SN Computer Science (2022) 3:139
https://doi.org/10.1007/s42979-022-01021-3

ORIGINAL RESEARCH

Threat Modelling of Cyber Physical Systems: A Real Case Study Based on Window Cleaning Business

Sion Brown[1,2] · Stephen Fox[2] · Chaminda Hewage[1] · Imtiaz Khan[1]

Received: 5 August 2021 / Accepted: 3 January 2022

Abstract

Threat modelling Cyber-Physical System built on cloud infrastructure to monitor and manage the window cleaning operation using Window Cleaning Warehouse as a case study. Focusing on IoT data collection and cloud infrastructure security and the connections with the Cyber-Physical System. External dependencies and trust levels are defined before using trust boundaries and data flow diagrams to highlight attack surfaces. Expected scenarios from the data flow diagrams are discussed to identify violated intended use of the system using STRIDE threat classification. A risk assessment of assets that may be of interest to an adversary aid the discovery of more security risks that are then prioritised using the DREAD methodology. The results of the research present a comprehensive breakdown of vulnerabilities associated with IoT data security for route optimisation ranging from GPS spoofing, to Firestore vulnerabilities in the real-time database to Bluetooth Low Energy vulnerabilities in the IoT hardware, all of which could be common risks in cyber-physical systems designed by SME businesses. The research concludes various security risks applicable to SME businesses adopting industry 4.0 to alleviate the risk of new security breaches to the business through this adoption, increasing the likelihood of successful adoption of industry 4.0.

Keywords Cloud computing · Internet of things · Cyber physical system · Cloud security · Database security

Introduction

Industrial revolutions have governed the success of businesses for centuries with the prospect of business' success being heavily dependent on adopting progressive business models. Pioneering technology has been a catalyst for industrial revolutions with the most recent being the fourth in the form of cyber-physical systems. With technology becoming ever more intertwined with the core success of a business the systems must be threat modelled to alleviate security catastrophes and breaches. Using Window Cleaning Warehouse (WCW) as a case study the design of the cyber-physical system (CPS) is threat modelled to identify and mitigate inherent risks.

WCW is a window cleaning equipment supplier looking to adopt industry 4.0 (I4.0) technologies to monitor and optimise the window cleaning operation (WCO). High tech van systems with on-board water purification systems have revolutionised the WCO compared to a bucket and ladder approach. WCW is striving to take this technology further and develop a CPS to monitor and optimise the WCO. This is achieved through the medium of real-time data exchange between internet of things (IoT) hardware in specialised van systems and machine learning (ML) models deployed in a cloud architecture to optimise route and resources.

The research will use WCW's theoretical framework as a case study of an innovative digital supply chain for the commercialisation of real-time data. The research will focus on the digital supply chains encompassment of security and privacy along with the electronic and physical security of the hardware for real-time data. WCW propose a novel cyber-physical system that can infer dynamic resource and routing based on real-time window cleaning operation data, such as water usage. WCW will be developing the IoT hardware in house and use the digital supply chain to market business

This article is part of the topical collection "Cyber Security and Privacy in Communication Networks" guest edited by Rajiv Misra, RK Shyamsunder, Alexiei Dingli, Natalie Denk, Omer Rana, Alexander Pfeiffer, Ashok Patel and Nishtha Kesswani.

✉ Sion Brown
SionBrown_97@outlook.com

[1] Cardiff Metropolitan University, Cardiff, UK

[2] Window Cleaning Warehouse, Cardiff, UK

Published online: 20 January 2022

intelligence of the pure water usage hotspots. The novel aspect of the research is the threat modelling of the digital supply chain's real-time data in the IoT based route and resource optimisation context and the security policy as a course of action to circumvent security risks.

The threat modelling process follows the Microsoft security development lifecycle to identify potential security threats in the design and strategize risk management to reduce inherent risk severity. This process involves defining the external dependencies of the CPS for the Google Cloud Platform (GCP) cloud functions since they have a direct impact on the security of the system. External entities and their privileges to access the system is then discussed to determine their trust levels for the system, thus setting a precedence of acceptable access privileges among expected entities. To represent the system schematically and represent how data flow is expected, data flow diagrams are used with trust boundaries bordering a change of privilege in the system, to highlight attack surfaces. From the dataflow diagrams the expected data exchange scenarios are documented to clearly define intended use of the system thus making it simpler to distinguish violated intended use of the system using STRIDE threat classification. Because attackers usually act with intent an assessment of assets that may be of interest to an adversary give context to the impacts these risks can cause which is summarised using the DREAD methodology before risks are prioritised and managed.

Aims and Objectives

This section outlines aims and objectives defining the success criteria of the research project. This will be achieved by focusing on the following aims;

1. Defining the entry and exit points of the system for real-time data
2. Defining the external entities and their trust level in the digital supply chain
3. Defining the intended use of the system and its real-time routing data
4. Defining the external dependencies that are interoperable with the real-time data
5. STRIDE threat classification to identify risks relating to digital supply chain innovation
6. DREAD risk assessment of the novel real-time route and resource optimising IoT data risks
7. Specify the security measures for the identified criticalities and policy to be implemented to curb the problem

To fulfil the objective of novel research in threat modelling real-time IoT data for route optimisation based on the physical and electronic security and the digital supply chains encompassment of security and privacy of real-time data.

Scope and Constraints

The research will focus on the novel aspects which are to threat model the innovative digital supply chain of real-time IoT data for route and resource optimisation. The delimitations of the research are aspects not associated with the cloud infrastructure, IoT hardware, data exchange between these systems and the cyber-physical system. These delimitations include but are not limited to, risks associated with the underlying Flutter framework and the multiple operating systems it supports.

Related Work

The contextual background that the research will be conducted against includes;

1. The novelty of real-time IoT data for resource and route optimisation
2. The novelty of small and medium-sized enterprises (SME) digital supply chain's encompassment of security and privacy of real-time data for IoT route optimisation
3. The novelty of electronic and physical security of IoT devices to monitor resources affects the efficiency of a route

Literature review of related work to IoT data being used for resource and route optimisation is summarised as route optimisation of freight logistics based on vehicle capacity, customer time-window, the maximum travelling distance, the road capacity and traffic data [11]. Other IoT based route optimisation is based on how planned routes are performed using IoT devices to monitor vehicles and drivers to learn preferences [12]. Research has also been conducted on IoT use in waste management routing problems [13, 14].

Research objectives aligning with the literature review for real-time IoT data for route and resource optimisation is that the literature does not consider the security of the IoT data for routing problems. This is a significant knowledge gap since attacks could occur to IoT routing such as physical denial of service attacks on roads by routing all vehicles towards congested areas if the integrity of the data

is breached or a breach of confidentiality of the routes could lead to digital supply chain loses of marketable real-time data for WCW in the context of this study.

According to a review on cyber risk analytics and artificial intelligence in the industrial IoT and I4.0 supply chains [1] there are knowledge gaps for Small and mid-size enterprises (SMEs) since;

> *"the SME's digital supply chains need to encompass the security and privacy, along with electronic and physical security of real-time data"*, *"the SMEs need security measures to protect themselves from a range of attacks in their supply chains, while cyber attackers only need to identify the weakest links"* and *"the weakness of existing cyber risk impact assessment models is that the economic impact is calculated on organisations stand-alone risk, ignoring the impacts of sharing supply chain infrastructure"*.

The research expressed [1] stresses the lack of knowledge for research objectives 1–3 and how this case study will add to the body of knowledge since it is very important for SMEs looking to adopt I4.0 to have real-time data infrastructures for a more efficient production process and economies of scale [6]. The synthesis of the literature review for objective 2 is that convolutional neural networks (CNN) have been used to detect cross-site scripting attacks (XSS) in SME IoT network payloads after applying data preparation methods [4]. Critical analysis is that the CNN is used on fog compute nodes which require the integration of CNN inference and data pre-processing into self-hosted compute units. This method is expensive to develop and there are also cloud solutions readily available such as Google Cloud Armor which would be cheaper ($0.75 per million requests), easier and quicker to deploy and develop by security experts.

Bluetooth Low Energy (BLE) will be used to connect a mobile device to the IoT hardware to monitor variables affecting the route optimisation. In line with research objective 3 an exploration of prior work has revealed case studies, where unauthenticated BLE devices have been exposed allowing anyone to connect to the BLE device using a BLE sniffer. There have also been researched studies on bypassing the passkey authentication in BLE [2] and the exploration of BLE security [3]. This case study will add to the body of literature by exploring the WCW case study and look at these security risks in the context of real-time data exchange in the WCO.

After comparing and contrasting the literature to identify knowledge gaps it is clear there is a gap in knowledge about the use of real-time IoT data for resource and route optimisation that this paper will address. This paper's contributions will also be in the form of building knowledge for SME's digital supply chain's security and privacy of real-time IoT data for route optimisation. The final contribution to knowledge gaps in the electronic and physical security of IoT devices is to monitor resources affecting the efficiency of a route which is presented in this paper.

Research Methodology

To fulfil the research objective the data is collected through a non-probabilistic convenience sample using WCW as a case study of a theoretical CPS design. The data analysis method is grounded theory [5] which is a systematic method of constructing hypotheses, and theories of possible security risks based on the threat modelling of the design of the CPS. Since ideas and concepts of security risks become apparent from the qualitative threat model data they can then be succinctly summarised with codes and grouped into threat classifications before being analysed further to discuss risk severity, impacts and mitigations.

Entry and Exit Points

The confidentiality, integrity and availability of the real-time data are important since it is a fundamental part of the CPS and the digital supply chain. Figure 1 shows an abstract view of the architecture consisting of the components used to monitor the WCO.

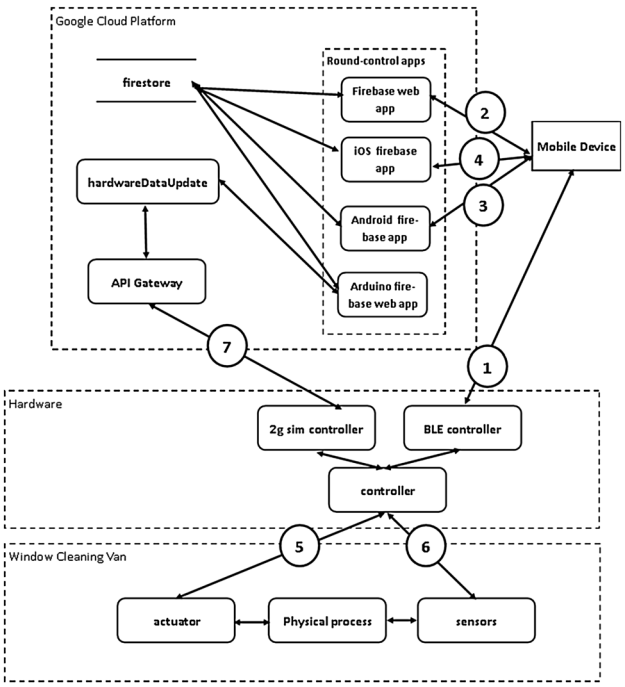

Fig. 1 CPS architecture overview

Round-Control's data is to be stored on GCP's FireStore which is a real-time NoSQL database. Only authorised WCW staff can create, read, update, delete (CRUD) and make backups of the data through the GCP console. It is encrypted automatically by GCP but is decrypted to read in the Firebase console through an authenticated admin account. The IoT hardware is composed of Arduino components consisting of an HM-10 Bluetooth Low Energy (BLE) transceiver enabled microcontroller, inflow and outflow Hall Effect sensors, temperature sensor, fill level sensor, total dissolved solids (TDS) inflow and outflow and a Global Positioning System (GPS) sensor. The Flutter application on the mobile device can connect to the hardware via BLE and forward the real-time data to the platform-specific Firebase app endpoint. The communication with the Firebase app endpoints is authenticated via Firebase Authentication which requires validation of email ownership. The Flutter application is authenticated to use the Firebase app using the Firebase app credentials for each platform. Changes made to the Firestore is broadcasted to all authenticated users signed in that have access to that user's data in the Firestore so the real-time data of the IoT hardware is updated in real-time across Android, iOS, Linux, Windows, macOS and web derived apps.

It is important to define the external entities and their trust levels to access the system. The expected entities are presented in Table 1.

Figure 1 illustrates the data flow and trust boundaries but does not intuitively describe the expected scenarios and the intended use of the system to identify deviations. The intended use of the system is presented in Table 2.

Scenarios deviating from the intended scenarios of the system in Table 2 help identify violated deployment of the application and intended use of the system thus impacting the security of the system.

External Dependencies

The external dependencies are directly interoperable with the system. The external entities relating to the real-time data are presented in Table 3.

STRIDE Threat Classification

The qualitative data collected about WCW's adoption of I4.0 is analysed in this section for risks by analysing the intended use, external dependencies, and the descriptions of the data flow diagrams. The qualitative data can

Table 1 Trust level of external entities

Entity	Privilege description
Firestore admin	Has access to the Firestore database with create, read, update and delete capabilities. Can manually make backups of the database. Can edit the security rules for the database and the indexing for the NOSQL data
Web client	Round-Control users using the web app. Has access to the Firebase Hosting Flutter website which is connected to the Firebase Web App which is the intermediary to access the Firestore database to create, read, update and delete data for the authenticated user session. Can also create, read and update Firebase Authentication data. For enterprise subscriptions of the app, only enterprise admin accounts can delete jobs and their data
Android device	Round-Control users using an Android device. Hosts the Android Flutter app or can be used to access the app using the web client on the device. Is able to access the Android Firebase app endpoint to create, read, update and delete data to the Firestore database for the Authenticated user session. Can also create, read and update Firebase Authentication data. For enterprise subscriptions of the app, only enterprise admin accounts can delete jobs and their data
iOS device	Round-Control users using an iOS device. Hosts the iOS Flutter app or can be used to access the app using the web client on the device. Is able to access the iOS Firebase app endpoint to create, read, update and delete data to the Firestore database for the Authenticated user session. Can also create, read and update Firebase Authentication data. For enterprise subscriptions of the app, only enterprise admin accounts can delete jobs and their data
WCO IoT hardware	The Arduino controller and sensors were developed by WCW to monitor the WCO. Can either be used to connect to a mobile device via Bluetooth Low Energy to monitor IoT data or can send the IoT data via the integrated 2 g sim card to the Application Programming Interface (API) Gateway endpoint using an API key in the Hypertext Transfer Protocol (HTTP) POST request. Can also control the actuators in the WCO van and receive data from the sensors connected to the van equipment

Table 2 Intended use of the system

ID	Scenario/circumstance	Description	Trust level
1	Mobile device connects to Bluetooth Low Energy (BLE) controller	The iOS and Android mobile devices should connect to the hardware via an authenticated BLE connection to monitor and control the hardware in the WCO. Currently, there is no authentication on pairing only identification. Data is received from the BLE controller every 500 ml variation in the inflow/outflow water of the WCO physical process	Android device, iOS device
2	Mobile device connects to FireBase web app	The Flutter web app can be accessed via the Firebase Hosting website. The web client on the mobile device should not be able to connect to the BLE controller, since the external dependency used (flutter_blue) does not currently support Bluetooth via JavaScript on Flutter Web. The intended use is, therefore, limited to being able to see the real-time data exchange for the job on the web that has been instigated either on the Arduino or an Android, iOS or Mac OS device. The web client should, therefore, only be able to receive real-time Firestore data exchange of IoT data being written to the Firestore	Web client, Android device, iOS device
3	Mobile device connects to FireBase Android app	The Android app should be able to connect to the Firebase Android app to create, read, update and delete job monitoring data for the authenticated Firebase user for the specified job. The deletion of jobs for enterprise subscriptions is limited to enterprise admin accounts	Android device
4	Mobile device connects to FireBase iOS app	The iOS app should be able to connect to the Firebase iOS app to create, read, update and delete job monitoring data for the authenticated Firebase user for the specified job. The deletion of jobs for enterprise subscriptions is limited to enterprise admin accounts	iOS device
5	Controller communicates with actuators	The actuators are installed on the van system in the form of components to open and close water valve outlets, components of the water pump to begin and stop pumping water to the WCO brushes and pump components to pump source water through the reverse osmosis (RO) system into the pure water storage tanks. The controller can send a control signal to the actuators which will use a battery source as energy to enable the physical process of the WCO	IoT hardware
6	Sensors data to controller	Data is provided to the controller every 3 s from the sensors	IoT hardware
7	2 g sim controller connects to API gateway	If the controller is being used without a Bluetooth connection then the data is sent to the API gateway via an HTTP POST request which requires a valid API key. Authentication of the Firebase user and selection of job to monitor is to be done on the Arduino to assign the data to the correct user and job in the Firestore database	IoT hardware

Table 3 External dependencies

Cloud function	Package name	Source	Description
ShopifyTargetedAdvert	requests	https://docs.python-requests.org/en/master/	Used to call the Shopify API using a Hypertext Transfer Protocol Secure (HTTPS) GET request to get the information needed about customer purchase history and similar items to the last three purchases via their email address. Also used to get adverts based on job IoT data to detect filter fouling
HardwareDataUpdate	pyrebase	https://github.com/thisbejim/Pyrebase	Used to authenticate Firebase Authentication user to assign the data from the IoT van hardware to an authenticated user with only using the van 2 g sim instead of the Flutter app
HardwareDataUpdate	jwt	https://github.com/GehirnInc/python-jwt	The python implementation of JavaScript Object Notation (JSON) Web Token is used by Pyrebase to securely transmit the information as a JSON object which is trusted, because it can be digitally signed and verified
HardwareDataUpdate	google-cloud-firestore	https://github.com/googleapis/python-firestore	A python package which is an official google APIs implementation used to write the IoT data to the Firestore database

be succinctly summarised through a thematic grouping of threats into STRIDE classifications. STRIDE is an acronym for spoofing, tampering, repudiation, information disclosure, denial of service and elevation of Privilege. The derived data from the data flow diagram in Fig. 1 can be succinctly summarised as threat classifications of STRIDE as presented in Table 4.

Risk Assessment

The identified risks severity is quantified using the DREAD risk assessment model. DREAD is an acronym for damage, reproducibility, exploitability, affected users and discoverability. Each category is given a rating from 1 to 10, where 10 is the worst. The sum of the ratings helps to prioritise risks. The DREAD methodology for risk assessment is typically inconsistent among assessors and ratings tend to be subject to debate so the rationale for the ratings is provided (Table 5).

Discussion of Risks and Mitigation

The high prioritised risks and their mitigation is discussed in this section and their novel contribution to real-time IoT data security for route and resource optimisation. The novel aspects of the research is the threat modelling of real-time IoT data for route optimisation for the physical and electronic security of the system as well as the digital supply chains encompassment of security and privacy of real-time data. Through literature review, the common variables used for routing are presented in Table 6.

To address risks 18, 19 and 20 the Bluetooth module should enforce pin pairing where the pin for the van system hardware is generated differently for each van installation and provided to the customer. The HM-10 BLE module should be genuine by having a crystal fitted alongside the bottom four solder connections otherwise you cannot add pin authentication.

Table 4 STRIDE threat classification

DFD Element	Threats
Firestore	Tampering with the data in Firestore through the User Interface (UI) by accidentally deleting data (1). Non-repudiation without the Firestore rules, because the allowed actions should be limited (2)
2 g sim	Physical denial of service through being covered to not omit 2 g signal (8). 2 g was created in 1991 and encryption between tower and device can be cracked in real-time to disclose information, since HTTP POST is used and the users' Firebase Authentication details and password and email is not encrypted before sending over 2 g (9). Non-repudiation is caused by the system not being able to have enough evidence to prove that it should deny a malicious process, since there is no authentication between the tower and 2 g enabled hardware (10). Spoofing is an issue, since a man in the middle attacks can happen as someone posing as a 2 g tower is possible due to no authentication between device and tower (11). Tampering with the data is possible with a man in the middle attacks (12)
IoT sensors	Due to the significant number of sensors the attack surface is quite broad for compromising sensors for example if the sensor is unauthenticated then a spoofing attack can occur where false sensor signals are injected causing malicious data input like the considered by Huang et al. [7] (14). An example of spoofing attacks on IoT sensors is using laser microphones [8] where oscillating laser signals from a fixed location can deflect off of the microphone receiver and cause vibrations mimicking audio signals. Tampering with the Hall Effect sensors could compromise the validity of the water flow which might happen if there are incentives to reduce water usage on jobs (15). Denial of service attacks can happen on the path between the sensors, since they are exposed in the van system by delaying or blocking the transmission aiding stale data attacks (16)
GPS mobile	GPS spoofing on the mobile device is easy using free PlayStore and App Store apps (21)
Arduino controller	Tampering with the Arduino controller is possible, since it is easily accessible so compromising the controller can send incorrect control signals to the actuators [9] (13). A denial of service attack to the user can happen through compromising actuators through zero dynamics attacks, since the actuators are exposed so the actuator will execute a different command than what was intended by the controller [10] (17)
BLE	Denial of service since only one BLE connection at a time (18). Connecting to the BLE and operating the actuators in the van while not being the owner of the van system is a spoofing attack (19). If the IoT device is operated without a mobile device and there is currently no signal then data is stored in temporary memory on Arduino which could be erased if an adversary connects and modifies the data by beginning a process (20)
Shopify targeted advert	Information disclosure and spoofing, since API Gateway API keys are programmed into Flutter code and not encrypted so access to API key allows an adversary to pose as an email address owner to find their purchase history (3)
API Gateway	Denial of service, since the number of invocations of cloud functions is not capped so spamming requests to a cloud function could yield a big bill (4). Spoofing since API keys are sent in the HTTP POST request URL and can be obtained (5)
Hardware Data Update	Pyrebase is required, since using API key alone to access API gateway is unsafe, since the API key is quite easy to obtain through social engineering or other vulnerabilities discussed. Authentication with Firebase Authentication is required before being able to change data in the database but Pyrebase is not an official Google package so could have vulnerabilities allowing for tampering (6). Not restricted to a number of invocations so denial of service through large compute bill (7)

Conclusion

The researcher set out to bridge the identified knowledge gap through threat modelling real-time IoT data for route optimisation based on the physical and electronic security of the system as well as the digital supply chains encompassment of security and privacy of real-time data using WCW as an SME case study. The main points of the research summarise that numerous cyber security vulnerabilities have been found with particular focus on real-time data exchange that other SMEs can consider when designing CPSs. The results are significant, since IoT data transmission enabled by 2 g is

Table 5 Risk assessment of threats

ID	D	R	E	A	D	Total	Rationale
1	1	2	1	1	1	6/50	Minimal damage as the database is backed up twice a day. The rights and freedoms of the individual's data through GDPR is not affected. It is difficult to reproduce the attack, since Firestore makes you type in to confirm the deletion
2	10	4	6	10	2	32/50	The damage would be high, since Firestore CRUD operations could be performed. The affected users would be WCW customers and their customers and WCW
3	8	7	3	10	8	36/50	Quite difficult to decompile into dart code from Android application Package (APK). High damage to WCW
4	10	10	8	10	9	47/50	Uncapped cloud function invocations could yield an extortionate GCP bill for WCW and might be too much to pay to cause bankruptcy affecting the whole supply chain
5	10	10	9	8	10	47/50	Getting a user's API key could mean that an adversary can use the systems services and the API key owner would be billed
6	8	9	9	10	9	45/50	If Pyrebase was illegitimate then they would have full access to the Firebase services for the project
7	10	10	8	10	9	47/50	Same as risk 4
8	1	10	10	1	10	32/50	The attack is easy to reproduce and does not take much technical knowledge
9	10	7	5	9	8	39/50	The attack is severe, since users Firebase credentials are exposed. The affected users would be the user, their customers and WCW
10	10	7	5	9	8	39/50	The phone can't authenticate a legitimate 2 g receiver so and the same rationale as risk 9 applies
11	10	8	5	9	8	40/50	The same rationale as risk 10
12	10	9	4	10	8	40/50	The attack is easier to reproduce, since the HTTP packet structure is consistent and once the data structure is found data can be modified automatically through a malicious parsing program
13	2	10	10	1	9	32/50	The controller is easily accessible
14	2	3	2	1	5	13/50	The damage is to the validity of the compromised sensors data. Physical access to the sensor and modification is required
15	2	10	10	1	10	33/50	Easy to tamper with the sensor to make it not work anyone can do it without technical knowledge
16	2	6	4	1	3	16/50	Modification of the data transmitted through the wire connecting sensor and controller is not particularly easy
17	4	3	4	1	2	14/50	The actuators control things such as the outlet valves and pumps, so pumps can be broken by building pressure
18	4	10	10	4	10	38/50	Anyone within range and a BLE device can perform the attack
19	6	10	10	4	10	40/50	Can turn the pumps on and cause damage
20	2	10	10	4	10	36/50	This would cause data loss for that job
21	8	10	10	10	8	46/50	GPS spoofing could cause sub-optimal routes to be taken by affecting traffic data

likely to be considered for real-time data exchange by other SMEs, since it is low cost but the vulnerabilities discussed are significant. The significance of the risks found with BLE is also likely to apply to many other SME CPS projects.

The technical achievement of the paper is its identification of security vulnerabilities for novel IoT route optimisation variables and the proposed security measures and policies to circumvent, manage and monitor the risks.

Table 6 Security measures and policy to mitigate and monitor threats

Control variable	Relating research	Relating threats	Mitigation and monitoring
Vehicle capacity	[11, 13, 14] and this study	5, 8, 9, 10, 11 and 12	Risks 5 can be addressed by storing the API key associated with the user in the Firestore database to then check that the API key used is associated with the authenticated user Risks 8, 9, 10, 11 and 12 can be completely averted using a more secure mobile network protocol such as 3 g, 4 g or 5 g, but measures against 2 g downgrade attacks should be considered to stop downgrade back to 2 g. For risk 9 the user's password should also be encrypted before transmission as an extra security measure
Travel distance	[11–14] and this study	4 and 7	To calculate travel distance based on roads the GCP Directions API is commonly used. The billing for this is \$5(~£3.67) per 1000 requests. Risks 4 and 7 relate to uncapped Cloud Function invocations. WCW is looking to build a digital supply chain for business intelligence that is fully scalable. The security measures to mitigate risks 4 and 7 is to cap the number of requests per minute from an Internet Protocol (IP) address and cap the number of function instances that can be invoked in parallel. Monitoring the risk would be in the form of monitoring the user base growth to ensure that the CPS is not hindering genuine requests by limiting the number of function instances
Road traffic data	[11–14] and this study	21	Security measures to circumvent risk 21 of spoofing GPS location of a mobile device to simulate standstill traffic on a popular road would be to implement mobile device side code to detect mock locations. In Android 17 this can be done through Setting. Secure to detect if ALLOW_MOCK_LOCATION is enabled. On Android 18 and above the Location.isFromMockProvider() API can be used. On iOS it is possible to detect if the iPhone is jailbroken that suggests the user could be spoofing their location
Historic preferences	[12] and this study	1 and 2	A policy to circumvent tampering with data in the firebase UI (risk 1) is to set up a Cloud Scheduler to publish a topic every specified duration that a Cloud Function is subscribed to. It would then be possible to write a Cloud Function in Node.js to back up a copy of the Firestore database to a Google Storage Bucket for disaster recovery, with the added benefit of having an offline data set you could export to a Comma-Separated Values (CSV) file using GCP's Big Query. The monitoring of the risk would be to check the Cloud Function logs to ensure it is being invoked routinely. Security measures addressing risk 2 are to implement Cloud Firestore Security Rules to restrict read and write access to authenticated users with verified emails. Further restricting the privileges of the users to roles is recommended so not any logged-in user has read and write access to entire database. Firebase Admin Software Development Kit (SDK) and Cloud Functions can still access the database regardless of closed access. It is, therefore, recommended to restrict access to public Cloud Function endpoints using API Gateway to enforce an OpenAPI specification with security definitions for API keys and authentication. Monitoring the risk would be in the form of setting up local unit tests using JavaScript version 9 SDK

Funding Funded by a Knowledge Transfer Partnership (KTP) between Cardiff Metropolitan University and Window Cleaning Warehouse. Grants for the KTP are in the form of a 67% contribution by the Welsh Government.

Availability of Data and Materials The authors confirm that the data supporting the findings of this study are available within the article [and/or] its supplementary materials.

Code Availability Code is maintained on a private GitHub repository and is property of Window Cleaning Warehouse.

Declarations

Conflict of Interest The authors are involved in a KTP. It is in the interest of the corresponding author to ensure the success of the KTP, exhaustive of cyber-security.

Ethical Approval No ethics approval is needed, since research does not deal with human participants or human tissue, and is not sensitive, deceptive or covert according to the University Ethics Committee at Cardiff Metropolitan University.

Consent to Participate No humans were involved in the participation of the research, since it was a theoretical threat analysis of the design of a cyber-physical system.

Consent for Publication Window Cleaning Warehouse give consent for publication.

References

1. Radanliev P. Cyber risk at the edge: current and future trends on cyber risk analytics and artificial intelligence in the industrial internet of things and industry 4.0 supply chains. Cybersecur. 2020. https://doi.org/10.1186/s42400-020-00052-8.
2. Rosa T. Bypassing Passkey Authentication in Bluetooth Low Energy. In: Cryptology ePrint Archive. 2013. https://eprint.iacr.org/2013/309.pdf Accessed 29 Jul 2021.
3. Ryan M. Bluetooth: With Low Energy Comes Low Security. In: USENIX. 2013. https://www.usenix.org/conference/woot13/workshop-program/presentation/ryan Accessed 29 Jul 2021.
4. Chaudhary P, Gupta B. Enhancing big data security through integrating XSS scanner into fog nodes for SMEs gain. Technol Forecast Soc Change. 2021. https://doi.org/10.1016/j.techfore.2021.120754.
5. Glaser B, Strauss A. The discovery of grounded theory: strategies for qualitative research. 1st ed. Milton Park: Routledge; 2000.
6. Nagy J, Olah J. The Role and Impact of Industry 4.0 and the Internet of Things on the Business Strategy of the Value Chain—the Case of Hungary. MDPI. 2018; https://www.mdpi.com/2071-1050/10/10/3491/pdf. Accessed 3 Oct 2021.
7. Huang Y, Cárdenas A. Understanding the physical and economic consequences of attacks on control systems. Int J Crit Infrastruct Protect. 2009;2(3):73–83.
8. Chounlakone M, Alverio J. The Laser Microphone. In: System Design. MIT. 2017. https://web.mit.edu/6.101/www/s2017/projects/jalverio_Project_Final_Report.pdf. Accessed 29 Jul 2021. Accessed 3 Oct 2021.
9. McLaughlin S. CPS: Stateful policy enforcement for control system device usage. ICPS. 2013. https://doi.org/10.1145/2523649.2523673.
10. Shim H. Zero-dynamics Attack, Variations, and Countermeasures. In: arXiv.org. 2021. https://arxiv.org/abs/2101.00556. Accessed 3 Oct 2021.
11. Lai M, Yang H, Yang S, Zhao J. Cyber-physical logistics system-based vehicle routing optimization, In: Research Gate. 2014. https://www.researchgate.net/publication/267179315_Cyber-physical_logistics_systembased_vehicle_routing_optimization. Accessed 3 Oct 2021.
12. Saijun S, Gangyan X, Ming L. The design of an IoT-based route optimization system: a smart product-service system (SPSS) approach. Adv Eng Inform. 2019;42:101006.
13. Khoa T, Phuc C. Waste management system using IoT-based machine learning in university. Wirel Commun Mobile Comput. 2020. https://doi.org/10.1155/2020/6138637.
14. Medvedev A, Fedchenkov P. Waste management as an IoT-enabled service in smart cities. Internet of things, smart spaces, and next generation networks and systems. Cham: Springer; 2015. https://doi.org/10.1007/978-3-319-23126-6_10.