems because they were entering those systems from a 'trusted' source system. All too often, corporates were lax on the implementation, and review, of anomalous exceptions, meaning intrusions were frequently missed. Oman and Schweitzer [2] expressed concern about how this trend could pose threats to both power substations and SCADA controllers. Creery and Byers [3] were very concerned about how this hybridization of systems could lead to unintended security consequences. Kropp [4] warned of the double increase to risk brought about through the move from regulated industries coupled with the use of networked systems. Ralston, Graham and Hieb [5] carried out a risk assessment for SCADA and Distributed Control Systems (DCSs) networks, and were very concered about the increase in security risks posed.

Thus, those attackers would not only have access to the sensitive corporate system, but they could also cause mayhem by interfering with the SCADA equipment. This allowed for the possibility to shut down gas, water or sewage pipelines, shut off electricity supply, or cause massive damage to the SCADA systems as a whole.

The solution is surely the development of highly secure IoT systems? Sadly, that can only go part of the way to solving the problem. That is because the main corporate systems and the SCADA systems remain weak. In the following decade, Ericsson [6] is concerned about the development of the smart grid, and is concerned that often there is insufficient separation between operational and administrative computer systems, leading to security weaknesses. Wilhoit [7] of Trend Micro, expresses concenns around the importance of these systems, yet their continued lack of security persists. Adding a highly secure IoT system simply means the attacker will go into the main system, then coming from the main source, will have authorisation to get into the new highly secure IoT system, thus allowing them to render the security ineffective.

There can only be one proper solution. We simply need to

 ISBN: 978-1-61208-778-8 

protect the one thing all attackers crave — the forensic trail! Will that ensure we finally have a secure system then? Not exactly. Attackers will still be able to get into the system. But now, with the forensic trail preserved, we now have the proof of what the attacker did once they got into the system. This means recovery will be able to become far more focussed than before. With no complete forensic trail to work with, a full search and investigation into all systems becomes necessary to try to work out what has been compromised or exfiltrated. However, with a full forensic record showing who did what, we instantly know what to check.

In 2016, Duncan and Whittington [8] emphasized the vital importance of the need to secure the audit trail. Duncan and Whittington [9] proposed the use of an immutable database to secure the audit trail and system logs. Duncan, Happe and Bratterud [10] proposed a novel method of achieving this using unikernels. Zhao and Duncan [11] considered the possibility of using Blockchain to secure the forensic trail, by considering how secure the Blockchain was in its original use in cryptocurrencies. Zhao and Duncan [12] looked at the possibility of using Blockchain without the cryptocurrecy element as a way forward for securing the forensic trail.

In Section II, we take a look at why companies should care about the implications of legislative and regulatory non-compliance for any company. In Section III, we identify what the Cloud Forensic Problem is, and address why it is such a challenging problem to overcome. In Section IV, we ask whether it is possible to attain compliance without addressing the cloud forensic problem. In Section V, we consider how we might secure corporate systems. In Section VI, we look at the detail of how Distributed Ledger Technology (DLT) might help us achieve a solution. In Section VII, we consider and discuss the limitations of this work, and in Section VIII, we discuss our conclusions.

## II. Why Should Companies Care About Legislative and Regulatory Compliance?

Why should companies be concerned about compliance with Legislative and Regulatory compliance requirements? The answer to that is quite simple. Criminals who wreak havoc by attacking online systems are extremely difficult to identify and track down, due to a combination of thier skills in covering their tracks, and also through challenging jurisdictional issues. The primary goal of any attacker is to remove all record of their presence in the system by identifying all elements recording their presence from the system forensic records.

After financial deregulation in the UK during the mid-1980s by the Margaret Thatcher Government, the 'free-for-all' that followed, along with the numerous losses that arose due to unethical behaviour, the Government invited Sir Adrian Cadbury [13] to carry out a review to see what could be done, and this resulted in the introduction of Corporate Governance for public listed companies, together with the introduction of the Combined Corporate Code. This has subsequently been revised and updated, usually every three years, and has accustomed corporates to adhere to the notion of compliance, in this case for corporate governance at the highest levels of these corporates. Of course there has always been the notion that compliance is required with legisalation, as well as many industry regulations.

Large corporates traditionally had a lax attitude to looking after customer data properly, so Legislators and Regulators decided that, since these corporates had a responsibility to look after customer records, which they were clearly failing to do, they would go after these companies. The recent introduction of the EU General Data Protection Regulation (GDPR) [14], took these penalties to new heights, with the power to fine companies who were non-compliant up to 4% of their annual turnover, or up to €20 million, whichever was the greater.

In the US, the US authorities have a raft of legislation to ensure companies do the right thing. Facebook were brought to task last year for privacy breaches, and a settlement was reached of some $3 billion. Of course, Facebook are not yet out of the woods. At they same time as the US intervention, they were also brought to task by the Canadian Authorities, as well as the EU under GDPR. Due to the significant size of the non-compiance, the investigations are being carried out sequentially, rather than concurrently. In the UK, the GDPR, whose regulator is the Information Commissioner's Office (ICO) proposed fines last year of £183.5 millon and £99.5 million respectively to British Airways and the Marriott Hotel Group for privacy breaches. This represents a significant change in approach from both countries.

The US is a particularly litigious country anyway, and when it comes to company wrongdoing, there is no change there. The UK regulator has recently become far more disposed to bring non-compliant corporates to task for their shortcomings. There is no doubt that other jurisdictions have taken notice of this and are also stepping up their approach to mirror these approaches. This means that wherever a large corporate operates in the globe, the regulatory and legislative environment will continue to become far more challenging as time passes. Thus it would make sense to ensure that they achieve compliance with all the relevant legislation and regulation to safeguard their own position.

Since the various legislators and regulators throughout the globe have yet to figure out how to catch cybercriminals with enough consistency to make any meaningful impact, the burden will continue to fall on corporate shoulders. While these shoulders might have been broad in previous years, now that they have had the adverse economic effects of a global pandemic to contend with, even their shoulders will no longer be so broad. This means that the economic shock of larger fines will potentially prove catastrophic over time.

Since the ICO investigation into the British Airways attack started, negotiations have been ongoing between British Airways and the ICO, and due to the huge economic impact of the global pandemic on the airline industry, a much reduced settlement of £20 million has now been reached. While this is significantly less than the proposed fone of £183.5 million, it will still hurt. No doubt the Marriott group will be hoping that their constrained economic circumstances as a result of the global pandemic might now also be taken into account when settling their eventual fine.

When it came into force, the EU GDPR was touted as the world's toughest privacy law, but not all of the 28 EU countries were ready to implement it at that time. During the last two and a half years since then, Countries like the UK, France, Germany and Italy have been starting to flex their regulatory muscles, although many smaller countries are yet

 ISBN: 978-1-61208-778-8 

to get serious. It is clear that smaller countries like Ireland and Luxembourg, where many tech companies are registered, have yet to bring any successful large action against any US big tech firm. Also, a number of EU countries still do not publish regulatory fines lists. Given the economic dependence of many of the smaller countries, one has to ask whether they are best placed to regulating big tech.

## III. The Cloud Forensic Problem (and Why it is Such a Difficult Problem)

All computing systems are constantly under serious attack, and where cloud computing is in use, this can become an even more serious issue. Once an attacker gains a foothold in a cloud system and becomes an intruder, there is little to prevent the intruder from helping themselves to any amount of data covered by legislation and regulation, either by viewing it, modifying it, deleting it or ex-filtrating it from the victim system [15], [16], [17]. Worse, there is nothing to prevent the intruder from gaining sufficient privileges to then completely delete all trace of their incursion, possibly deleting far more records than they need to in the process, leading to further problems for business continuity. Traditional non-cloud systems may also be equally vulnerable, particularly where transaction log monitoriing is not a priority.

This problem is often known as "The elephant in the room" in cloud circles. Pretty much everyone knows about it, yet nobody is prepared to discuss it, let alone try to resolve the problem, due to the difficulty of the challenge it presents. Make no mistake, this is a serious challenge to defend against, let alone overcome. However, not only is it a serious challenge for organisations using cloud, it also presents a major obstacle to compliance with legislation and regulation, thus exposing corporates to much further potential harm.

Once all trace of the intrusion has been deleted, there will be limited forensic trail left for authorities to follow. This means many companies may be totally unaware that the intrusion has even taken place, let alone be able to understand which records have been accessed, modified, deleted or stolen. All too often, companies will believe they have retained a full forensic trail in their systems, but often forget that without special measures being taken to save these records off-site [18], they will no longer be available.

Currently, in any computer system, there must be a complete and intact audit trail in order for the breached organisation to be able to tell which records have been accessed, modified, deleted or stolen. Where the audit trail and all forensic records have been deleted, there remains no physical means for any organisation to be able to tell which records have been accessed, modified, deleted or stolen, putting these organisations immediately in multiple breaches of the legislative and regulatory authorities, leaving them exposed to large potential fines.

## IV. Is It Possible to Achieve Compliance with Legislation and Regulation without Addressing the Cloud Forensic Problem?

There can be no guarantee that compliance can be achieved without addressing the cloud forensic problem [19]! It should be noted that this problem also can pertain to conventional systems as well as IoT systems. Looking to the previous section, we can see that there is nothing to prevent an intruder from destroying every scrap of forensic proof of their incursion into any computer system. It is clear that any form of forensic record or audit trail can not therefore be safely stored on any conventional computer system, nor any running cloud instance, nor any standard IoT system.

This means that the only safe method of storage of forensic data will be somewhere off-site from any running computer system. Clearly, separation of the storage from the running computer system would be the preferred solution. the off-site storage must be highly secure, preferably stored in an immutable database, and should especially be held in encrypted format, with all encryption keys held elsewhere.

There are those who say that as long as they are not breached, they will not be in breach of legislation or regulation. While it lasts, that would certainly be true, but consider, how will they be able to tell whether they have been breached, or not? What if they have been breached, and the breach has been very well covered up. They will have no means of knowing whether a breach has arisen, let alone who perpetrated it, how they got in or what they viewed, modified, deleted or ex-filtrated from the victim system. Given the propensity for modern hackers to boast about their attacking prowess, it is not likely that the attack will be missed by regulators for long.

What if a complaint is made that a customer's data has been stolen? The organisation will have no means of proving whether the data has been tampered with, or not. Equally, if, as is most likely, the breach has been extremely well covered up, they will neither have the means of complying with the reporting requirements, nor be able to understand exactly what has been compromised. This begs the obvious question: How do we secure the corporate system properly?

## V. How to Address Securing Corporate Systems

Let us first consider what we require. First, we need to ensure the integrity of our systems. This means we need to be able to retain a full forensic trail of all activities within the system. We also need to make it difficult for attackers to access. This means it needs to be separated from the main systems. It should also be difficult for attackers to understand where the records they seek to obliterate are. This would imply that encryption would be a prudent measure to include, along with some form of immutable database.

That does not seem to be a complicated requirements set. Will it be enough? Providing it is kept securely away from the main system, it provides exactly what we need to be able to understand what has happened to our system in the event of a breach. We can see from the complete forensic trail how the attacker got in, what they did from there, and what records they viewed, modified, deleted or ex-filtrated from the system. Investigative agencies can do a great deal with minimal information. How far they could go with a full forensic trail?

To meet these specific requirements, we can turn to the financial system to find a suitable solution, specifically to the area of cryptocurrencies. Anything to do with money is highly attractive to attackers. Cryptocurrencies have to be secure, have to have a bullet-proof audit trail to ensure the provenance of transactions, yet need a high level of privacy, which is possible with the assistance of Blockchain.

Typically, cryptocurrencies use a public blockchain approach, using a great many public "miners" to carry out all

 ISBN: 978-1-61208-778-8 

the provenance and privacy work using encryption algorithms along with a consensus mechanism to agree the audit trail. This does make the ledger fully public, but also introduces a high element of latency where thousands or hundreds of thousands of miners are involved. The cryptocurrency record becomes effectively immutable after consensus through this DLT. A private blockchain approach could deliver a vastly reduced latency, with the administration being funded by the corporate, whereby they either run their own blockchain system, or they might contract this DLT work in, if such facilities were offered by professional firms. These are the kind of services the big four auditing firms could offer, which could provide high levels of assurance to the corporate users. We shall consider the detail in the next section.

## VI. How can Distributed Ledger Technology Help Solve the Problem?

Let us first have a brief look at the detail of how cryptocurrencies work. We will take a brief overview of Bitcoin, since this was the cryptocurrency that was able to get cryptocurrencies off the ground back in 2009. To use Bitcoin, a user must first install a Bitcoin Wallet, which is require in order to pay or to receive money. We will return to this later. The core of the strength of all cryptocurrencies is the Blockchain, which is a Shared Public Ledger (SPL). This ledger is fullly distributed, hence Distributed Ledger Technology. Once a new transaction is made to or from the user's wallet, this transaction is deemed to be 'pending' until it has been verified by a number of 'miners' until consensus is reached, at which point it will become part of the blockchain. This provides the verification of the transaction's integrity in the bitcoin wallet. This process involves entering the transactions into the blockchain in a specific order, enforced by a strict cryptographic process (carried out by the 'miners') to ensure the integrity and chronological order of the Blockchain, in essence, creating an immutable record of all verified transactions. Once entered into the Blockchain, it is not possible to modify or delete these transactions. It is only possible to add a plus or minus transaction at a later date or time, thus ensuring a robust audit trail of all the financial transactions that have been processed. Thus, the blockchain provides the immutable audit trail, and this verifies the user bitcoin wallets.

For our purposes, we do not require a public Blockchain, or SPL, and thus do not need an army of 'miners', all of whom need to be rewarded. This usually happens by awarding them a specific fraction of a bitcoin for their work. Instead, the corporate will need to provide, secure, and pay for, their own private distributed blockchain ledger. Since this is likely to become a target for attack, each of the many versions of the Blockchain the corporate sets up should be stored away from the primary system it is trying to protect. These blockchain systems should be set up with only the absolute minimum software required, with all public facing access removed. All software should be extensively hardened, with no option to delete or amend the Blockchain software.

Then, it is a simple matter for the corporate to decide on precisely what to defend. It is important to be absolutely clear on exactly what needs to be protected, and what will be involved. Clearly, adequate resources will need to be provisioned to collect the considerable volume of data that will be needed. There is no doubt that it will be more expensive to collect, store, and protect this information than under normal operations. However, it is important to realise that instead of being clueless in the face of a successful breach, the corporate will have a considerable amount of verified data to hand, which will clearly help mitigate any potential breach penalties, since very targeted information on the attackers can be passed to both the regulatory authorities as well as to the relevant government agencies, such as police and security services, and so on.

The data collected will also be useful for performing data analytics to discover the footprint used by attackers, which can be used to adapt existing access control systems to become more robust. It would also be ineteresting to have the capability to turn the tables on the attackers.

## VII. Limitations and Discussion

Many people point to the significant cryptocurrency breaches we have seen during the past decade:

- Bitcoinica 2012 [20], 46,703 bitcoins stolen followed by another 18,757;
- Mt Gox 2014 [21], $460 million hack, following a previous hack in 2011 of $8.75 million;
- Bitfinex 2016 [22], $72 million hack;
- Decentralized Autonomous Organization (DAO) 2016 [23], $70 million hack;
- Coincheck 2018 [24], $530 million hack.

All very damning evidence for the weakness of Blockchain. Or was it? Zhao and Duncan [25] carried out an investigation on whether these attackes had been able to exploit any weakness in the Blockchain and discovered that:

- Bitcoinica stored large amounts of bitcoin online, rather than in off-line stecure storage;
- Mt Gox attack succedded due to a combination of poor management, neglect and inexperience;
- Bitfinex thought they made their systems more secure, but failed to spot they had created an exploitable weakness, which was duly exploited;
- DAO there was a flaw in their system which could be exploited by a recursion attack. It was duly exploited. Nice return for a couple of hours work.;
- Coincheck did not use secure networks.

Thus it is clear that in every one of these successful attacks, the Blockchain could not be breached. The lesson here is that it is impossible to simply rely on the blockchain alone for good security. Every element of a system must be properly secured in order to ensure the success of the whole.

It is also true that the original aim of Blockchain was to provide a high level of privacy, but Meiklejohn et al., [26], Ober, Katzenbeisser and Hamacher [27], Reid and Harrigan [28], plus Ron and Shamir [29] all observed that Bitcoin delvered much weaker privacy than was first expected. However, since this was based on the use of the public Blockchain, this is not likely to be an issue where a private Blockchain is in use.

Another area of concern arose in observing how some 'miners' exhibited selfish behaviour to try to increase their gains by 'pool hopping'. To try to prevent this, Rosenfeld

 ISBN: 978-1-61208-778-8 

[30] drew attention to the mechanism design problem of trying to keep rewards constant over time. Babioff et al., [31], and later Eyal and Sirer[32] expressed their concerns that the mining protocol rules can not be considered to provide true equilibrium strategies if users have the option to withhold information both on a selective and a temporary basis over time. The use of a private Blockchain can remove this issue.

The 2013 introduction of another cryptocurrency, Ethereum [33], opened up the possibility to use smart contracts to extend the capabilities of the Blockchain. It is likely that for forensic trail preservation, this is likely to be something of an overkill.

In 2016, McConaghy et al., [34] presented BigchainDB, a scalable Blockchain database, suitable for big data applications. In this paper, the authors presented a comprehensive description of their proposal, including a full analysis of performance, latency and preliminary experimentation results. They also introduced a new concept of Blockcahin pipelining which provides the mechanism to deliver scalability gains.

In looking at how IoT security could be revolutionised, Liu et al., [35] demonstrated how their proposed solution for a Blockchain based data integrity service framework for IoT data could outperform the use of Third Party Audit (TPA) offerings. Westerlund and Kratzke [36] suggested how the use of Blockchain could help address some of the inherent security issues of using IoT. Qu et al., [37] proposed a Blockchain based credibility verification method for IoT entities. Angin et al., [38] addressed the shortcomings of IoT devices and proposed a solution to improve their security. Dukkipati et al., [39] suggested that a Blockchain backed access control system could offer significant improvements to the security of IoT devices. Li et al., [40] suggested that by uding Blockchain in manufacturing, it could help provide more integrated and secure manufacturing ecosystems. Zhang et al., [41] proposed the use of Blockchain smart contracts for access control to IoT devices.

As we can see, there is a lot of work going on around the possible use of Blockchain as a serious means to improve IoT security. This is most certainly something that is very necessary, but ultimately, if we add a much more secure IoT system to existing corporate systems, then the security of the IoT system could be much better than the existing corporate system. This would result in the weakest link now becoming the strongest link, which will not improve that status quo, rather it will simply turn it on its head.

This is why the simple addition of a Blockchain based forensic trail mechanism to all main corporate systems would even the playing field, security wise, and would offer a means to understand whenever any breach arises. Policing for such an event could be automated into the overall system in order that rapid advance warning can take place, as well as any possible preventive measures that could also be quickly activated. Best of all, the attackers would then leave behind a complete forensic trail of their incursion into the system.

It is important to stress that this is not a ‘silver bullet’ to solve the security of corporate systems. However, it will clearly provide a welcome solution to the problem of dealing with the protection of the forensic trail that is so often obliterated from corporate systems by attackers in the process of covering their tracks. All too often, the less skilled attackers destroy more data than they need to, resulting in far more difficult challenges for corporate data controllers. This will, however, mean that the addition of a secure IoT system to any existing corporate system can result in a much tighter system, with the bonus of a means to understand exactly what is going on when any attack takes place.

## VIII. Conclusion and Future Work

In summary, we can see that the ability for conrporate sysems to have a new tool with which they can more fully understand exactly what is going on as the result of an attack will be a very good thing. This is particlarly the case when the corporate falls under the jurisdiction of many legislative and regulatory bodies, where failure to understand which records have been viewed, modified, deleted or ex-filtrated from the system can lead to punitive levels of fines being levied, as well as the expense and disruption of a lengthy investigation.

It will also be useful to be able to retain the full record of the forensic trail for investigation by the appropriate authorities. These records are not usually left behind, although investigators can do a great deal with fractional forensic snippets that sometimes get left behind in systems after a successful attack. With the full forensic trail now available, this will provide a transformative means for a fightback against these secretive attackers, who have long considered themselves immune to prosecution. While this will not solve the jurisdictional problems, at least the perpetrators can be publicised and added to public watchlists, as well as to various blacklists.

We have proposed how this challenging problem may be approached to ensure that corporate users can be fully compliant with the ever increasing leglative and regulatory requirements that they now have to comply with. Clearly, additional cost will require to be incurred, and there may be a very small impact on latency, but these costs could significantly mitigate the possibility of a huge regulatory fines in the event of a breach. It is also likely that this approach will ensure faster discovery of the occurrence of a breach, thus minimising the potential impact on business continuity.

For our next stage of this development, we propose to set up two small test corporate systems. One system will use existing security approaches, to which we will add a Blockchain secured IoT system, which we will subject to a systematic attack to demonstrate how even the addition of the secured IoT system cannot solve this problem. The second system will be a small test corporate system incorporating the Blockchain secured forensic trail, with added Blockchain secured IoT system to demonstrate how well the whole system can handle an attack. We will then be able to compare both systems and this will allow us to clearly demonstrate the different levels of compliance that could be achieved.

The beauty of this proposal is that it will not involve a major revision of existing corporate systems. Thus no massive expenditure will be required to completely change the system, with all the attendant workload to transfer all the data from the old format to the new. It will simply involve the insertion of a ‘software tool’ into existing corporate system, with which corporates are already intimately familiar with. Best of all, it is unlikely to involve massive expenditure, which in today’s constrained working environment will always be welcome.

## References

[1] K. Ashton, “That ’Internet of Things’ Thing,” RFiD Journal, vol. 22, no. 7, 2009, pp. 97–114.

 ISBN: 978-1-61208-778-8 

[2] P. Oman and E. O. Schweitzer, "Concerns About Intrusions Into Remotely Accessible Substation Controllers and Scada Systems," in Power, vol. 20, 2000, pp. 1–16.

[3] A. Creery and E. Byers, "Industrial Cybersecurity for Power System and Scada," in Management. IEEE, 2005, pp. 303–309. [Online]. Available: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1524567 Accessed 15 October 2020.

[4] T. Kropp, "System Threats and Vulnerabilities - SCADA EMS," Power and Energy Magazine, IEEE, vol. 4, no. april, 2006, pp. 46–50. [Online]. Available: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=1597995 Accessed 15 October 2020.

[5] P. A. S. Ralston, J. H. Graham, and J. L. Hieb, "Cyber security risk assessment for SCADA and DCS networks," ISA Transactions, vol. 46, no. 4, oct 2007, pp. 583–594. [Online]. Available: http://linkinghub.elsevier.com/retrieve/pii/S0019057807000754 Accessed 15 October 2020.

[6] G. N. Ericsson, "Cyber security and power system communicationessential parts of a smart grid infrastructure," IEEE Transactions on Power Delivery, vol. 25, no. 3, 2010, pp. 1501–1507.

[7] K. Wilhoit, "Who's Really Attacking Your ICS Equipment?" Tech. Rep., 2013. [Online]. Available: http://www.trendmicro.com.hk/cloud-content/apac/pdfs/security- intelligence/white-papers/wp-whos-really-attacking-your-ics-equipment.pdf Accessed 15 October 2020.

[8] B. Duncan and M. Whittington, "Cloud cyber-security: Empowering the audit trail," International Journal on Advances in Security, vol. 9, no. 3 & 4, 2016, pp. 169–183.

[9] B. Duncan and M. Whittington, "Creating an Immutable Database for Secure Cloud Audit Trail and System Logging," in Cloud Computing 2017: The Eighth International Conference on Cloud Computing, GRIDs, and Virtualization. Athens, Greece: IARIA, ISBN: 978-1-61208-529-6, 2017, pp. 54–59.

[10] B. Duncan, A. Happe, and A. Bratterud, "Using Unikernels to Address the Cloud Forensic Problem and help Achieve EU GDPR Compliance." Cloud Computing 2018: The Ninth International Conference on Cloud Computing, GRIDs, and Virtualization, February, 71–76.

[11] 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.

[12] Y. Zhao and B. Duncan, "Blockchain Challenges for Cloud Users," in Proceedings of the Tenth International Conference on Cloud Computing, GRIDs, and Virtualization, Venice, 2019, p. 6.

[13] A. Cadbury, "The Financial Aspects of Corporate Governance," HMG, London, Tech. Rep., 1992. [Online]. Available: http://www.ecgi.org/codes/documents/cadbury.pdf Accessed 15 October 2020.

[14] EU, "EU General Data Protection Regulation (GDPR)," 2017. [Online]. Available: http://www.eugdpr.org/ Accessed 15 October 2020.

[15] 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.

[16] G. Weir, A. Aßmuth, M. Whittington, and B. Duncan, "Cloud Accounting Systems, the Audit Trail, Forensics and the EU GDPR: How Hard Can It Be?" in The British Accounting and Finance Association: Scottish Area Group Annual Conference. Aberdeen: BAFA, 2017, p. 6.

[17] P. Tobin, M. McKeever, J. Blackledge, M. Whittington, and B. Duncan, "UK Financial Institutions Stand to Lose Billions in GDPR Fines: How can They Mitigate This?" in The British Accounting and Finance Association: Scottish Area Group Annual Conference, BAFA, Ed., Aberdeen, 2017, p. 6.

[18] R. K. L. Ko et al., "TrustCloud: A framework for accountability and trust in cloud computing," Proceedings - 2011 IEEE World Congress on Services, SERVICES 2011, 2011, pp. 584–588.

[19] B. Duncan, "Will Compliance with the New EU General Data Protection Regulation Lead to Better Cloud Security?" International Journal on Advances in Security, vol. 11, no. 3&4, 2018, pp. 254–263.

[20] L. Constantin, "Hackers break into bitcoin exchange site Bitcoinica, steal $90,000 in bitcoins," 2012. [Online]. Available: https://www.networkworld.com/article/2188554/applications/hackers-break-into-bitcoin-exchange-site-bitcoinica–steal–90-000-in-bitcoins.html Accessed 15 October 2020.

[21] R. McMillan, "Bitcoin's $460 Mliion Disaster," 2014. [Online]. Available: https://www.wired.com/2014/03/bitcoin-exchange/ Accessed 15 October 2020.

[22] C. Baldwin, "Bitcoin worth $72 million stolen from Bitfinex exchange in Hong Kong," 2016. [Online]. Available: https://www.reuters.com/article/us-bitfinex-hacked-hongkong/bitcoin-worth-72-million-stolen-from-bitfinex-exchange-in-hong-kong-idUSKCN10E0KP Accessed 15 October 2020.

[23] D. Siegel, "Understanding The DAO Attack," 2016. [Online]. Available: https://www.coindesk.com/understanding-dao-hack-journalists/ Accessed 15 October 2020.

[24] BBC, "Coincheck: World's biggest ever digital currency 'theft'," 2018. [Online]. Available: http://www.bbc.co.uk/news/world-asia-42845505 Accessed 15 October 2020.

[25] Y. Zhao and B. Duncan, "The Impact of Crypto-Currency Risks on the Use of Blockchain for Cloud Security and Privacy," in The 7th International Workshop on Security, Privacy and Performance in Cloud Computing (SPCLOUD 2018), 2018, p. 8.

[26] S. Meiklejohn et al., "A fistful of Bitcoins: Characterizing payments among men with no names," Proceedings of the Internet Measurement Conference - IMC '13, no. 6, 2013 (pp. 127-140).

[27] M. Ober, S. Katzenbeisser, and K. Hamacher, "Structure and anonymity of the bitcoin transaction graph," Future internet, vol. 5, no. 2, 2013, pp. 237–250.

[28] F. Reid and M. Harrigan, "An analysis of anonymity in the bitcoin system," in Security and privacy in social networks. Springer, 2013, pp. 197–223.

[29] D. Ron and A. Shamir, "Quantitative analysis of the full Bitcoin transaction graph," in Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), vol. 7859 LNCS, 2013.

[30] M. Rosenfeld, "Analysis of bitcoin pooled mining reward systems," arXiv preprint arXiv:1112.4980, 2011.

[31] M. Babaioff, S. Dobzinski, S. Oren, and A. Zohar, "On bitcoin and red balloons," in Proceedings of the 13th ACM conference on electronic commerce. ACM, 2012, pp. 56–73.

[32] I. Eyal and E. G. Sirer, "Majority is not enough: Bitcoin mining is vulnerable," in International Conference on Financial Cryptography and Data Security. Springer, 2014, pp. 436–454.

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

[34] T. Mcconaghy et al., "BigchainDB: A Scalable Blockchain Database (DRAFT)," BigchainDB, 2016, pp. 1–65.

[35] B. Liu, X. L. Yu, S. Chen, X. Xu, and L. Zhu, "Blockchain based data integrity service framework for IoT data," in 2017 IEEE International Conference on Web Services (ICWS). IEEE, 2017, pp. 468–475.

[36] M. Westerlund and N. Kratzke, "Towards distributed clouds: A review about the evolution of centralized cloud computing, distributed ledger technologies, and a foresight on unifying opportunities and security implications," in 2018 International Conference on High Performance Computing & Simulation (HPCS). IEEE, 2018, pp. 655–663.

[37] C. Qu, M. Tao, J. Zhang, X. Hong, and R. Yuan, "Blockchain based credibility verification method for IoT entities," Security and Communication Networks, vol. 2018, n. pag. 2018.

[38] P. Angin, M. B. Mert, O. Mete, A. Ramazanli, K. Sarica, and B. Gungoren, "A blockchain-based decentralized security architecture for IoT," in International Conference on Internet of Things. Springer, 2018, pp. 3–18.

[39] C. Dukkipati, Y. Zhang, and L. C. Cheng, "Decentralized, blockchain based access control framework for the heterogeneous internet of things," in Proceedings of the Third ACM Workshop on Attribute-Based Access Control, 2018, pp. 61–69.

[40] Z. Li, W. M. Wang, G. Liu, L. Liu, J. He, and G. Q. Huang, "Toward open manufacturing," Industrial Management & Data Systems, 2018.

[41] Y. Zhang, S. Kasahara, Y. Shen, X. Jiang, and J. Wan, "Smart contract-based access control for the internet of things," IEEE Internet of Things Journal, vol. 6, no. 2, 2018, pp. 1594–1605.


 ISBN: 978-1-61208-778-8 