frontiers | Frontiers in Communications and Networks

TYPE Original Research
PUBLISHED 30 November 2023
DOI 10.3389/frcmn.2023.1096841

OPEN ACCESS

EDITED BY
Adnan Anwar,
Deakin University, Australia

REVIEWED BY
Riadul Islam,
University of Maryland, United States
Pramod Mathew Jacob,
Providence College of Engineering and School of Business, India

*CORRESPONDENCE
Michele Maasberg,
maasberg@usna.edu

RECEIVED 12 November 2022
ACCEPTED 14 November 2023
PUBLISHED 30 November 2023

CITATION
Maasberg M, Butler LG and Taylor I (2023), Key parameters linking cyber-physical trust anchors with embedded internet of things systems.
Front. Comms. Net 4:1096841.
doi: 10.3389/frcmn.2023.1096841

Key parameters linking cyber-physical trust anchors with embedded internet of things systems

Michele Maasberg[1]*, Leslie G. Butler[2,3] and Ian Taylor[4]

[1]Department of Cyber Science, United States Naval Academy, Annapolis, MD, United States, [2]Department of Chemistry, Louisiana State University, Baton Rouge, LA, United States, [3]Refined Imaging LLC, Baton Rouge, LA, United States, [4]SIMBA Chain, Plymouth, IN, United States

Integration of the Internet of Things (IoT) in the automotive industry has brought benefits as well as security challenges. Significant benefits include enhanced passenger safety and more comprehensive vehicle performance diagnostics. However, current onboard and remote vehicle diagnostics do not include the ability to detect counterfeit parts. A method is needed to verify authentic parts along the automotive supply chain from manufacture through installation and to coordinate part authentication with a secure database. In this study, we develop an architecture for anti-counterfeiting in automotive supply chains. The core of the architecture consists of a cyber-physical trust anchor and authentication mechanisms connected to blockchain-based tracking processes with cloud storage. The key parameters for linking a cyber-physical trust anchor in embedded IoT include identifiers (i.e., serial numbers, special features, hashes), authentication algorithms, blockchain, and sensors. A use case was provided by a two-year long implementation of simple trust anchors and tracking for a coffee supply chain which suggests a low-cost part authentication strategy could be successfully applied to vehicles. The challenge is authenticating parts not normally connected to main vehicle communication networks. Therefore, we advance the coffee bean model with an acoustical sensor to differentiate between authentic and counterfeit tires onboard the vehicle. The workload of secure supply chain development can be shared with the development of the connected autonomous vehicle networks, as the fleet performance is degraded by vehicles with questionable replacement parts of uncertain reliability.

KEYWORDS

embedded sensors, internet of things, cyber-physical trust anchor, secure supply chain, blockchain

1 Introduction

Consider the question "Why will a modern automobile, with over 100 million lines of code,[1] tolerate the installation of counterfeit parts?" The modern automobile has exceptional computational power and facile Internet access to secure databases (Zhang et al., 2022) which, when combined with embedded sensors and Internet of Things (IoT) concepts, have

1 Millions of Lines of Code, https://informationisbeautiful.net/visualizations/million-lines-of-code/

the potential to facilitate part authentication along the automotive supply chain from manufacture through installation and acceptance by connected and autonomous vehicle driving networks. Herein, we ask what can be done in the repair process to ensure authentic parts are installed during automotive repairs?

In this work, we review the magnitude of the counterfeit automobile parts problem and attempted solutions. The automobile counterfeit problem ranks fourth among commodity items in commerce today, with deadly results for the vehicle occupants. Today, parts are usually validated based on identifying marks on packaging, which is inadequate, hence the motivation for embedded sensors as described in this Journal.

We note the rapid growth of research in the cyber security of vehicles, infrastructure, and autonomous vehicles. We suggest that forthcoming autonomous vehicle policies should include required processes for counterfeit detection of repair parts installed in the autonomous vehicles else the system-wide failure rate due to counterfeit items on members of the autonomous fleet will become unacceptable.

Our contributions are summarized as follows.

- We develop an architecture for anti-counterfeiting in automotive supply chains with key components linking a trust anchor with systems, data, sensors, and monitoring.
- We advance trust anchor technology and develop a new model based on acoustic signatures for installed automotive components linked to embedded sensors systems.
- We integrate cost effective security features into the process.

The rest of the paper is organized as follows. Section 2 presents a background and review of current anti-counterfeiting technologies for automotive embedded systems, highlighting the gaps for a secure supply chain. In section 3, the architecture is developed based on key components linking the technology and systems, integrating a current model. In Section 4, the model is advanced for automotive embedded systems, incorporating acoustic signature for authentication along with discussion and analysis of this work. In Section 5, conclusions and future work are discussed.

2 Background

2.1 Magnitude of the problem

Counterfeit automotive parts pose serious risks to public safety. They are among the most dangerous counterfeits due to risk of harm, injury, or death.[2] According to the World Health Organization, approximately 1.3 million deaths and 20–50 million injuries annually are caused by motor vehicle accidents; in India, approximately 20% of the accidents are attributed to counterfeit automotive parts (Shen et al., 2022).

Automotive parts and electronics are currently among the top four most commonly counterfeited products.[3] Demand for counterfeit automotive parts has nearly tripled in the wake of the global COVID-19 pandemic due to increased costs and shortage of replacement parts. The integration of automotive embedded devices in IoT further increased demand for fake parts due to a shortage in electronic components.

The magnitude of automotive counterfeiting is staggering. Toyota Australia recently reported that 62% of their products online were counterfeit.[4] BMW has reported fakes from Amazon, eBay, and other online marketplaces. German automaker Daimler AG discovered $1.7 million in counterfeit parts in 1 year. In July 2021, U.S. Customs and Border Protection seized 5,657 counterfeit ($295,302) vehicle parts from China. In 2022, automotive parts suppliers in three retail stores were charged with selling counterfeits in New York.

Counterfeiters tend to focus on profitable automotive parts that are most often replaced. Commonly counterfeited auto parts include brake pads, lights, tires, rims, windscreens, and body parts. These parts are counterfeited in high volumes, and they can lead to premature failure, injuries, and accidents. Figure 1[5] depicts commonly counterfeited parts that are particularly dangerous, including airbags, engine components, and brakes.

The detection of counterfeit automobile parts should be coordinated with the growing field of cyber security of autonomous vehicles. The research activity in this field is, recently, very high. For example (Kennedy et al., 2019), discuss automotive cyber security from the viewpoint of criminology theory and vehicle-related cybercrime. Especially pertinent to this work is the role of guardianship strategies. Collaboration and information sharing among automakers, suppliers, policymakers, and security researchers is an effective approach counterfeit and other cybercrime prevention.

There is an opportunity to merge counterfeit prevention with the cyber technologies and policies under development protecting vehicles. Ensuring security of authentication systems poses a significant challenge. Advanced anti-counterfeiting architectures are based on embedded systems, IoT, sensing, networking, and communication technologies. Currently, these technologies in vehicles are vulnerable. A remote attack was demonstrated in 2015 by security researchers with the compromise of a 2014 Jeep Cherokee's electronic functions.[6] The researchers were able to control everything from locks to steering by attacking the Jeep's Controller Area Network (CAN) bus system through the entertainment system. Further research into connected vehicle vulnerabilities revealed that the on-vehicle computer and communication systems are unsecured. (Hashem Eiza and Ni, 2017; El-Rewini et al., 2020; Khan et al., 2020; Aliwa et al., 2021; Elkhail et al., 2021; Khan et al., 2022; Labrado et al., 2022). Other connected vehicles communications could be compromised, including transmission of geolocation data (Kumar et al., 2019),

2 Counterfeit Goods: A Danger to Public Safety. https://www.ice.gov/features/dangers-counterfeit-items

3 The 4 Most Common Counterfeit Products. https://nabcore.com/top-4-most-common-counterfeited-products/

4 Toyoto Australia sting finds parts purchased online are often fake. https://www.drive.com.au/news/counterfeit-car-parts-renewed-warnings-after-an-increase-in-busts/

5 Commonly counterfeited automotive components. https://a2c2.com/resources

6 Jeep Hacking 101: https://spectrum.ieee.org/jeep-hacking-101\#toggle-gdpr

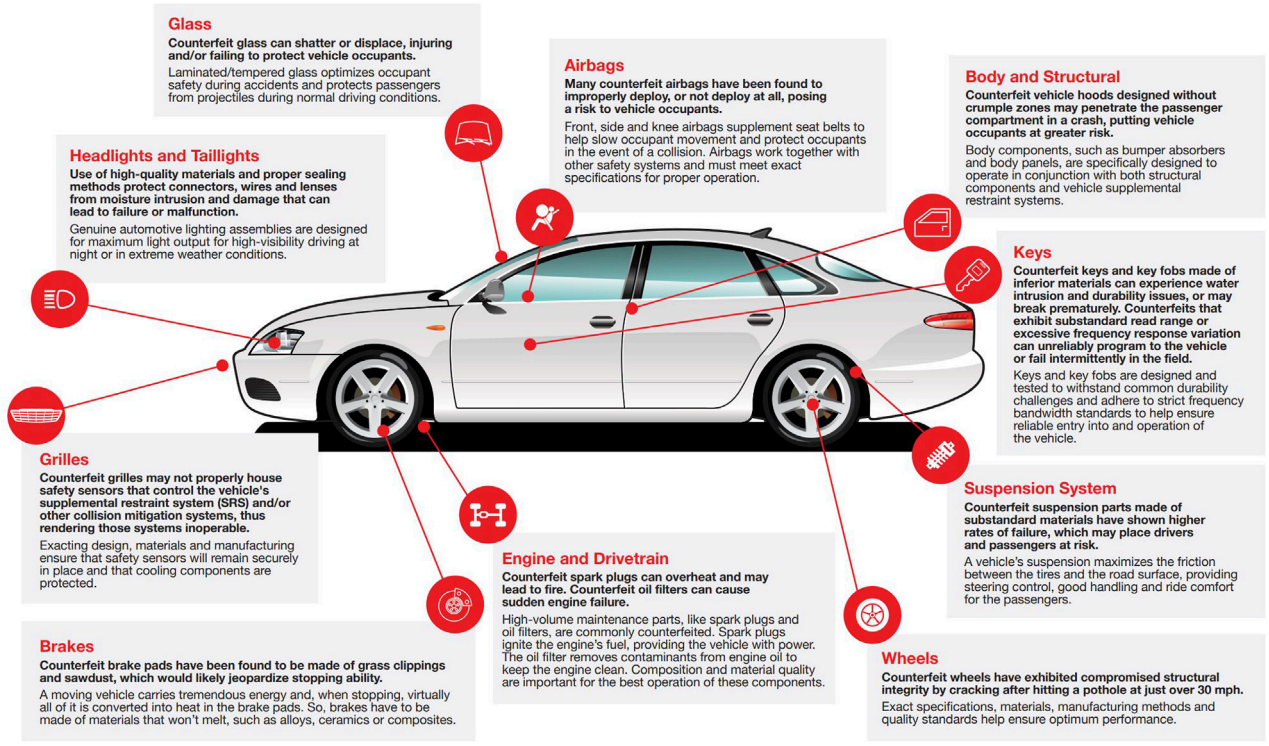

FIGURE 1
Commonly counterfeited high risk automotive components. Source: reproduced with permission from Automotive Anti-Counterfeiting Council (A2C2), 2023[5].

communication with charging stations for electric vehicles (Acharya et al., 2020), and communication with traffic signals (Feng et al., 2022). If vehicle systems are not secured, then counterfeit detection and monitoring systems could also be easily compromised.

In the next section, we review current anti-counterfeiting strategies and highlight the gaps in anti-counterfeiting technology for automotive supply chains.

2.2 Current anti-counterfeiting strategies

The automotive industry relies heavily on customer education to fight counterfeits. One of the leading recommendations for customers to spot fakes is inspection of the packaging. The automobile parts supply chain relies heavily on packaging to establish part authenticity. Figure 2 shows an example of authentic and counterfeit packaging, where color and print errors reveal the counterfeit part.[7] A true counterfeit, as opposed to a generic replacement, copies the appearance, dimensions, color, and logos of an authentic part down to the packaging. Counterfeiters often fail at reproducing packaging that is hard to duplicate. However, they are continuously enhancing their techniques to replicate intricate packaging on a larger scale.

Another leading strategy to avoid automotive counterfeit components is to encourage customers to purchase from a legitimate source. A recent arrest of automotive parts suppliers in the U.S. for selling counterfeit auto replacement parts demonstrates that packaging and validity of supplier are ineffective with the increasing sophistication of counterfeiters.

Automakers, Original Equipment Manufacturers (OEM), and suppliers play integral roles within the automotive supply chain, wherein each entity bears a significant responsibility to prevent counterfeits. Recently, these companies have stepped up their efforts to combat counterfeit parts. For example, many have issued counterfeit warnings, initiated lawsuits against counterfeiters, embarked on counterfeit education campaigns, and become members of anti-counterfeiting organizations like Automotive Anti-Counterfeiting Council (A2C2)[6]. For example, BMW and Honda both issued counterfeit product alerts and guidance on how to spot fakes. BMW also tracks the sources of fakes from customers, which include Amazon, eBay, other online vendors, and retail stores.

A Google search of "Gates timing counterfeit" yields websites sponsored by Gates Corporation in their effort to ensure a secure supply chain. Unfortunately, counterfeit timing belts have entered the automobile parts supply chain. One feature available through the website is authentication via a serial number. Unfortunately, the serial number is printed on the opaque package, so the contents are not easily verified.

7 ACDelco, General Motors, https://www.acdelco.com/content/dam/acdelco/na/us/en/index/counterfeit-parts/02-pdfs/acdelco-counterfeit-article.pdf, (accessed: 04.04.2021)

FIGURE 2
ACDelco's authentic packaging (left) has been copied, as shown on the right, for a fake spark plug.

The current anti-counterfeiting strategies in the automotive supply chain are insufficient. Multi-pronged anti-counterfeiting efforts and methods are needed as counterfeiting becomes more sophisticated. Physical, cyber-physical, and technical anti-counterfeiting techniques and processes must be implemented in conjunction with legal measures to secure the automotive supply chain.

2.3 Supply chain and the need for anti-counterfeiting technology

The supply chain is vulnerable in the absence of anti-counterfeiting technology. A recent lawsuit revealed a problem with Kona coffee, coffee grown in Hawaii (Bruce Corker et al. v. Costco Wholesale Corp. et al., 2:19-CV-00290-RSL (Western District of Washington at Seattle, 25 June 2021). The annual Kona coffee bean production in Hawaii was 2.7 million pounds, yet annual retail sales exceeded 20 million pounds. Farmers in the Kona region of Hawaii sued more than 20 retailers for selling counterfeit coffee after lab testing revealed that beans being sold were not from Kona. While the lawsuit reimburses the farmers, it is not at all clear if the underlying problem is solved.

The Kona coffee lawsuit illustrates the cost to legitimate companies incur from counterfeiting. In the automotive supply chain, manufacturers lose approximately $2 billion annually to counterfeit tires and batteries. Virtually any automotive part can be counterfeited, as shown in Figure 1. The automotive supply chain also includes the aftermarket and spare parts, where the prevalence of counterfeit parts is increasing. Figure 3 shows mission critical parts, one of which is counterfeit.[8] Chemical analysis would show the authentic part to have a metal-ceramic pad whilst counterfeit brake pads has been found with cellulose/resin composites and to have extremely poor braking performance. We note the absence of any authentication mechanism on the part.

Current supply chain risk management standards require tests and inspections to determine component authenticity.[9] Inspection to verify part identity requires technologies to facilitate authentication. The United States National Institute of Standards and Technology (NIST) refers to technologies that verify identity of authentic hardware and software in digital environments as a "trust anchor." The NIST mission statement is "To promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life." In April 2022, the NIST center, the National Cybersecurity Center of Excellence (NCCoE) published the report NIST.IR

8 Toyota Tacloban, Leyte, Inc., Leyte, Philippines, https://toyotatacloban.com/toyota-genuine-parts

9 SAE Aerospace Standard (AS) AS6171 https://www.sae.org/standards/content/as6171/

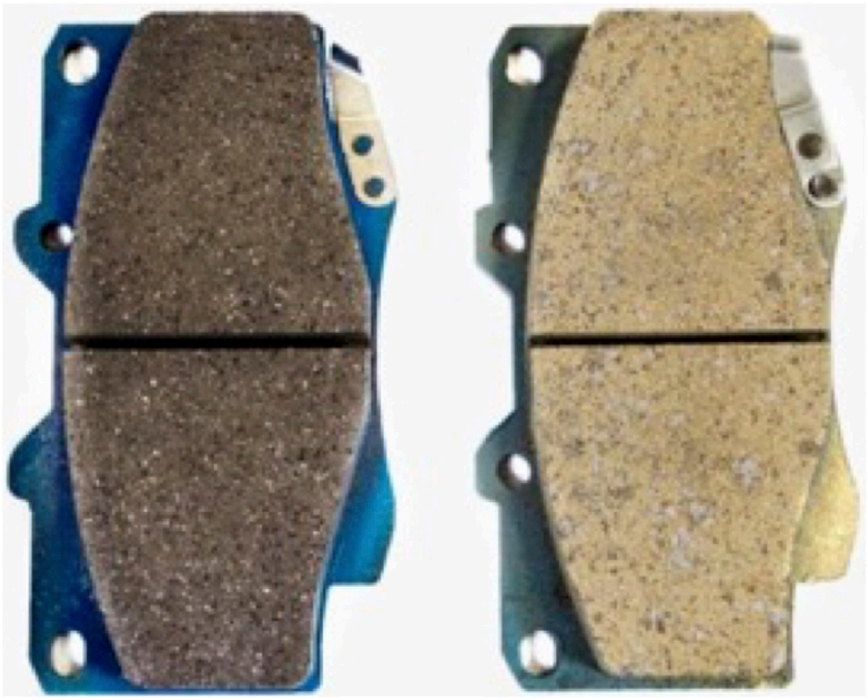

FIGURE 3
The automobile part, isolated from the vehicle's communication network, are difficult to authenticate. The (left) authentic brake pad is difficult to distinguish from (right) the counterfeit brake pad, once installed on the vehicle.

8419 "Blockchain and Related Technologies. . .".[10] The industry case studies listed in the report span a range of points of view, ranging from food, aerospace and traditional manufacturing to digital signatures and embedded trust anchors, collectively called cyber-physical trust anchors. The authors participated in the NIST NCCoE working group discussions and believe the report represents a valid snapshot of many manufacturing supply chains today. Other topics of concern included identity, traceability, linking physical objects to data and records, interoperability, metrics, and standards. In the following sections, we discuss the cyber-physical trust anchor implementation in our work, identify the key parameters linking it to automotive systems developing our model, and describe security features.

3 Proposed architecture with cyber-physical trust anchors

In this section, we develop an architecture for anti-counterfeiting in automotive supply chains with crucial components linking a trust anchor with systems, data, sensors, and monitoring. The core of the architecture consists of a cyber-physical trust anchor and authentication mechanisms connected to tracking processes. The key parameters for linking a cyber-physical trust anchor in embedded IoT include identifiers (i.e., serial numbers, special features, hashes), authentication algorithms, blockchain, and sensors. We use the US $100 currency as an example of the origin of the hashes as a unique identifier, and then an example of quite simple hashes, coupled with blockchain, bringing security to a coffee bean supply chain. Following the use case with tracking coffee, we advance the architecture to include acoustic signature for tires.

3.1 Trust anchors

Many organizations address counterfeiting with legal measures and physical anti-counterfeiting techniques. For example, in the United States, the Secret Service investigates financial crimes, and currency includes a number of features to authenticate it with inspection. The US $100 currency, shown in Figure 4, has at least twelve physical trust anchors—paper, printing, ink, ribbon—and each bill has a unique serial number[11]. It is believed the serial number is tracked throughout the banking system. Hence, low-quality counterfeit bills are detected by flaws in the physical trust anchors and high-quality counterfeits, the "superbills", are detected by mismatch of the serial number.

10 NIST.IR 8419 "Blockchain and Related Technologies to Support Manufacturing Supply Chain Traceability: Needs and Industry Perspectives", https://csrc.nist.gov/publications/detail/nistir/8419/final

11 U.S. Currency Education Program. https://www.uscurrency.gov/denominations/100

FIGURE 4
A US $100 dollar bill to illustrate trust anchors in a physical object of high value. The serial number is used to generate a cryptographic hash and the perceptual hash is generated from the features, some of which are labeled above.

The $100 currency anti-counterfeiting techniques can be transferred to the digital world. The serial number and composite of features in currency can be transformed into unique digital identifiers, constituting a digital trust anchor. An effective mechanism for linking unique digital identifiers to cyber records is hashing. A cryptographic hash is limited to perceptibly different items, and a perceptual hash uses features that are similar under small change. The similarity between perceptual hashes is quantified by computing distance between the hashes.

We use hashes for generating different two types of fingerprints for authenticity. A cryptographic hash enables bit-by-bit authenticity using content based verification. However, a cryptographic hash bares no correlation in the hash space to the input space; this makes them exceedingly powerful at detecting identical images but not similar ones. A perceptual hash, on the other hand, proves verification of the image by generating a comparable fingerprint representation of the image. One perceptual hash of an image will be closer in distance to a similar image that a non similar image. Perceptual hashes are also insensitive to different codecs and updates to the media metadata.

Cyber-physical trust anchors can use a variety numerical structures for linking physical attributes of an object with a secure database. For the purpose of this discussion, we label the serial number as a "cryptographic hash" and the ink, print details, etc., as a "perceptual hashes". Then, each hash has its own definition of distance. The distance for a cryptographic hash is either zero or one, i.e., a perfect match or not. The Euclidean distance in a perceptual hash is a positive real number, i.e., a small positive number for a near perfect match or larger for poor match.

In a truth table of possibilities, an amateur's counterfeit $100 currency is detectable based on large perceptual hash distance, i.e., many print errors and flaws, and a cryptographic hash distance of zero, the counterfeited serial number is not contained in the database at the US. Federal Reserve. A superbill will have a small perceptual hash distance—it looks authentic—yet the cryptographic hash distance is zero, the counterfeited serial number is not contained in the database at the US. Federal Reserve, so long as the database is not compromised.

3.2 Security considerations

A cyber-physical trust anchor is a component of the broader identification, authentication, authorization, and accounting framework for access controls. The lack of end-to-end access control solutions has been an ongoing concern in conventional automotive supply chain security. Although IoT transformed the supply chain with efficiency in tracking, prediction, and automation, challenges exist in connectivity, sensor selection and costs, battery life, and security.

The potential for cyber attacks on vehicles, infrastructure, and autonomous networks has already yielded some protective actions: situation reviews (Chen et al., 2022; Sharma and Gillanders, 2022), policy recommendations (Girdhar et al., 2022; Khan et al., 2022; Kukkala et al., 2022; Benyahya et al., 2023), honey-pots (Panda et al., 2022; Anastasiadis et al., 2023; Baldo et al., 2023), and attack detection (Chen et al., 2021; Zelle et al., 2022; Zhang et al., 2023). This activity demonstrates a high level of concern for the cybersecurity of vehicles, infrastructure, and autonomous vehicles.

We note the interest of the economic sector in the discussions on cyber security in the automotive industry. Authors at the Lloyds Banking Group (London UK) have recently published a literature review, noting gaps in the technology and proposed standards (Fernandez de Arroyabe et al., 2022). The technology and standards gaps are visually presented in a system dynamics model (Khan et al., 2022). In a 2021 review article on future research directions for secure supply, blockchain is described as a promising candidate (Cheung et al., 2021). A 2022 article on zero trust architecture (Rose et al., 2020) gives a more detailed analysis of the role of blockchain for access control (Syed et al., 2022). One issue is privacy, and a strategy is proposed for employing blockchain for security objectives while maintaining private product information and business relationships (Zhang et al., 2022).

3.3 Authentication and tracking

Part traceability in automotive supply chains is predicated on certainty that the part is genuine from factory to customer. In this work, parts are authenticated at point of reading the cyber-physical trust anchor, and establishing provenance. When a part is created, the cyber-physical trust anchor is registered in a secure database

with auditing capabilities. The audit logs must be resistant to attackers hiding their actions.

Blockchain is an ideal technology for auditing and tracking due to immutable logs. Each block contains the cryptographic hash of the previous block, timestamp, and transaction data. Since a cryptographic hash function is used for linking two nodes (i.e., each event is appended to the cryptographic hash of the preceding event), the integrity of events is ensured.

The authentication process can be automated with capture and encoding of data and signals, and readout with sensors. For example, GS1 global standards for streamlining traceability include Two-Dimensional (2D) barcodes, Quick Response (QR) codes, and radio-frequency identification (RFID) (GS1, 2021). Past research has examined RFID for authentication and tracking of patients in healthcare settings (Wamba and Chatfield, 2009; Mabad et al., 2021). Within this Journal, there are a few very popular embedded sensors, with RFID tags being one of the leading examples (Elgazzar et al., 2022; Lin et al., 2022; Lv, 2022). For a proof-of-concept, we use an non-RFID solution—QR codes, mass, and moisture content—in a use case with tracking Toks coffee, Sec. 3.4. Then, we explore non-RFID solutions such as acoustic signatures, as described in Sec. 4.2, for vehicle applications.

In the next section, we briefly discuss results from a nearly 2-year long application of blockchain to provide a secure supply chain.

3.4 Use case: Secure coffee beans with blockchain and simple trust anchors

In January 2021, small farmers in the Tacaná Natural Reserve[12]—a distinct biosphere around the Tacaná Volcano in Chiapas, Mexico, on the border with Guatemala—started using a secure supply chain developed by Dr. Ian Taylor, chief technical officer of SIMBA Chain and his colleagues. The problem solved was an inefficient, and sometimes unfair, supply chain. With blockchain and a very simple physical trust anchor—mass and moisture content—the outcome has been a secure supply chain from individual farmers to more than 200 Toks Restaurants across Mexico. Figure 5 shows the different tiers in the supply chain. A bag of coffee (about 100 kg) is delivered from a farm to the cooperative. The cooperative uses an app on a tablet to register the bag of coffee, measuring the weight and humidity amongst other attributes, and then the farmer digitally signs to hand off in return for payment. A QR code for the bag is generated and registered on the blockchain. The bag of coffee then is sent to the desheller (also registered on chain) and when it returns, the new weight and humidity are measured. The new weight will be roughly 70 kg but each bag is different. Also, the bean's moisture content for each bag will vary. These new measurements are recorded on chain and associated with the QR code. This coupling of the physical attributes with a QR code makes counterfeiting extremely challenging. A counterfeiter cannot simply copy the QR code onto a fake bag of deshelled coffee because it would be very unlikely that the weight and moisture content would match. This simple scheme therefore provides sufficient authenticity and, based on a 4-fold increase in income to the farmer, is a robust anti-counterfeit mechanism.

For the restaurant customers, the secure supply chain ensures the coffee is sustainably sourced. The supply chain has become more efficient, and the return to the farmer increased from $50/bag to $200/bag.[13]

The on-going cost is paper labeling, measurement of weight and moisture content of the coffee beans, a cell phone app, and a blockchain-secured database. These costs are minimal, and barely more than normal product tracking, yet the combination of simple trust anchors linked to a blockchain has a massive, favorable impact on the supply chain. Blockchain in batches distributed across many areas is cheaper than using RFID. Just the cost of a single passive RFID tag can be 50 cents per tag. Blockchain is particularly cost effective when implemented in a private blockchain, as it is in this model. Is the model of a simple trust anchor with blockchain transferable to automobile parts?

3.5 Architecture considerations: Can low-cost authentication work for automobile parts?

Many automobile parts have serial numbers or batch numbers. The $100 currency has a serial number and fingerprint features. The coffee bean bag has a QR code and logged mass and moisture content. Is a trust anchor possible for installed automobile parts, parts not directly connected to the vehicle communication bus? Will this trust anchor have a uniqueness somewhere between currency print features and coffee bean bag mass and moisture content? The search space and procedure are.

1. A unique physical property of the potentially counterfeited part;
2. After the part is installed on the vehicle, the part can be linked to a vehicle sensor;
3. The signal detected by the vehicle sensor can be converted to a perceptual hash;
4. The perceptual hash is uploaded by smart contract and compared with a reference perceptual hash secured on a private blockchain; and
5. The hash comparison yields a probability of part authenticity.

We note that many of the parts that are both subject to counterfeiting and also not directly connected to the vehicle communication bus are parts that move. In general, moving parts emit an acoustic signature. One of the authors is on the faculty of the US Naval Academy and the detection and identification of acoustic signatures is a core expertise of the Navy.

12 Tacaná Natural Reserve, https://en.wikipedia.org/wiki/Volcn_Tacan_Biosphere_Reserve

13 Dr. Ian Taylor's lecture on blockchain and the coffee bean supply chain. https://www.youtube.com/watch?v=DWjP8Igox1o

FIGURE 5
Coffee bean bags with QR labels, mass, and moisture content, when linked to blockchain by a cell app, is sufficient to track sustainably-grown coffee beans from farmer to restaurant. The evidence for success is a 4-fold increase in farmer income.

3.6 Architecture options: Sensors

Automobiles today have a number of embedded devices, sensors, and features. Many of the features are supported by embedded software and electronic control units (ECUs). Luxury cars like Mercedes Benz and Lexus can have over 100 ECUs[14] Other examples of embedded devices and systems in automobiles are ignition systems, antilock braking systems, and airbag control units. The integration of these embedded devices and sensors enable an embedded Internet of Things (IoT) for vehicles.

An efficient implementation of counterfeit part detection will benefit from leveraging the IoT structure associated with connected and autonomous vehicles. In return, autonomous vehicles containing only authentic parts are judged to be more reliable participants in the network. Sensors, data capture and storage mechanisms, and wireless communications can help in tracking automotive parts with proper authentication and security features.

One of the authors of this paper is a chemist and would like to point out the availability of sensors covering a wide range of chemical and material properties. The scientific instruction supply company Vernier Science Education has a website showing sensors for pH, optical spectroscopy, magnetic field, radiation, gas chromatography, polarimetry, moisture, salinity, acoustics and more.[15] This is not a commercial recommendation for this vendor, but is given for the purpose of illustration. These sensors, with corresponding controllers, can increase the range of physical properties measured by embedded sensors. For example, acoustical sensors can be used to track physical items. In ecology, distributed networks of acoustical sensors are used to track and identify insects and bats (Phung et al., 2017; Gallacher et al., 2021). The data processing has characteristics of the *Shazam* app, with Fourier transforms of short time windows and classification operations (Swierczek, 2005; Phung et al., 2017).

With regard to IoT sensors, automobile repair parts can be separated into those parts connected to the vehicle computer network—ECM, airbags, information panel, and door locks—and those parts isolated from the computer network—brake pads, windscreen, and tires. The former can be authenticated by established methods of embedded digital codes which are queried by the vehicle's computer system. The latter, parts isolated from the computer network, are more challenging and are the subject of this paper. In the next section, we will explore the adaptation of the coffee bean model onto detection of counterfeit tires based on an acoustical signature.

4 Tires and embedded internet-of-things: Two options

4.1 RFID in automobile tires: Patents

In March 2022, Bridgestone Corporation was awarded US patent 1,288,628 B2 with an abstract describing a digital tag mounted in a tire and the validation procedure (Yamada et al.,

14 From Silicon to Software https://blogs.synopsys.com/from-silicon-to-software/2021/05/20/ecu-automotive-cybersecurity/

15 Vernier Science Education, https://www.vernier.com/product-category/?category=sensors

2022). An earlier patent described the physical mounting of an RFID tag in a tire, but with less detail on the validation procedure (Bracq and Lauragais, 2020). Bridgestone has announced implementation of RFID tags for Gran Touring race car tires.[16] Let us look at the Bridgestone patent from the point of view of the $100 currency trust anchors and the coffee bean supply chain. What are the strengths and weaknesses of the Bridgestone patent?

"An information presentation system includes an information presentation apparatus, a transmitter attached to a tire and configured to transmit tire ID information for identifying the tire, and a database configured to store tire ID information of tires which are genuine products, and the information presentation apparatus includes a reader configured to perform near field communication with the transmitter, to acquire the tire ID information transmitted by the transmitter, and a controller configured to cause an information presenter to present information indicating that the tire identified with the tire ID information is a genuine product in a case where the tire ID information is stored in the database, and/or cause the information presenter to present information indicating that the tire identified with the tire ID information is a counterfeit product in a case where the tire ID information is not stored in the database." (Yamada et al., 2022).

For the purpose of this discussion, we will assume the Bridgestone patent describes.

- A full-featured RFID tag with secure authentication,
- A secure database, and
- A handheld RFID reader not integral with the vehicle.

First, we note the impressive capabilities of passive RFID tags (Landaluce et al., 2020), security (Good and Benaissa, 2013), and the further development of features such as privacy (Ding et al., 2022). In addition to the RFID, tires have a identifying production number that gives manufacture, location, week, and year of production.[17] The tire identification number (TIN) is not as unique as a serial number, but instead identifies a batch of tires. The TIN is plainly visible on the tire sidewall. The patent also mentions using photography of the tread pattern to match against the RFID. In summary, the Bridgestone patent describes an effective process to establish tire authenticity in the shop.

However, an authentic tire in the shop does not mean an authentic tire is installed on the vehicle. For comparison, as a bank accepts $100 currency, authenticity is checked by the bank at the time of acceptance of the currency. As the coffee bean bags proceed along the supply chain from farmer to the restaurant, the acceptance of the bag is checked by the recipient along the supply chain. We note that a transaction order which schedules authentication *before transfer of ownership* allows fraud.

Another issue is vehicle owner privacy. After the RFID has served its purpose for the supply chain security, how is owner privacy enabled? Can bad actors track people through the tires on their vehicles?

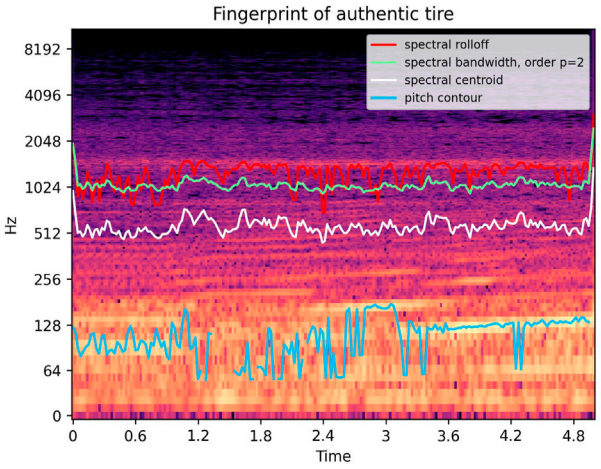

FIGURE 6
A proposed unique fingerprint of a tire based on acoustic signature. Pirelli tire on Fiat 500, GoPro Hero3 with suction cup mount.

4.2 The acoustical signature of an installed tire

We propose connecting physical properties of the tire, installed on the vehicle, with a blockchain-secured database. From the sensors listed in Section 3.6, an acoustic sensor is a logical first choice. Then as described for the coffee bean supply chain in Section 3.4, the cryptographic hash is generated from the tire identification number and the perceptual hash is generated from the acoustic signature of the tire. The calculation of part authenticity is based on the distance of the new perceptual hash *versus* the reference perceptual hash.

The term acoustic signature is used to describe a combination of acoustic emissions of sound emitters, such as those of ships, submarines, aircraft, machinery, animals, and music which can be used for identification, condition, behavior, and physical location. For music, the popular *Shazam* application readily identifies music from just a few seconds of audio data. Similarly, the acoustic signature of a tire, as shown in Figure 6, is rich in detail with the potential of generating a fingerprint with sufficient uniqueness to meet part authentication needs.The acoustic features that one looks for include acoustical power at well-spaced frequencies, as shown in Figure 6. Another useful characteristic is the ability to modulate the signal; in the case of tire noise, modulation is possible with a defined acceleration-deceleration profile. The combination of resolvable frequencies and their response to external modulation creates a signal pattern than can be converted into a perceptual hash. In an N-dimensional hash space, the objective are hashes from new tires of the same batch that are clustered and well separated from hashes derived from tires of either a different batch or counterfeit.

A draft validation app, akin to the Toks Coffee Tracking app shown in Figure 5, is outlined in Figure 7. The table shows the physical item, its characteristic features, and the logging of the cyber-physical trust anchor with blockchain.

16 Rain Alliance, 31 October 2022: https://rainrfid.org/bridgestone-japan-selects-avery-dennison-maxdura-tire-tags/

17 Tire Identification and Recordkeeping: https://www.federalregister.gov/documents/2015/04/13/2015–08418/tire-identification-and-recordkeeping

TIRE VALIDATION APP (draft)

Physical	Features	Blockchain
Tire produced at factory with batch number on sidewall	Acoustic signal measured with speed, acceleration protocol	Batch number and acoustics hashed and chained
Tires move through supply chain	Batch numbers read optically	Provenance logged through batch numbers
Tire mounted on car	Batch number read optically	Provenance logged through batch number
Car driven through speed, acceleration protocol	Acoustic signal measured with car-mounted microphones	Acoustics hashed and compared with chain. Probability of tire authenticity calculated

FIGURE 7
A proposed tire validation app modeled after the Toks Coffee Tracking app. The last line is key: part authenticity is calculated based on features measured by the car with the tire mounted on the car.

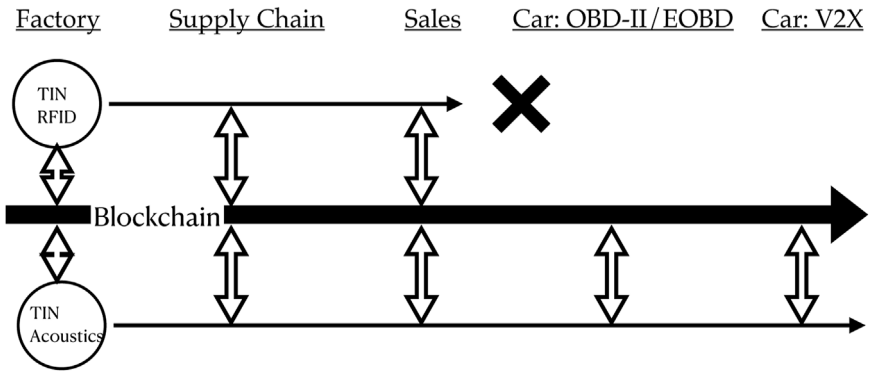

FIGURE 8
Two proposed architectures for car tire supply chain security. The top row shows TIN/RFID enables security to the salesroom, whilst the bottom row with TIN/acoustics preserves security through tire installation and demonstrates tire authentication to the vehicle OBD-II/EOBD on-board diagnostics network and vehicle-to-infrastructure (V2X) network. TIN is the human-readable tire identification number printed on the tire showing batch production information. The doubleheaded arrows show usage of the cyber-physical trust anchor to validate authentication and record provenance with the blockchain.

Relative to the Bridgestone patent, the use of an acoustical signature has the capital equipment cost of additional microphones in the vehicle; noise isolation in the vehicle will likely prevent the microphone in the steering wheel from measuring tire noise with sufficient fidelity. On the other hand, the authenticity is established for the installed tire, not just the tire in the shop. Because the perceptual hash is a one-way function, the acoustical noise signature cannot be regenerated from a captured hash. Roadside microphones cannot use the perceptual hash to identify a vehicle. Thus, the owner privacy is preserved.

When do you allow the cloud to know where your car is? While advances in technology enhance safety and convenience, the technology also generates a significant amount of sensitive or personal vehicle data, such as location (Good and Benaissa, 2013; Zhang et al., 2022) With respect to privacy, a non-connected car currently allows location to be known under two conditions. One involves utilizing devices that are distinct from the automobile. Another requires historical information linking a VIN to location, such as maintenance records or CARFAX reports. In connected and autonomous networks, GPS and other sensors collect real-time location data, which can be compromised if connectivity includes cloud based applications (i.e., infotainment). Automated counterfeit detection systems in vehicles require privacy considerations. We incorporate hashing as a means to preserve privacy in connected and autonomous vehicle networks.

4.3 Proposed architecture

A proposed architecture is shown in Figure 8. A key component of the TIN/acoustics cyber-physical trust anchor architecture is tire-to-vehicle authentication via an acoustical cyber-physical trust anchor. The on-vehicle authentication reduces a potential attack vector in which the customer is shown an authentic tire in the salesroom, but the mechanic, working out-of-sight of the customer, installs a counterfeit tire.

5 Conclusion

Embedded sensors from the Internet of Things can be applied to vehicle parts not directly connected to the vehicle's communication bus. Then, a cyber-physical trust anchor can be established and used to verify part authenticity. The workload of secure supply chain development can be shared with the development of the autonomous vehicle networks, as the fleet performance is degraded by vehicles with questionable repair parts of uncertain reliability.

This manuscript develops the key parameters for a low-cost part authentication strategy. First, there is the cyber-physical trust anchor.

- A serial number converted to a cryptographic hash,
- Unique features or physical properties converted to a perceptual hash,
- A database secured by blockchain, and
- A truth table and thresholds for hash distances developed to report probability of part authenticity.

Second, the readout of the print features or physical properties is recommended *after installation* of the part onto the vehicle. This is challenging for those parts not normally connected to the vehicle communication network. To address this challenge, alternative IoT sensors are devised. For moving parts such as tires, motion will generate an acoustical signature. Herein, we propose investigation of tire noise, the reduction of tire noise to a perceptual hash, and the comparison of the measured hash *versus* a reference hash secured by blockchain to leading to the calculation of the probability of part authenticity.

Third, the financial incentives are both carrot and stick. The secure supply chain yields market recovery for the tire manufacturer. There is also a financial incentive from a policy, yet to be developed, for participation of vehicles in an autonomous vehicle network. Only vehicles participating in secure supply chain processes, such as described herein for tires, should be allowed to participate in autonomous vehicle network. Vehicles not participating in a secure supply chain process to ensure authentic repair parts are used in vehicle repair should not be allowed to participate in the autonomous vehicle network. The risk to the other vehicles in the network is unacceptable.

Data availability statement

The original contributions presented in the study are included in the article/Supplementary material, further inquiries can be directed to the corresponding author.

Author contributions

MM evaluted the cyber security assessment and the magnitude of the counterfeit problem. LB provided the perspective of a chemist and former mechanic. IT provided the expertise on blockchain and the secure coffee bean supply chain. All authors contributed to the article and approved the submitted version.

Acknowledgments

We gratefully acknowledge the support of the National Institute of Standards and Technology, U.S. Department of Commerce in providing the SBIR support for this project, as well as the U.S. National Science Foundation under grant number OIA-1946231, the Louisiana Board of Regents for the Louisiana Materials Design Alliance (LAMDA), and the U.S. Naval Academy.We thank Commander Brien Croteau for bringing the Frontiers special issue on Embedded Systems and Network Security to our attention.

Conflict of interest

Author IT is employed by SIMBA Chain, Inc. Author LB is a co-founder of Refined Imaging.

The remaining author declares that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Publisher's note

All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers. Any product that may be evaluated in this article, or claim that may be made by its manufacturer, is not guaranteed or endorsed by the publisher.

Author disclaimer

The views expressed in this article do not necessarily represent the views or opinions of the U. S. Naval Academy, Department of the Navy, or Department of Defense (DoD) or any of its components.

References

Acharya, S., Dvorkin, Y., Pandzic, H., and Karri, R. (2020). Cybersecurity of smart electric vehicle charging: a power grid perspective. *IEEE Access* 8, 214434–214453. doi:10.1109/ACCESS.2020.3041074

Aliwa, E., Rana, O., Perera, C., and Burnap, P. (2021). Cyberattacks and countermeasures for in-vehicle networks. *ACM Comput. Surv.* 54, 1–37. doi:10.1145/3431233

Anastasiadis, M., Moschou, K., Livitckaia, K., Votis, K., and Tzovaras, D. (2023). "A novel high-interaction honeypot network for internet of vehicles," in 2023 31st Mediterranean Conference on Control and Automation (MED), Limassol, June 26 – 29, 2023, 281. –286. doi:10.1109/MED59994.2023.10185669

Baldo, M., Bianchi, T., Conti, M., Trevisan, A., and Turrin, F. (2023). *HoneyEVSE: an honeypot to emulate electric vehicle supply equipments. arXiv* doi. doi:10.48550/arXiv.2309.06077

Benyahya, M., Collen, A., and Nijdam, N. A. (2023). Analyses on standards and regulations for connected and automated vehicles: identifying the certifications roadmap. *Transp. Eng.* 14, 100205. doi:10.1016/j.treng.2023.100205

Bracq, M., and Lauragais, M. (2020). *LDL technology, assignee. Method for managing type identifiers*. Tech. Rep. United States patent US10682892 B2. France: LDL Technology.

Chen, Q., Romanowich, P., Castillo, J., Roy, K. C., Chavez, G., and Xu, S. (2021). ExHPD: exploiting human, physical, and driving behaviors to detect vehicle cyber attacks. *IEEE Internet Things J.* 8, 14355–14371. doi:10.1109/JIOT.2021.3069951

Chen, Y., Shiwakoti, N., Stasinopoulos, P., and Khan, S. K. (2022). State-of-the-Art of factors affecting the adoption of automated vehicles. *Sustainability* 14, 6697. doi:10.3390/su14116697

Cheung, K.-F., Bell, M. G., and Bhattacharjya, J. (2021). Cybersecurity in logistics and supply chain management: an overview and future research directions. *Transp. Res. Part E Logist. Transp. Rev.* 146, 102217. doi:10.1016/j.tre.2020.102217

Ding, H., Han, J., Zhao, C., Wang, G., Xi, W., Jiang, Z., et al. (2022). Arbitrator2.0: preventing unauthorized access on passive tags. *IEEE Trans. Mob. Comput.* 21, 835–848. doi:10.1109/TMC.2020.3017484

Elgazzar, K., Khalil, H., Alghamdi, T., Badr, A., Abdelkader, G., Elewah, A., et al. (2022). Revisiting the internet of things: new trends, opportunities and grand challenges. *Front. Internet Things* 1, 1073780. doi:10.3389/friot.2022.1073780

Elkhail, A. A., Refat, R. U. D., Habre, R., Hafeez, A., Bacha, A., and Malik, H. (2021). Vehicle security: a survey of security issues and vulnerabilities, malware attacks and defenses. *IEEE Access* 9, 162401–162437. doi:10.1109/ACCESS.2021.3130495

El-Rewini, Z., Sadatsharan, K., Sugunaraj, N., Selvaraj, D. F., Plathottam, S. J., and Ranganathan, P. (2020). Cybersecurity attacks in vehicular sensors. *IEEE Sensors J.* 20, 13752–13767. doi:10.1109/JSEN.2020.3004275

Feng, Y., Huang, S. E., Wong, W., Chen, Q. A., Mao, Z. M., and Liu, H. X. (2022). On the cybersecurity of traffic signal control system with connected vehicles. *IEEE Trans. Intelligent Transp. Syst.* 23, 16267–16279. doi:10.1109/TITS.2022.3149449

Fernandez de Arroyabe, I., Watson, T., and Angelopoulou, O. (2022). Cybersecurity in the automotive industry: a systematic literature review (slr). *J. Comput. Inf. Syst.* 1, 716–734. doi:10.1080/08874417.2022.2103853

Gallacher, S., Wilson, D., Fairbrass, A., Turmukhambetov, D., Firman, M., Kreitmayer, S., et al. (2021). Shazam for bats: internet of Things for continuous real?time biodiversity monitoring. *IET Smart Cities* 3, 171–183. doi:10.1049/smc2.12016

Girdhar, M., You, Y., Song, T.-J., Ghosh, S., and Hong, J. (2022). Post-accident cyberattack event analysis for connected and automated vehicles. *IEEE Access* 10, 83176–83194. doi:10.1109/ACCESS.2022.3196346

Good, T., and Benaissa, M. (2013). A holistic approach examining RFID design for security and privacy. *J. Supercomput.* 64, 664–684. doi:10.1007/s11227-010-0497-9

GS1 (2021). *Standards*. Available at: https://www.gs1.org/standards.

Hashem Eiza, M., and Ni, Q. (2017). Driving with sharks: rethinking connected vehicles with vehicle cybersecurity. *IEEE Veh. Technol. Mag.* 12, 45–51. doi:10.1109/MVT.2017.2669348

Kennedy, J., Holt, T., and Cheng, B. (2019). Automotive cybersecurity: assessing a new platform for cybercrime and malicious hacking. *J. Crime Justice* 42, 632–645. doi:10.1080/0735648X.2019.1692425

Khan, S. K., Shiwakoti, N., and Stasinopoulos, P. (2022). A conceptual system dynamics model for cybersecurity assessment of connected and autonomous vehicles. *Accid. Analysis Prev.* 165, 106515. doi:10.1016/j.aap.2021.106515

Khan, S. K., Shiwakoti, N., Stasinopoulos, P., and Chen, Y. (2020). Cyber-attacks in the next-generation cars, mitigation techniques, anticipated readiness and future directions. *Accid. Analysis Prev.* 148, 105837. doi:10.1016/j.aap.2020.105837

Kukkala, V. K., Thiruloga, S. V., and Pasricha, S. (2022). Roadmap for cybersecurity in autonomous vehicles. *IEEE Consum. Electron. Mag.* 11, 13–23. doi:10.1109/MCE.2022.3154346

Kumar, S., Dohare, U., Kumar, K., Prasad Dora, D., Naseer Qureshi, K., and Kharel, R. (2019). Cybersecurity measures for geocasting in vehicular cyber physical system environments. *IEEE Internet Things J.* 6, 5916–5926. doi:10.1109/JIOT.2018.2872474

Labrado, C., Thapliyal, H., and Mohanty, S. P. (2022). Fortifying vehicular security through low overhead physically unclonable functions. *ACM J. Emerg. Technol. Comput. Syst.* 18, 1–18. doi:10.1145/3442443

Landaluce, H., Arjona, L., Perallos, A., Falcone, F., Angulo, I., and Muralter, F. (2020). A review of IoT sensing applications and challenges using RFID and wireless sensor networks. *Sensors* 20, 2495. doi:10.3390/s20092495

Lin, S., Shi, Q., and Zhou, N. (2022). Construction of a traceability system for food industry chain safety information based on internet of things technology. *Front. Public Health* 10, 857039. doi:10.3389/fpubh.2022.857039

Lv, Z. (2022). Practical application of internet of things in the creation of intelligent services and environments. *Front. Internet Things* 1, 912388. doi:10.3389/friot.2022.912388

Mabad, T., Ali, O., Ally, M., Wamba, S. F., and Chan, K. C. (2021). Making investment decisions on RFID technology: an evaluation of key adoption factors in construction firms. *IEEE Access* 9, 36937–36954. doi:10.1109/ACCESS.2021.3063301

Panda, S., Rass, S., Moschoyiannis, S., Liang, K., Loukas, G., and Panaousis, E. (2022). HoneyCar: a framework to configure honeypot vulnerabilities on the internet of vehicles. *IEEE Access* 10, 104671–104685. doi:10.1109/ACCESS.2022.3210117

Phung, Q. V., Ahmad, I., Habibi, D., and Hinckley, S. (2017). Automated insect detection using acoustic features based on sound generated from insect activities. *Acoust. Aust.* 45, 445–451. doi:10.1007/s40857-017-0095-6

Rose, S., Borchert, O., Mitchell, S., and Connelly, S. (2020). *Zero trust architecture*. Tech. rep. United States: National Institute of Standards and Technology. doi:10.6028/NIST.SP.800-207

Sharma, P., and Gillanders, J. (2022). Cybersecurity and forensics in connected autonomous vehicles: a review of the state-of-the-art. *IEEE Access* 10, 108979–108996. doi:10.1109/ACCESS.2022.3213843

Shen, A., Turner, S., and Antonopoulos, G. (2022). Driven to death: a Chinese case study on the counterfeiting of automotive components. *Asian J. Criminol.* 17, 311–329. doi:10.1007/s11417-022-09365-8

Swierczek, R. (2005). *Music identification system*. Tech. Rep. United States patent US6,941,275 B1.

Syed, N. F., Shah, S. W., Shaghaghi, A., Anwar, A., Baig, Z., and Doss, R. (2022). Zero trust architecture (zta): a comprehensive survey. *IEEE Access* 10, 57143–57179. doi:10.1109/ACCESS.2022.3174679

Wamba, S. F., and Chatfield, A. T. (2009). A contingency model for creating value from RFID supply chain network projects in logistics and manufacturing environments. *Eur. J. Inf. Syst.* 18, 615–636. doi:10.1057/ejis.2009.44

Yamada, K., Hirajima, S., and Yamaguchi, S. (2022). *Bridgestone, assignee. Information presentation system, information presentation apparatus, and information presentation method*. Tech. Rep. United States patent US11288628. Japan: Bridgestone Corporation.

Zelle, D., Plappert, C., Rieke, R., Scheuermann, D., and Krauß, C. (2022). ThreatSurf: a method for automated Threat Surface assessment in automotive cybersecurity engineering. *Microprocess. Microsystems* 90, 104461. doi:10.1016/j.micpro.2022.104461

Zhang, C., Zhu, L., Xu, C., Sharif, K., Lu, R., and Chen, Y. (2022). APPB: anti-counterfeiting and privacy-preserving blockchain-based vehicle supply chains. *IEEE Trans. Veh. Technol.* 71, 13152–13164. doi:10.1109/TVT.2022.3196051

Zhang, F., Wang, M., Parker, J., and Roberts, S. C. (2023). The effect of driving style on responses to unexpected vehicle cyberattacks. *Safety* 9, 5. doi:10.3390/safety9010005