Federated Blockchain-based Tracking and Liability Attribution Framework for Employees and Cyber-Physical Objects in a Smart Workplace

Gabriela Ahmadi-Assalemi
Wolverhampton Cyber Research Institute (WCRI)
University of Wolverhampton
Wolverhampton, UK
https://orcid.org/0000-0002-4461-9847

Haider M. al-Khateeb
Wolverhampton Cyber Research Institute (WCRI)
University of Wolverhampton
Wolverhampton, UK
H.Al-Khateeb@wlv.ac.uk

Gregory Epiphaniou
Wolverhampton Cyber Research Institute (WCRI)
University of Wolverhampton
Wolverhampton, UK
G.Epiphaniou@wlv.ac.uk

Jon Cosson
JM FINN and Northumbria University
London, UK
John.Cosson@jmfinn.com

Hamid Jahankhani
Computer and Information Sciences
Northumbria University and QAHE
London, UK
hamid.jahankhani@northumbria.ac.uk

Prashant Pillai
Wolverhampton Cyber Research Institute (WCRI)
University of Wolverhampton
Wolverhampton, UK
P.Pillai@wlv.ac.uk

***Abstract*—The systematic integration of the Internet of Things (IoT) and Cyber-Physical Systems (CPS) into the supply chain to increase operational efficiency and quality has also introduced new complexities to the threat landscape. The myriad of sensors could increase data collection capabilities for businesses to facilitate process automation aided by Artificial Intelligence (AI) but without adopting an appropriate Security-by-Design framework, threat detection and response are destined to fail. The emerging concept of Smart Workplace incorporates many CPS (e.g. Robots and Drones) to execute tasks alongside Employees both of which can be exploited as Insider Threats. We introduce and discuss forensic-readiness, liability attribution and the ability to track moving Smart SPS Objects to support modern Digital Forensics and Incident Response (DFIR) within a defence-in-depth strategy. We present a framework to facilitate the tracking of object behaviour within Smart Controlled Business Environments (SCBE) to support resilience by enabling proactive insider threat detection. Several components of the framework were piloted in a company to discuss a real-life case study and demonstrate anomaly detection and the emerging of behavioural patterns according to objects' movement with relation to their job role, workspace position and nearest entry or exit. The empirical data was collected from a Bluetooth-based Proximity Monitoring Solution. Furthermore, a key strength of the framework is a federated Blockchain (BC) model to achieve forensic-readiness by establishing a digital Chain-of-Custody (CoC) and a collaborative environment for CPS to qualify as Digital Witnesses (DW) to support post-incident investigations.**

***Keywords*— Insider threat, Anomaly Detection, Digital Witness, IoT, Smart building, Smart City, Monitoring, Authenticity, Non-repudiation**

I. INTRODUCTION

The emergence of digitalization has a massive impact on businesses and the wider society. Within the current trend of automation and data exchange forming the concept of Industry 4.0 [1], the manufacturing industry has paved way for a systematic integration of Internet of Things (IoT) and Cyber-Physical Systems' (CPS) to develop and support products, converging physical entities, digital technology as well as creating a sphere of inclusivity in the workplace. However, as Smart Cities grow and progressively digitalise, numerous challenges must be addressed to remain competitive, innovative, sustainable and more efficient in ways the Critical National Infrastructure (CNI) is managed and controlled.

Smart Buildings, a core component of Smart Cities, are considered a complex growing network of fragile [2] Cyber-Physical-Natural (CPN) ecosystem incorporating human-users and a variety of connected SPS Objects. Similar to the wider IoT landscape, Smart Buildings are governed by a fragmentation of standards [3] due to the fast evolvement of the technology. However, companies continue to adopt and adapt to new business models to capitalize on the opportunities provided by such disruptive technologies. IoT and CPS help to gather information in real-time to maintain a global visibility and trackability of the supply chain [4]. Intelligence gathering in buildings is achieved by establishing connectivity between the different services using CPS that can be managed automatically and controlled remotely over the network. However, these advances come with numerous risks and pose significant challenges [4]. Often, legacy technology is combined with innovative IoT products to achieve a competitive edge. For example, the components and sensors for the conventional Physical Building Access Control (PBAC), Heating Ventilation and Air Conditioning (HVAC), Closed-Circuit Television (CCTV) or Building Monitoring Systems (BMS) were strictly controlled through specific vendor channels but the advancement of IoT commoditized many of these components resulting in cheaper but uncontrolled route to the market. Manufacturers producing smart devices frequently apply their own proprietary standards leading to heterogenous overcomplicated systems making interoperability extremely challenging [5]. The conventional buildings' automation, control components and systems were constructed to an internal only design. The increased interconnectivity and the heterogeneity of the current landscape in Smart Buildings have inherent cybersecurity risks [6] resulting in a large threat

G. Ahmadi-Assalemi, H. M. Al-Khateeb, G. Epiphaniou, J. Cosson and P. Pillai, "Federated Blockchain-based Tracking and Liability Attribution Framework for Employees and Cyber-Physical Objects in a Smart Workplace", In *12th Annual International Conference on Global Security, Safety and Sustainability (ICGS3)*, London, UK: IEEE, 16 – 18 Jan 2019. DOI: 10.1109/ICGS3.2019.8688297. [online]. Available: https://doi.org/10.1109/ICGS3.2019.8688297.

surface with potentially serious impacts and consequences in the event of a security breach, not only in critical buildings but also in strictly regulated sectors such as finance. It is estimated that in 2018 as much as 20% of Smart Buildings are subject to digital vandalism [7].

The human factor, an important dimension in the CPN ecosystem, is an inherent weakness that is usually overlooked and underestimated [8, 9]. Therefore, it is exploited by most intruders to gain access to computer systems. As such, Phishing attacks continue to grow as one of the most common and serious threats in the cyberspace with evidence of recent Phishing scams targeting the emerging domain of IoT [10]. The threat from human insiders in the workplace is real [11] as organisations face severe security challenges including but not limited to unauthorised access, fraud and industrial espionage. In a Smart Workplace, the risk associated with insiders extends the threat model beyond the human factor to include "Smart Insiders" [11]. The control of Smart Insiders or CPS Objects becomes more complex with the increased number of CPS devices and connected services; IoT are forecasted to be around 30 Billion [12] and that by 2018 more than 3 million workers will be supervised by robots [7].

This paper addresses the potential problem of identification and object-tracking within Smart Controlled Business Environment (SCBE). We argue that anomaly detection related to the movement and location of insiders as a means of Security-by-Design requires digital forensics readiness to facilitate post-incident investigations. Therefore, our framework incorporates BC technology. A significant amount of research is available pertaining to video and network surveillance, however, to the best of our knowledge there is little research covering internal threat detection within SCBE and the significance of collecting, identifying and revealing data without compromising it within the realm of digital forensics. Further research is needed into this growing research area to streamline concepts and develop Security-by-Design frameworks. Further to acknowledging the complexity and challenges introduced by IoT (including CPS Objects) inside the workplace, the motivation for this paper arises from the opportunities presented. For instance, we argue that CPS Objects can be modelled as "Digital Witnesses" (DW) to support DFIR; logs generated by CPS Objects can help in the process of event reconstruction, while the integrity, and therefore admissibility of this data, can be achieved with a BC-based Chain-of-Custody (CoC).

In the remainder of this paper, we discuss related work in Section II, present our tracking and liability attribution framework in Section III. Section IV shares a case study of internal threats detection in the workplace based on object movement. Finally, we conclude our study in Section V.

II. Background and Related Work

A. Inherent and Emerging Threats facing CPS in the Work Place and beyond

While Smart Devices comprise the backbone of CPS structures, CPS forms the basis of Smart Workplaces scaled up to Smart Buildings and Smart Cities with their sensing, processing, and communication capabilities. The requirement for a robust CPS deployment requires threat modelling of the several security challenges many of which are surveyed and reported in recent studies [13-15]. The Smart Workplace is an indispensable component of a Smart City infrastructure. Smart Workplaces deploy controlling and scheduling tasks to facilitate the management of the supply chain.

CPS attracts compromised-key attacks because many sensor nodes utilise cryptographic keys to participate in handshake protocols which include authenticity checks [13]. Likewise, the data storage within CPS is targeted aiming to break the confidentiality or integrity of the stored data. Other targeted components include but are not limited to communication channels, actuation control and end points [16]. The prevention, detection and mitigation of attacks against CPS are still emerging [17] while attack strategies are transformed from older implementations such as Man-in-The-Middle (MiTM), Spoofing, Denial-of-Service (DoS) and Eavesdropping. Hence, the exploitation of security vulnerabilities in Smart Devices continue with a long list that includes security cameras, smart TVs, smart door locks, power outlets, and even smart toilets within buildings [15].

Although integrated security systems are transformational to Smart Buildings, myriad of sensors are used to increase automation without appropriate security testing in favour of ease of use [18]. For example, in 2016 guests in an Austrian hotel were locked out of their room subject to a ransom payment [19] whilst in Finland, a DDoS targeted the heating system [20]. A taxonomy of security threats in Smart Devices can be listed as Boot Process Vulnerabilities, Hardware Exploitation, Chip-Level Exploitation, Encryption and Hash Function Implementations, Backdoors in Remote Access Channels, and finally Software Exploitation [15].

B. Behavioural Attribution and Tracking

Despite the transition from traditional to an IoT-enabled workplace, research suggests that threat detection strategies are limited to the organisational boundary. There is little evidence of cross-organisational information security sharing, structure and coordination [21]. Practices are in silos with centralised control management [22] lacking cyber-defence collaboration or clear strategy to deal with the insider threat. To address the increasingly more sophisticated, coordinated and targeted cyber-attacks including Advanced Persistent Threats (APTs) [23], innovative solutions are required to support a modern defence-in-depth strategy.

That said, the data collected through IoT connected CPS provides an unprecedented wealth of information which can be used to profile behaviour attributes and track movement of human insiders and CPS Objects within SCBE. For example, IoT-connected motion detectors were used to identify the number of occupants in a living space [23] and in Campus' Sports Facilities [24]. Recent research in connected cars demonstrates that data generated from in-car sensors yield outcomes about drivers' behaviours and patterns of movement [24, 25]. Research suggests that transferable solutions should emerge from individual sectors within smart environment [26], for instance, analysing information from proximity sensors in combination with other information such as Global Positioning System (GPS) data aided by AI could detect anomalies [40] more proactively and faster.

To achieve forensic readiness and to support modern DFIR it is necessary to establish and maintain the privacy and integrity of evidence. BC technology was recently proposed for the area of liability attribution in autonomous vehicles [27] and forensic analysis in road traffic accidents [28]. In behavioural attribution and tracking in Smart Workplaces, it is particularly important to protect the privacy and integrity of data. In the case of a private network, permissioned BC is more suitable because access to data is restricted to relevant stakeholders. Furthermore, a hybrid implementation of a permissioned BC facilitates federation for a shared collaborative approach for cyber resilience.

C. *Regulatory Landscape*

The regulatory landscape is very diverse and dynamic aiming at establishing an international baseline approach for DFIR. For instance, the ISO/IEC 27037 covers the initial acquisition of digital evidence, ISO/IEC 27041 ensures the appropriate methods are utilised for the digital forensics process, ISO/IEC 27042 focuses on the analysis and interpretation phases, and ISO/IEC 27043 covers earlier pre-incident preparations but also advising on other aspects such as evidence storage. Additionally, the IT security catalogue from ISO contains multi-part standards focusing on electronic discovery (eDiscovery) namely the ISO/IEC 27050-1:2016, ISO/IEC 27050-3:2017, and ISO/IEC 27050-2:2018. They are concerned with the location and preservation of pertinent Electronically Stored Information (ESI) including data by any stakeholder involved in the investigation. In the European Union, there is no common approach to IoT security. However, there are initiatives to publish baseline cybersecurity recommendations [3]. Moreover, the General Data Protection Regulation (GDPR) enforces data protection by design.

Beyond IoT technical security challenges, many new legal and regulatory concerns are yet to be addressed. A study focusing on Australian perspectives discussed the impact of IoT-based ubiquitous surveillance on the basic structure of society [29] concluded that more efforts to reform a responsive regulation are required. In the United State (US), the Department for Homeland Security and Federal Trade Commission (FTC) have already promoted guidelines and best practices for IoT security based on frameworks and standards by the National Institute of Standards and Technology (NIST) but they are non-binding. Recently, the "Internet of Things Cybersecurity Improvement Act of 2017" was recently introduced to establish the minimum set of requirements for IoT implementations [3].

III. Blockchain-based Tracking and Liability Attribution Framework (BTLA-Framework)

To address the research question of this study which can be expressed as: How can we facilitate a DFIR-enabled automated process for proactive threat detection related to Smart Insiders (Employees and CPS Objects) in the workplace?

We integrate BC technology to achieve Forensic-enabled proactive insider threat detection. Furthermore, we apply Bluetooth technology to a Proximity Monitoring model to demonstrate behaviour patterns of employees in the workspace. We utilize empirical data collected from a Bluetooth-based Proximity Monitoring Solution implemented in a real company.

A. *Threat Model*

To appreciate the value of proactive insider threat detection, consideration should be given to challenges in existing Smart Workplaces. For example, technology misuse related to hacking digital gateways could lead to unauthorised access to SCBE. Another complex yet underestimated area is "social challenges". We suppose a situation where sabotage by a disgruntled employee or unmonitored access by an external contractor, who have authorized access and an in-depth knowledge of the environment could lead to disruption of critical equipment or services. Likewise, in this situation, an easy access to computers could result in an event where a computer is used to commit a crime, or where unauthorized data manipulation is carried out resulting in financial or reputational damage to the business. Access to a floor or part of a building may not be unusual but could reflect anomalous behaviour when linked and considered collectively over a period of time. Developments in CPS provide opportunities to proactively mitigate these threats, relying on object profiling and pattern analysis to identify anomalies. Likewise, establishing an online CoC for auditing and forensic purposes.

B. *Framework Principles*

The integration of CPS proliferates the opportunities for digital forensic analysis, enabling it to take advantage of the huge amounts of data being collected. The ability to collect data from CPS Objects and understand their behaviour can support DFIR, for instance in cases of investigating unauthorized access. Partially collected data is insufficient as it does not always cover the object's history in full. Trust and integrity of data could be questionable or its integration from various stakeholders. The ultimate goal for the BTLA-framework is to improve cyber defence and provide a way to ensure that the generated data is verifiable as a credible evidence for the digital forensics' realm.

Traditionally, the Confidentiality, Integrity and Availability (CIA) model was considered the core of good security practice. Recent research proposes the Parkerian Hexad [26, 30] as a basis for a forward-looking approach to retain the effectiveness of CPS cybersecurity in smart cities. Other approaches were considered [28, 31] and we argue that [26] provides more robust and comprehensive principles for the complex and fragmented CPN ecosystem than the conventional CIA. Hence, our framework's key principles are defined as:

Confidentiality. All access must be compliant with current legislation and regulation, preventing unauthorized access.

Integrity. Data must be protected from unauthorized change.

Availability. Data must be highly available, from multiple sources of trust and each trusted source must be assured.

Authenticity. Verification of data source and change is critical throughout its lifecycle.

Possession. Prevent unauthorized manipulation of data

Utility. Maintain the data throughout its lifecycle. For digital forensics, it is critical to have access to comprehensive current and historical data. For example, the emergence of behavioural patterns or movement patterns is manifested over time.

Safety. A seventh dimension proposed by [26] asserts that the generation and use of data should not be harmful. This is a particularly relevant area considering the complexity and immaturity of CPN ecosystems with people being a key facet. In addition, the framework should be **computationally efficient** and **agile.**

C. *Blockchain Technology Integration*

To help support the proactive [17] insider threat detection with a verifiable audit trail to facilitate DFIR, the value of BC technology should be exploited. Initially implemented for the Bitcoin cryptocurrency, BC technology is composed of cryptographically-linked append-only blocks forming a trusted, shared and distributed ledger of transactions. It fulfils the purpose of decentralization of trusted sources, authenticity, integrity and responsibility. Different types of BC were initially considered. Public, permissionless BC structure, like Bitcoin or Ethereum, is not controlled by anyone but inspectable by everyone whereas private permissioned BC structure requires permissions-based membership. In a BC, all participating nodes retain the full BC copy, which comprises chronologically arranged blocks containing the hash of the previous block in the chain. As the transactions are received, new blocks are created and accepted by members' consensus. Public BC consensus is based on Proof-of-Work (PoW), while it can withstand up to 50% compromised nodes, the implementation of the consensus protocol results in fewer transactions per second. The key criticism, therefore, is the computational complexity of the model. An alternative form of consensus, Proof-of-Authority (PoA) is based on pre-authorized validators, typically suited for a permissioned network where all validators are known. The computational algorithm of the private BC, Practical Byzantine Fault Tolerance or Stellar Consensus is less demanding with a higher throughput but requires a higher number of nodes to remain trustworthy. Leveraging the features of a permissioned BC, we propose that, for threat detection, all objects must be registered based on the predefined process and criteria for access control. Permissioned (private or federated) BC will provide speed, manageability, privacy, tracking without delay, trust and integrity amongst a group of Smart Workplaces with a commitment to a common framework.

D. *Framework Participants*

We define typical participants (Fig. 1) and their interactions (Fig. 2) to guide the design of the proposed framework:

Objects (Employees or CPS Objects). We define employees as persons with an authorized contractual association to the Smart Workplace, like employees, workers, supply chain contractors. CPS Objects are smart physical or virtual objects capable of performing tasks. Objects are assumed to have the ability to provide the primary evidence for digital forensics, to have a tamper-proof storage for the data it stores, and logs metadata such as Object Identifier, and Date/Time Stamps, Authorized Zones and Schedules.

Manufacturers. They periodically receive CPS patch status information and provide updates logging the current and applied patch status.

Witnesses. We refer to Digital Witness (DW or W) [32] as CPS Objects which are functionally capable to maintain an admissible evidence to a Court-of-Law similar to human witnesses. They receive, store data and have the ability to transfer their perceived knowledge (evidence) according to a predefined set of rules.

Security Authority. internal physical or virtual entities who analyse anomalies and breaches. They act as a gatekeeper and a hand-off point coordinators when digital evidence is requested by the legal authority.

Legal Authority. includes law enforcement agencies, Police and Courts of Law. They receive digital evidence as part of an investigation process. As breach resolution authorities, the Security Authority and the Legal Authority has separate roles in the framework to enforce data governance within a legal context as a measure to prevent data abuse. This maintains the principles of the framework e.g. Object ID is only revealed when these two entities cooperate

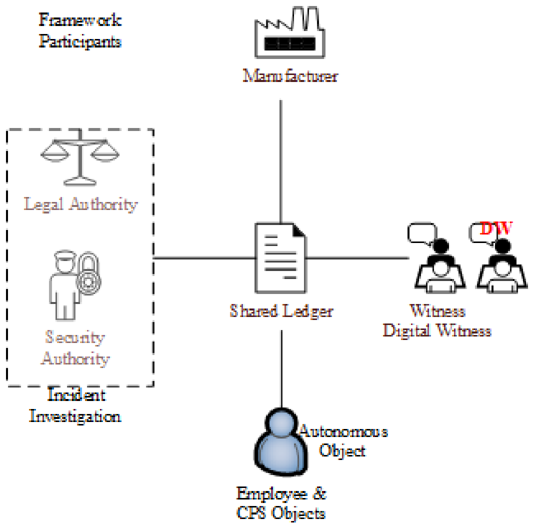


Fig. 1Tracking and Liability Attribution Framework Participants

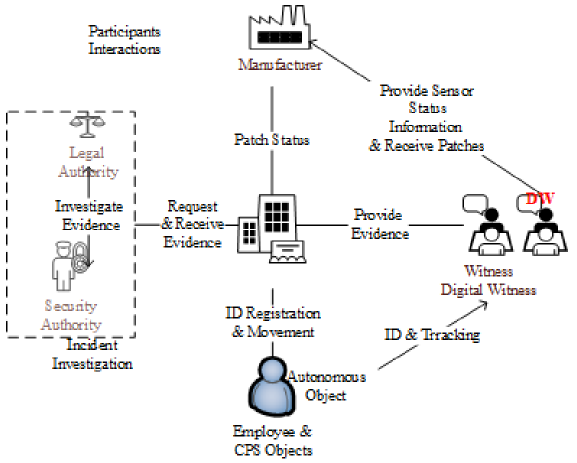


Fig. 2 Tracking and Liability Attribution Framework Interactions between

E. Framework Deployment

The framework requires a **daemon** component, it can be a physical or a virtual appliance, an application or a network daemon that communicates with the objects to collect data in (near) real-time. The daemon has read access to receive the data streams. There are three **types of data**; *information data* related to object movement through the security zones, *event data* triggered by an exception based on pre-defined parameters and *device status data*.

As part of the **core infrastructure,** the power and sensitivity of each sensor and beacon are controlled through the communication server allowing authorized manipulation of the monitoring capabilities according to requirements. The objects' storage capability is either local or referenced collectively to a Cloud-based Evidence Storage facility that is robust and highly available. It is assumed that modern core infrastructure complies with the ISO/IEC 27001 Information Security and ISO/IEC 22301 Business Continuity standards. There are several **roles** within the realm of a smart workplace. Objects (proposers) offer transactions processed by validator nodes. The verification process is enabled by hashes submitted to the BC. The proposer (a lightweight node) is the entity that stores the data (potential evidence). The validator is an authorized node forming the Consortium of Validators defined by their ability to store data and validate the transaction.

The framework **structure** is based on a permissioned BC (private or federated) with Smart Contracts proposed to control the transfer of ownership at an authorized handover point to the legal authority. Physically or virtually connected objects are capable of transmitting data within the smart workplace. Therefore, each device could be utilised either as a DW or a Hearsay DW. To describe the data lifecycle within our framework, we consider a single digital evidence and move it through the data lifecycle phases following the Digital Witness processes in ISO/IEC 27050:2016.

With the assumption that a digital investigation is taking place, all related data is potential digital evidence. An authorized entity that initially holds the ownership periodically transmits this data due to the limited local storage attached to CPS Objects but also for better data confidentiality and availability. The daemon within the BC consortium (validator node) continuously polls the beacons over a peer-to-peer network arrangement. Identities are cryptographically validated using public-private key pairs for each transaction, which then must be validated using an appropriate pre-defined byzantine agreement algorithm to reach a consensus of a valid transaction. Each block in the chain contains the hash, random nonce and root hash, timestamp and metadata of all transactions permanently recorded with the ability to trace back to the first (Genesis) block. DW logs the data in the BC while the actual records/logs (Digital Evidence) can be stored across a range of authorized storage nodes, forming a 'Hearsay' cluster of nodes referenced in a CoC based on the BC's metadata as demonstrated in Fig. 3.

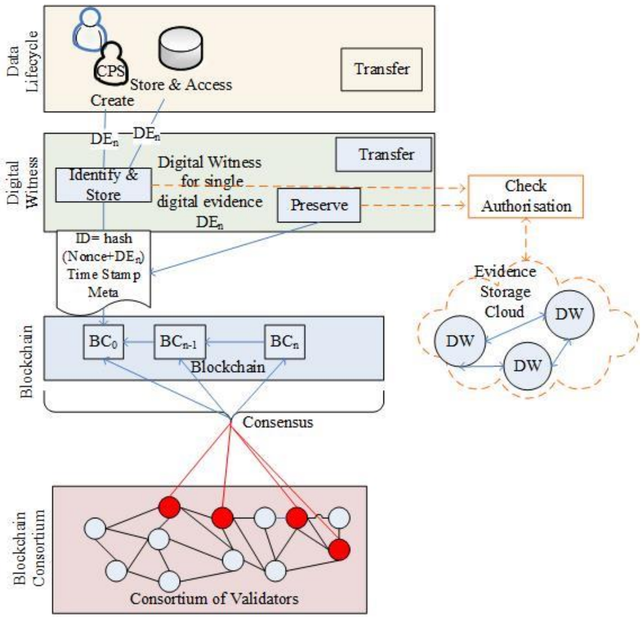


Fig. 3 Proposed Blockchain process for tracking and liability attribution

Any interaction with the records (Digital Evidence) is subject to approvals by the Consortium of Validators within the permissioned BC. If a request is made to pull evidence, the current owner issues a request for ownership transfer. This request can only be initiated by the Security Authority designated node. Upon evidence request, the requester takes on the role of the proposer, and the validators verify the request. Transfer record is then written in the Evidence Log and the metadata on the BC is updated. Evidence Log and the Smart Contract is used when the transfer of ownership is required on evidence request (Fig. 4). The Processing, Review and Analyses of digital evidence maintain the BC process (Fig. 5).

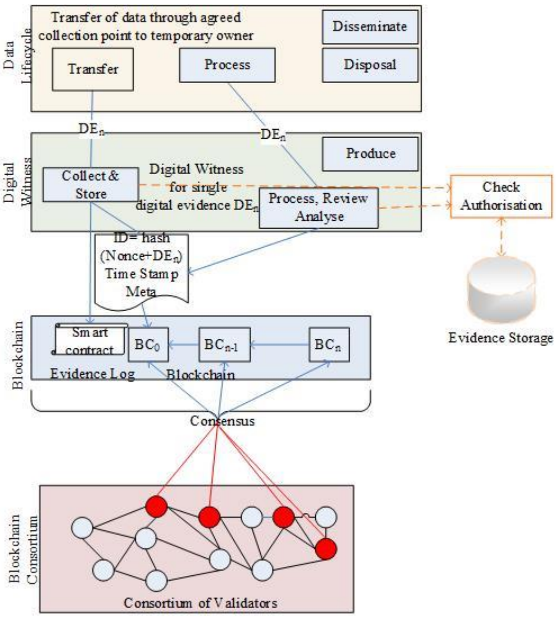


Fig. 4 Proposed Blockchain process to transfer the ownership of digital evidence

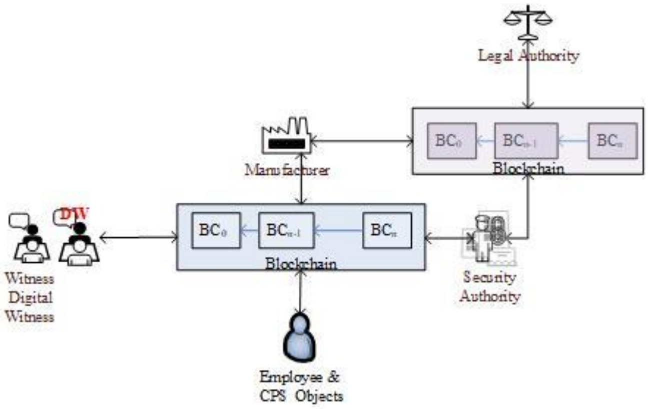


Fig. 5 Proposed Bluetooth Proximity Monitoring Model

The behaviour characteristics model. Bluetooth-based Proximity Monitoring model is an integral part of the framework to identify human-users and CPS Objects based on their behavioural attributes to maintain their visibility and traceability. Activities are registered when objects move through predefined security zones. Data streams are harvested in (near) real time from Bluetooth enabled devices. That said, to enhance the model's resilience against possible intruders, connection disruption or signal jamming it could be strengthened and combined with supplementary technology like GPS that could be considered a key factor to enhance a proactive approach of predictive monitoring. The dataset is enriched by combining it with data identified during registration thus allowing for a wider range of typical characteristics to be captured (Fig. 6). It is then processed and stored securely as it must be protected from cyber-attacks.

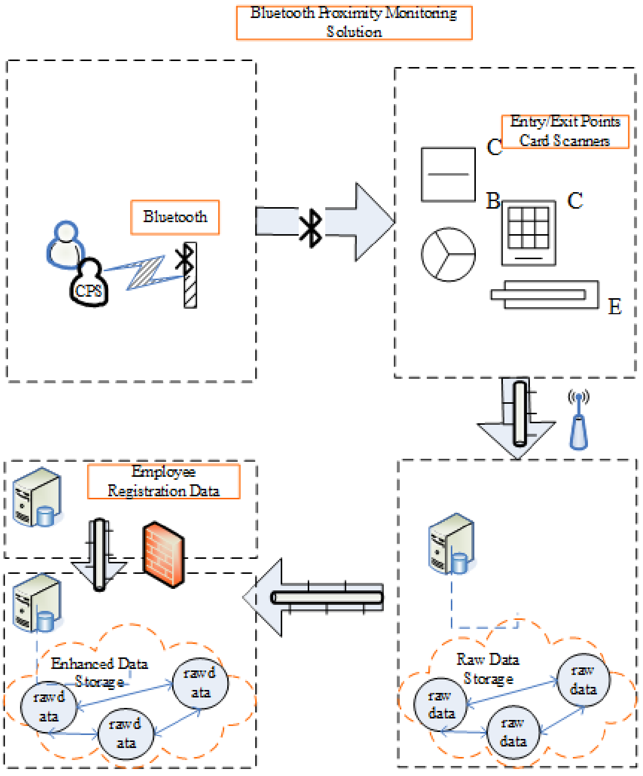


Fig. 6 Proposed Bluetooth Proximity Monitoring Model

The research question in this paper covered automation and proactive threat detection to minimize the window-size between insider attacks and the time required to detect and verify the malicious event. Furthermore, to investigate the correlation within the cluster and the object's own behavioural pattern in time-series. Therefore, an embedded **algorithm** is constructed to provide accurate results against a comparative baseline with triggers for unusual or abnormal behavioural patterns. This proactive identification could lead to a timely mitigation of insider threat.

IV. Case Study: Dakota

A. *Dakota's Threat Landscape*

Dakota (a fictional name) is a medium-sized organization that occupies 5 floors in a typical open plan modern shared workspace leased from a corporate landlord, who employs a Management Agency (MA) to look after facilities and maintenance. Dakota, regulated by the Financial Conduct Authority (FCA) in the UK must pre-screen all their employees, but this cannot be assured for the numerous external contractors employed by the MA that Dakota has to rely on and share with the other organizations within the building. Security reception staff, forming the first layer of security defence, are employed by MA. External contractors are subject to a registration process before entering Dakota's own reception but are not issued with an access control pass unless access is required to floors other than Dakota's. Insider threat [33-35] by external contractors requiring access potentially unsupervised and outside of normal operational hours was identified by Dakota as a significant risk to the business.

B. *Piloting the BTLA-Framework for Anomaly Detection*

Several components of our tracking and liability attribution framework were piloted as a proof-of-concept for the Dakota case study to provide Forensic-enabled anomaly detection as briefed below:

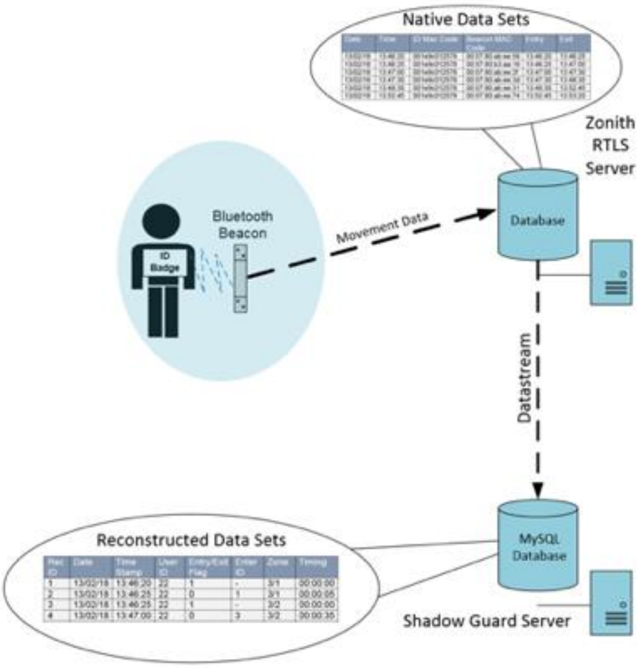
Environment. Various models were presented to mitigate the risk of access control and internal building movement that characterise types of internal threat which are often underestimated. Advances in GPS technology, Bluetooth, Wi-Fi, Radio Frequency Identification (RFID) enabled indoor employee tracking but many are considered costly. Android-based indoor tracking solution using magnetic map matching was implemented by [36] whilst [37] tested the magnet-based tracking on a robot. These solutions are computationally inexpensive with several limitations as they require predefined walking routes. RFID was used by [38] as a method of tracking usage of Campus' Sports Facilities. Interoperability, cost and coverage are key guiding principles for the proximity monitoring solution, which can be further enhanced by combining Bluetooth with other technologies such as RFID, Wi-Fi or GPS to increase and enhance the resilience. In this use case, the building access control is based on RFID technology [39], it is separate from Dakota's own access control that uses Bluetooth Proximity Monitoring Solution, there is an agreement on technology standard to ensure that a single security pass can be programmed to use both access control systems. The proximity system forms an integral part of Dakota's access control solution, combining a door entry system that incorporates elevator access and

Closed-Circuit Television (CCTV). Furthermore, the prototype for this experimental study considered a consortium BC in which several companies can, by design, be able to practice control, it is, therefore, a permissioned and semi-decentralised system.

Objects. In this case study, these are the individuals in a role (including external contractors) with a related set of parameters. Each role with its own set of parameters and in some cases multiple functions fulfilled by a single role. Examples of roles include but are not limited to cleaners, electricians, building maintenance, catering, waste disposal, cabling engineers, security, and external IT support staff.

Procedure. The Bluetooth beacons and scanners with preloaded floor plans were strategically fitted in the building. Therefore, the individuals were registered and given a Bluetooth and RFID enabled ID badge. As the individuals entered and exited a controlled zone, the relevant beacon registered them. The data was received from the Bluetooth enabled ID badge by the beacon. The data was processed by a server and stored onto an embedded database. A trigger was configured to copy the data from local native data sets to a separate secondary database where it was reconstructed and stored into a new format as shown in Fig. 7. The data collection was an automated process.

Collected Data. Data about business-critical operational areas zones, beacon deployment, individuals' roles, and tracked movement were identified and collected for a period of 2 months. Firstly, the raw data was gathered with a limited feature set only allowing the individual's position. Secondly, to start profiling movement over time the raw data was enhanced, reconstructed and stored on a Shadow Guard server logging attributes such as the Reconstructed ID, Date/Timestamp, UserID, Entry/Exit Flag, EnterID, Zone and Timing. No personal data was collected.



Date	Time	ID Mac Code	Beacon MAC Code	Entry	Exit
13/02/18	13:46:20	[illegible]	[illegible]	13:46:20	[illegible]
13/02/18	13:46:25	[illegible]	[illegible]	13:46:25	[illegible]
13/02/18	13:47:00	[illegible]	[illegible]	13:47:00	[illegible]
13/02/18	13:47:30	[illegible]	[illegible]	13:47:30	[illegible]
13/02/18	13:48:30	[illegible]	[illegible]	13:48:30	[illegible]
13/02/18	13:52:45	[illegible]	[illegible]	13:52:45	[illegible]

Rec ID	Date	Time Stamp	User ID	Entry/Exit Flag	Enter ID	Zone	Timing
1	13/02/18	13:46:20	22	1	-	3/1	00:00:00
2	13/02/18	13:46:25	22	0	1	3/1	00:00:05
3	13/02/18	13:46:25	22	1	-	3/2	00:00:00
4	13/02/18	13:47:00	22	0	3	3/2	00:00:35

Fig. 7: Data stream between the Bluetooth badge and the servers

C. Data Analysis

Behavioural patterns emerged with relation to individuals' pattern of movement relevant to their job role, workspace position and nearest entry or exit. Analysis of the data demonstrates a clear behavioural pattern (Fig. 8) and anomalies (Fig. 9), as defined by [40], were accurately detected.

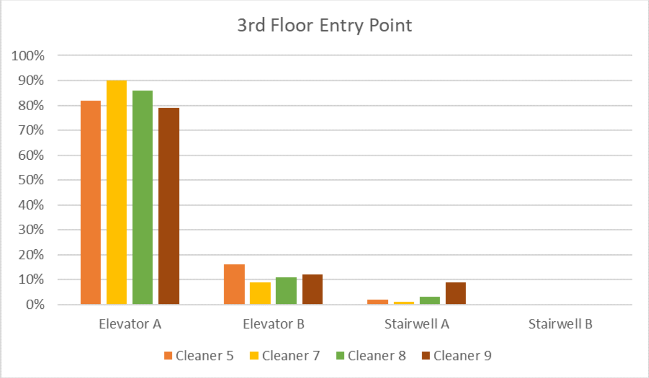
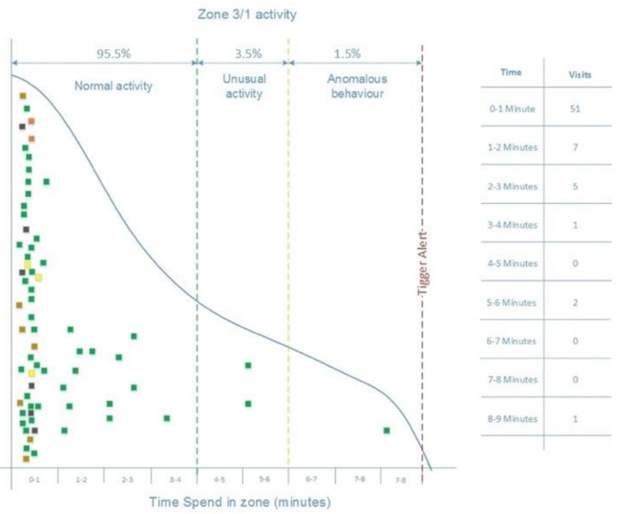


Fig. 8: data collected over the two-month period shows, that the cleaners access the floor through the same entry point 90% of the time.



Time	Visits
0-1 Minute	51
1-2 Minutes	7
2-3 Minutes	5
3-4 Minutes	1
4-5 Minutes	0
5-6 Minutes	2
6-7 Minutes	0
7-8 Minutes	0
8-9 Minutes	1

Fig. 9: Anomalous Activity point-based anomaly chart detailing user activity

We optimised the algorithm by reducing the effect of data noise [41], in Dakota's case noise being defined as the zone bleedover, by setting the minimum time period to 10s within the security model. (Fig. 10) references the demarcation point as a percentage of normal operating activity that includes a margin of error based on the data observed over a 7-day period. Activity has been correlated into three bands - normal, unusual and abnormal activity. It is evident that the normal time spent within a specific zone (location: 3rd floor) by one job role accounts for 95.5% of all activity, representing normal activity. The data defines a much smaller grouping that can be identified as unusual behaviour (3.5%). The last recorded data point for this zone was between 7-8 minutes (1.5%) and this has been designated as abnormal. Data recorded beyond this demarcation point would be considered a potential threat and an alert generated. However, a single event may not be reflective of anomalous behaviour and could generate a false positive alert. Data captured over 2 days (Fig. 10) shows how movement pattern differs on a daily basis whilst retaining the ability to detect anomalous behaviour within a complex pattern of movement. Our results were then validated against the RFID access control being the needed DW in this context, while the BC could facilitate the required integrity checks as part of the established digital CoC.

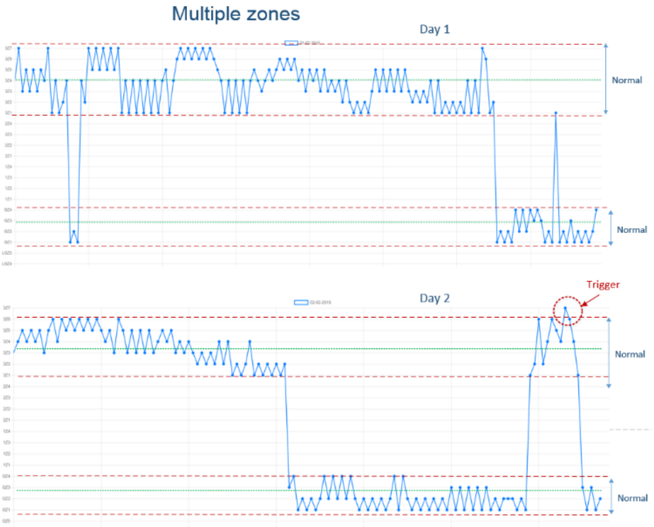


Fig. 10: Data Capture over two days for the same employee showing movement pattern with an anomalous behaviour exception alert trigger.

V. Conclusions

Conventional access control systems secure physically separated areas but still rely on human intervention to prevent unauthorized access. However, they are insufficient to address emerging threats beyond the human factor in Smart Workplaces. For example, a security personnel will have to use a special toolkit to verify the identity of drones and robots. We argue that (near) real-time detection is required to replace conventional methods but still insufficient to deal with the inherent cybersecurity weakness in Smart Environments. Therefore, we proposed a framework that incorporates forensic-readiness for post-incident investigations utilising IoT and CPS Objects as DW [33].

We outlined and discussed the threat landscape, identified key principles to be maintained by the framework and prototyped the anomaly detection capability using a Bluetooth Proximity Monitoring Solution. We have also presented the Dakota case study in which several components from our framework were implemented. we acknowledge that further prototyping is required before all the models are standardised. For example, results collected by the Bluetooth-based solution could be enhanced if combined with technologies such as GPS.

While our case study was piloted in a traditional workplace, the BTLA-Framework, by design, covers the CPN ecosystem incorporating both humans (employees) and CPS Objects. The choice of technology to support DFIR by the framework and to identify and track behavioural patterns in time series were scrutinized. Several key facets were taken into consideration in constructing the framework, such as the Parkerian Hexad elements of information security [13], safety [14], computational efficiency, privacy and integrity of the digital evidence. For example, private permissioned BC technology does not permit unauthorised parties to manage digital evidence, therefore, one of the key advantages of this approach is to maintain a digital CoC without exposing any data to the public [42] aiming to preserve object's privacy as part of the digital investigation process [43]. The strengths of the public BC include freedom, neutrality and openness, whereas any participant can volunteer to send or validate a transaction, we assert that private BCs are a better choice for Smart Workplaces since all the participants are known and permissions are restricted, therefore the support for privacy is greater. A hybrid, consortium-based BC approach is also possible in a modern shared workspace, as our case study suggests. The nodes are trusted and reliably connected at high speeds resulting in a computationally lightweight solution if compared to the significantly higher cost public BC.

The case study played a critical role in demonstrating employee behavioural attributes in relation to the participants' pattern of movement relevant to their job role. Point-based and time-series behavioural anomalies were revealed (Fig. 8 - Fig. 10). Data showed that during a set test period 95.5% of all captured activity was normal, with 3.5% being unusual and 1.5% abnormal, amounting to as little as 8 minutes' time segment. The data capture accurately detected such anomaly over a 2 and a 7 days reference period with the availability of historical data. The strength of our framework is in its ability to converge the physical and digital domain through exploiting the opportunities of human-users and connected CPS Objects.

The concept of modelling CPS Objects as DW supports DFIR and secure integrity of data using BC technology helps to achieve BC-based Digital Chain-of-Custody (CoC). The framework's architecture could be applied collaboratively across multiple domains to better realise the value of a federated BC-based technology and its impact on realising forensic-readiness at a larger scale (e.g. smart cities) [5]. The directions for future work in this area could focus on testing several models within the framework to provide further recommendations related to the usual trade-off between privacy and digital forensics, or between usability and the cybersecurity principles.

References

[1] J. Lee, B. Bagheri, and H.-A. Kao, "A Cyber-Physical Systems architecture for Industry 4.0-based manufacturing systems," *Manufacturing Letters*, vol. 3, pp. 18-23, 2015/01/01/, 2015. doi: 10.1016/j.mfglet.2014.12.001

[2] H. Haughey, G. Epiphaniou, and H. M. al-Khateeb, "Anonymity networks and the fragile cyber ecosystem," *Network Security*, vol. 2016, no. 3, pp. 10-18, 2016. doi: 10.1016/S1353-4858(16)30028-9

[3] European Union Agency For Network And Information Security (ENISA), *Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures*, 2017. doi: 10.2824/03228

[4] I. Lee, and K. Lee, "The Internet of Things (IoT): Applications, investments, and challenges for enterprises," *Business Horizons*, vol. 58, no. 4, pp. 431-440, 2015/07/01/, 2015. doi: 10.1016/j.bushor.2015.03.008

[5] R. Giaffreda, L. Capra, and F. Antonelli, "A pragmatic approach to solving IoT interoperability and security problems in an eHealth context." pp. 547-552. doi: 10.1109/WF-IoT.2016.7845452

[6] Z. A. Baig, P. Szewczyk, C. Valli, P. Rabadia, P. Hannay, M. Chernyshev, M. Johnstone, P. Kerai, A. Ibrahim, K. Sansurooah, N. Syed, and M. Peacock, “Future challenges for smart cities: Cyber-security and digital forensics,” *Digital Investigation*, vol. 22, pp. 3-13, 2017/09/01/, 2017. doi: 10.1016/j.diin.2017.06.015

[7] D. C. Plummer, V. L. Baker, T. Austin, C. Smulders, and J. Tully, “Top strategic predictions for 2016 and beyond: The future is a digital thing,” *Gartner Research G*, vol. 291252, 2015.

[8] H. A. Boyes, R. Isbell, P. Norris, and T. Watson, "Enabling intelligent cities through cyber security of building information and building systems," *IET Conference Proceedings*, 2014]. doi: 10.1049/ic.2014.0046

[9] K. Krombholz, H. Hobel, M. Huber, and E. Weippl, “Advanced social engineering attacks,” *Journal of Information Security and Applications*, vol. 22, pp. 113-122, 2015/06/01/, 2015. doi: 10.1016/j.jisa.2014.09.005

[10] B. B. Gupta, A. Tewari, A. K. Jain, and D. P. Agrawal, “Fighting against phishing attacks: state of the art and future challenges,” *Neural Computing and Applications*, vol. 28, no. 12, pp. 3629-3654, 2017/12/01, 2017. doi: 10.1007/s00521-016-2275-y

[11] F. Kammüller, J. R. C. Nurse, and C. W. Probst, "Attack Tree Analysis for Insider Threats on the IoT Using Isabelle." pp. 234-246.

[12] J. Navarro-Ortiz, S. Sendra, P. Ameigeiras, and J. M. Lopez-Soler, “Integration of LoRaWAN and 4G/5G for the Industrial Internet of Things,” *IEEE Communications Magazine*, vol. 56, no. 2, pp. 60-67, 2018. doi: 10.1109/MCOM.2018.1700625

[13] Q. Shafi, "Cyber Physical Systems Security: A Brief Survey." pp. 146-150. doi: 10.1109/ICCSA.2012.36

[14] W. Wu, R. Kang, and Z. Li, "Risk assessment method for cyber security of cyber physical systems." pp. 1-5. doi: 10.1109/ICRSE.2015.7366430

[15] J. Wurm, Y. Jin, Y. Liu, S. Hu, K. Heffner, F. Rahman, and M. Tehranipoor, “Introduction to Cyber-Physical System Security: A Cross-Layer Perspective,” *IEEE Transactions on Multi-Scale Computing Systems*, vol. 3, no. 3, pp. 215-227, 2017. doi: 10.1109/TMSCS.2016.2569446

[16] D. Gollmann, and M. Krotofil, "Cyber-Physical Systems Security," *The New Codebreakers: Essays Dedicated to David Kahn on the Occasion of His 85th Birthday*, P. Y. A. Ryan, D. Naccache and J.-J. Quisquater, eds., pp. 195-204, Berlin, Heidelberg: Springer Berlin Heidelberg, 2016. doi: 10.1007/978-3-662-49301-4_14

[17] H. al-Khateeb, G. Epiphaniou, A. Reviczky, P. Karadimas, and H. Heidari, “Proactive Threat Detection for Connected Cars Using Recursive Bayesian Estimation,” *IEEE Sensors Journal*, vol. 18, no. 12, pp. 4822-4831, 2018. doi: 10.1109/JSEN.2017.2782751

[18] E. Bajramovic, K. Waedt, A. Ciriello, and D. Gupta, "Forensic readiness of smart buildings: Preconditions for subsequent cybersecurity tests." pp. 1-6. doi: 10.1109/ISC2.2016.7580754

[19] M. Mansfield, C. Morisset, C. Gamble, J. C. Mace, K. Pierce, and J. Fitzgerald, "Design Space Exploration for Secure Building Control." p. 71.

[20] L. Mathews, “Hackers use DDoS Attack to Cut Heat to Apartments,” *https://www.forbes.com/sites/leemathews/2016/11/07/ddos-attack-leaves-finnish-apartments-without-heat/*, 2016.

[21] F. Skopik, G. Settanni, and R. Fiedler, “A problem shared is a problem halved: A survey on the dimensions of collective cyber defense through security information sharing,” *Computers & Security*, vol. 60, pp. 154-176, 2016/07/01/, 2016. doi: 10.1016/j.cose.2016.04.003

[22] M. Postránecký, and M. Svítek, "Smart city near to 4.0 — an adoption of industry 4.0 conceptual model." pp. 1-5. doi: 10.1109/SCSP.2017.7973870

[23] C. Tankard, “Advanced Persistent threats and how to monitor and deter them,” *Network Security*, vol. 2011, no. 8, pp. 16-19, 2011/08/01/, 2011. doi: 10.1016/S1353-4858(11)70086-1

[24] B. I. Kwak, J. Woo, and H. K. Kim, "Know your master: Driver profiling-based anti-theft method." pp. 211-218. doi: 10.1109/PST.2016.7906929

[25] D. Hallac, A. Sharang, R. Stahlmann, A. Lamprecht, M. Huber, M. Roehder, R. Sosič, and J. Leskovec, "Driver identification using automobile sensor data from a single turn." pp. 953-958. doi: 10.1109/ITSC.2016.7795670

[26] H. A. Boyes, R. Isbell, P. Norris, and T. Watson, "Enabling intelligent cities through cyber security of building information and building systems." pp. 1-6. doi: 10.1049/ic.2014.0046

[27] C. Oham, S. Kanhere, R. Jurdak, and S. Jha, *A Blockchain Based Liability Attribution Framework for Autonomous Vehicles*, 2018.

[28] M. Cebe, E. Erdin, K. Akkaya, H. Aksu, and S. Uluagac, “Block4Forensic: An Integrated Lightweight Blockchain Framework for Forensics Applications of Connected Vehicles,” *IEEE Communications Magazine*, vol. 56, no. 10, pp. 50-57, 2018. doi: 10.1109/MCOM.2018.1800137

[29] M. Richardson, R. Bosua, K. Clark, J. Webb, A. Ahmad, and S. Maynard, “Towards responsive regulation of the Internet of Things: Australian perspectives,” *Internet Policy Review*, vol. 6, no. 1, 2017. doi: 10.14763/2017.1.455

[30] D. B. Parker, "Toward a New Framework for Information Security?," *Computer Security Handbook*: John Wiley and Sons, 2015. doi: doi:10.1002/9781118851678.ch3

[31] S. S. K. Chuka Oham, Raja Jurdak, Sanjay Jha, “A Blockchain Based Liability Attribution Framework for Autonomous Vehicles,” *Cryptography and Security (cs.CR)*, 2018. doi: abs/1802.05050

[32] A. Nieto, R. Roman, and J. Lopez, “Digital Witness: Safeguarding Digital Evidence by Using Secure Architectures in Personal Devices,” *IEEE Network*, vol. 30, no. 6, pp. 34-41, 2016. doi: 10.1109/MNET.2016.1600087NM

[33] M. G. Gelles, *Insider threat: Prevention, detection, mitigation, and deterrence*: Butterworth-Heinemann, 2016.

[34] M. Button, “Industrial Espionage and Information Security.”

[35] D. A. Mundie, S. Perl, and C. L. Huth, "Toward an Ontology for Insider Threat Research: Varieties of Insider Threat Definitions." pp. 26-36. doi: 10.1109/STAST.2013.14

[36] P. K. Binu, R. A. Krishnan, and A. P. Kumar, "An efficient indoor location tracking and navigation system using simple magnetic map matching." pp. 1-7. doi: 10.1109/ICCIC.2016.7919537

[37] J. Haverinen, and A. Kemppainen, "A global self-localization technique utilizing local anomalies of the ambient magnetic field." pp. 3142-3147. doi: 10.1109/ROBOT.2009.5152885

[38] A. R. A. Rudin, L. Audah, A. Jamil, and J. Abdullah, "Occupancy monitoring system for campus sports facilities using the Internet of Things (IoT)." pp. 100-105. doi: 10.1109/ICWISE.2016.8188550

[39] J. Barjis, and S. Fosso Wamba, “Organizational and business impacts of RFID technology,” *Business Process Management Journal*, vol. 16, no. 6, pp. 897-903, 2010. doi: doi:10.1108/14637151011092973

[40] V. Chandola, A. Banerjee, and V. Kumar, “Anomaly detection: A survey,” *ACM Comput. Surv.*, vol. 41, no. 3, pp. 1-58, 2009. doi: 10.1145/1541880.1541882

[41] H. S. Teng, K. Chen, and S. C. Lu, "Adaptive real-time anomaly detection using inductively generated sequential patterns." pp. 278-284. doi: 10.1109/RISP.1990.63857

[42] S. Bonomi, M. Casini, and C. Ciccotelli, *B-CoC: A Blockchain-based Chain of Custody for Evidences Management in Digital Forensics*, 2018.

[43] A. Nieto, R. Rios, and J. Lopez, *IoT-Forensics Meets Privacy: Towards Cooperative Digital Investigations*, 2018. doi: 10.3390/s18020492