International journal of imaging science and engineering

ISSN: 1934--9955 www.ijise.net

Vol-20 Issue-01 April 2025

Block Chain Security In Connected Autonomous Vehicles: A Comprehensive Review

Kallutla Tarun Reddy[1], Dogiparthi Hitesh[2], P. Venkat Sahithi[3] , T. Bhargavi[4]
[1,2,3] UG Scholar, Dept of IT, St. Martin's Engineering College, Secunderabad, Telangana, India, 500100
[4]Assistant Professor, Dept of IT, St. Martin's Engineering College, Secunderabad, Telangana, India, 500100
ktarunreddy2003@gmail.com

Abstract:

This project explores the integration of blockchain technology to enhance security in connected autonomous vehicles (CAVs). As the automotive industry increasingly adopts connectivity and automation, the vulnerabilities associated with data privacy, system integrity, and communication networks have become critical concerns. This research presents a framework that leverages blockchain's decentralized and immutable nature to secure data transactions among vehicles, infrastructure, and users. By implementing smart contracts, we aim to facilitate secure, transparent interactions, thereby mitigating risks related to hacking, data tampering, and unauthorized access. The project also investigates the scalability and interoperability of blockchain solutions in real-world scenarios, considering factors such as latency and computational efficiency. Through simulation and case studies, we demonstrate the effectiveness of our proposed model in enhancing the overall security posture of CAVs, ultimately contributing to safer and more reliable autonomous transportation systems.

Keywords: Connected Autonomous Vehicles, Block Chain security, Decentralization, System Integrity, Data tampering, Unauthorized access.

1. INTRODUCTION

Cyber-Physical Systems (CPS) integrate computational and physical processes to enhance automation, monitoring, and control in various domains. CPS aims to create an intelligent and interconnected environment by utilizing smart devices, sensors, and cloud computing to process real-time data and generate appropriate responses. These systems enable efficient management of critical infrastructures such as transportation, healthcare, smart cities, and industrial automation. By ensuring seamless communication between cyber and physical components, CPS enhances safety, efficiency, and decision-making capabilities in modern technological ecosystems. The rapid advancement of information technology has led to significant developments in Cyber-Physical Systems (CPS), which combine physical components (such as buildings, vehicles, and sensors) with cyber components (such as cloud computing, artificial intelligence, and smart applications). CPS enables intelligent automation by using communication networks and advanced networking devices like routers and switches to facilitate seamless data exchange between the physical and digital worlds. CPS has been widely deployed in diverse sectors, including smart grids, autonomous transportation systems, healthcare, and industrial automation. One key application of CPS is Connected and Autonomous Vehicles (CAVs), where real-time data processing ensures safe navigation and decision-making. However, implementing CPS comes with challenges such as cybersecurity threats, system complexity, and the need for robust networking infrastructure. With continuous advancements in artificial intelligence, the Internet of Things (IoT), and cloud computing, CPS is expected to play a transformative role in shaping the future of smart and automated environments.

2. LITERATURE SURVEY

V. Sundararajan, A. Ghodousi and J. E. Dietz. (2022) The Most Common Control Deficiencies in CMMC non-compliant DoD contractors The Cybersecurity Maturity Model Certification (CMMC) was developed to enhance the security posture of contractors working with the U.S. Department of Defense (DoD). Research on common control deficiencies among non-compliant contractors reveals recurring issues that hinder certification. Key deficiencies include inadequate access control, insufficient incident response planning, lack of multi-factor authentication, and poor system monitoring practices. Additionally, many contractors struggle with properly securing sensitive data, enforcing encryption standards, and maintaining regular security audits. These gaps indicate a broader challenge in aligning contractor cybersecurity practices with CMMC requirements, often due to limited resources or misunderstanding of compliance obligations, which leaves critical DoD information vulnerable to cyber threats.

A. Mehra and S. Badotra. (2021) Artificial Intelligence Enabled Cyber Security In recent years, the integration of Artificial Intelligence (AI) in cybersecurity has garnered significant attention due to its potential to enhance the detection, prevention, and response to cyber threats. The 2021 6th International Conference on Signal Processing, Computing, and Control (ISPCC) highlights advancements in AI-driven cybersecurity solutions. AI techniques such as machine learning, deep learning, and natural language processing are being employed to analyze vast amounts of data,

International journal of imaging science and engineering

ISSN: 1934--9955 www.ijise.net

Vol-20 Issue-01 April 2025

identify patterns, and predict potential security breaches in real-time. These AI models improve the accuracy of threat detection, mitigate the risks posed by evolving cyber- attacks, and automate incident responses, significantly bolstering cybersecurity frameworks.

W. Matsuda, M. Fujimoto, T. Aoyama and T. Mitsunaga. (2019) Cyber Security Risk Assessment on Industry 4.0 using ICS testbed with AI and Cloud The integration of Industry 4.0 technologies, such as the Industrial Control Systems (ICS), artificial intelligence (AI), and cloud computing, has transformed industrial operations but also introduced new cybersecurity risks. Studies utilizing ICS testbeds 2 for cybersecurity risk assessment in Industry 4.0 environments emphasize the need for enhanced security measures to address these risks. AI-driven models are being employed to detect anomalies and predict potential cyber threats in real time, while cloud-based solutions offer scalable security management. However, research highlights vulnerabilities in data transmission, cloud infrastructure, and remote access, which can be exploited by cyber-attacks. These assessments provide critical insights into developing robust, AI- powered cybersecurity frameworks that can effectively safeguard Industry 4.0 systems against emerging threats.

L. Li, W. He, L. Xu, A. Ivan, M. Anwar and X. (2014) Does Explicit Information Security Policy Affect Employees Research on the impact of explicit information security policies on employees' cybersecurity behavior suggests that clear, well-communicated policies can significantly influence how employees adhere to security practices. A pilot study on this topic indicates that when employees are aware of specific security guidelines, they are more likely to engage in protective behaviors such as using strong passwords, avoiding phishing scams, and following data protection protocols. However, the study also emphasizes that the mere existence of a security policy is not enough. The effectiveness depends on factors such as policy clarity, organizational culture, and continuous training. Employees' understanding and perception of these policies play a critical role in shaping their cyber hygiene and reducing human-related security vulnerabilities.

Cisco Systems. (2008b). Data leakage worldwide: The effectiveness of corporate security policies. Retrieved May 12, 2011, from World WideWeb:http://www.cisco.com/en/US/solutions/collateral/ns170/ns 896/ns895/Cis co-STL- Data-Leakage-2008-.pdf Data leakage has become a critical global concern, with increasing incidents compromising sensitive information across various industries. The effectiveness of corporate security policies plays a crucial role in mitigating such risks. Research shows that well-implemented policies, including data encryption, access control, and employee training, can significantly reduce vulnerabilities. However, the rapid evolution of cyber threats and the rise of remote work have exposed gaps in traditional security approaches. Studies highlight that while many organizations adopt robust policies, the lack of continuous monitoring, policy enforcement, and adaptation to new attack vectors often undermines their effectiveness, leading to persistent data leakage challenges worldwide.

3. PROPOSED METHODOLOGY

The proposed system overcomes the limitations of the existing approach by leveraging blockchain technology to provide a decentralized, scalable, and secure platform for user registration, simulation, and data analysis. In this system, users are registered, and their accounts are activated by an administrator using a streamlined and efficient process. Once activated, users can initiate real-time simulations involving vehicle networks, which are recorded and validated in a blockchain ledger to ensure transparency and security. The decentralized nature of blockchain ensures that every transaction, from user actions to vehicle simulations, is securely logged, minimizing the risk of tampering. Moreover, the use of advanced algorithms tailored for distributed systems ensures fast processing, real-time data retrieval, and highly efficient simulation outputs, which makes the system suitable for applications like connected and autonomous vehicles (CAVs) Significantly improved efficiency and speed in policy creation.

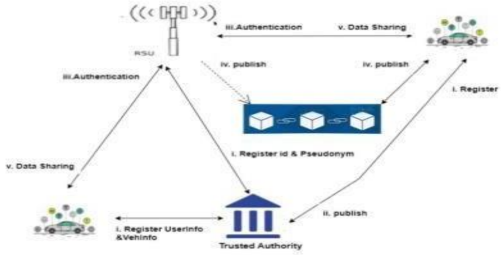
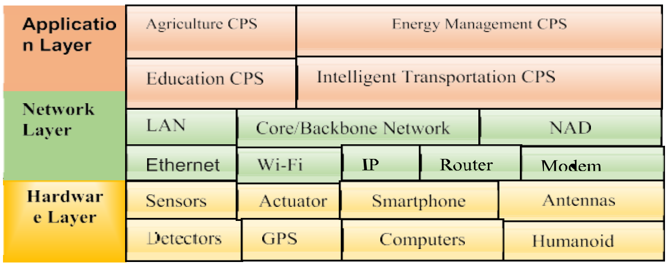


Figure 1: Block-Chain base Multimedia Sharing.

proposed in which is based on Blockchain for mul- timedia sharing within VSNs. The proposed system used cryptographical primitives such as pseudonyms to hide the identities of vehicles, users and Road Side Units (RSUs). Trusted Authority has been used by to verify the user, vehicle and RSU. TA authority uses pseudo-random function F to generate unique identities of users and RSUs, key generation algorithms to generate keys (public and private keys) for the users and the RSUs and generates hash chain H for both users as well as RSUs for authentication purposes. RSUs uses a signature algorithm to sign the transaction and a verification algorithm to verify the messages sent by users. TA stores the user, vehicle and RSU information on Blockchain along with a time stamp duly signed by TA as a transaction. The multimedia data sharing can be either peer-to-peer or broadcasting to the network. For sending peer-to-peer multimedia data, the user gets authenticated to RSU. This is done by sending its hash value verified by RSU and then retrieving hash associated with the user from the Blockchain.

Architecture:



Application Layer	Agriculture CPS	Energy Management CPS			
	Education CPS	Intelligent Transportation CPS			
Network Layer	LAN	Core/Backbone Network	NAD		
	Ethernet	Wi-Fi	IP	Router	Modem
Hardware Layer	Sensors	Actuator	Smartphone	Antennas	
	Detectors	GPS	Computers	Humanoid	

The proposed system claims to help in privacy protection, reliability and integrity of the messages, traceability of the malicious user. The proposed system has been evaluated uses a signature algorithm to sign the transaction and a verification algorithm to verify the messages sent by users. It is managing

for experimental results. It has been observed that the proposed system assumes the trustworthiness of TA, which is highly risky in a situation where almost every entity can be under attack. That means if the proposed system verifies the integrity of users, vehicles, and multimedia data, it must have to verify TA's integrity and authenticity. If the TA is under attack, all the data stored on it and the transactions it creates can become malicious, spoiling the whole Blockchain network.

Applications:

Secure Data Sharing (V2V): Ensures integrity and authenticity of vehicle-to-vehicle communication**.**

Vehicle-to-Infrastructure (V2I) Security: Secures critical data exchanged between AVs and smart infrastructure.

Immutable Event Logs: Provides tamper-proof logs for accident analysis and system audits.

Secure Software Updates: Verifies authenticity of updates and prevents malicious injections.

Decentralized Identity Management: Ensures authorized access to AV systems and services.

Automated Secure Payments: Enables safe and transparent transactions for tolls and services.

Sensor Data Protection: Prevents manipulation of sensor inputs and detects spoofing.

Crowdsourced Map Validation: Validates and aggregates map data from multiple AVs.

Charging Station Security: Protects EV charging stations from unauthorized access.

Collaborative Simulation Security: Secures shared AI models and simulation data.

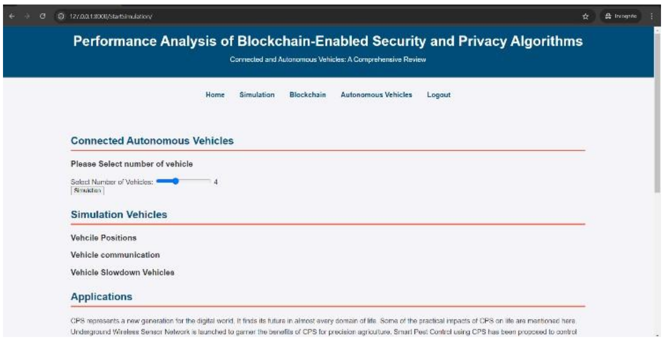
Advantages:

The ETC (Extra Tree Classifier) algorithm is commonly used in multi- armed bandit problems and online learning settings. Here are some advantages of the ETC algorithm:

- **Decentralization**: The system uses blockchain to decentralize user management, enhancing system efficiency and removing bottlenecks.
- **Improved Security**: With blockchain encryption and hashing algorithms, data security and integrity are significantly enhanced.
- **Real-time Processing**: The system supports real-time vehicle simulations with instant blockchain-based validation.
- **Scalability**: The system can handle multiple users and transactions without compromising performance, making it suitable for large-scale simulations.
- **Enhanced Transparency**: Every transaction and user activity is logged in the blockchain, ensuring complete transparency and auditability.
- **Accountability and Auditability:** Provides a transparent and traceable record for legal and regulatory compliance.
- **Efficient Identity Management:** Ensures only authorized devices and users interact with AVs.
- **Increased Public Trust:** Boosts user confidence by ensuring safety and privacy in autonomous transportation.

4. EXPERIMENTAL ANALYSIS

Figure 1 Shows that the allows users to select the number of autonomous vehicles (AVs) and simulate their behavior. It tracks vehicle positions, monitors secure communication between AVs, and analyzes vehicle slowdown scenarios. The application section highlights real-world uses of Cyber-Physical Systems (CPS), demonstrating how blockchain enhances security and privacy in AV networks.



Performance Analysis of Blockchain-Enabled Security and Privacy Algorithms

Connected and Autonomous Vehicles: A Comprehensive Review

Connected Autonomous Vehicles

Please Select number of vehicle

Select Number of Vehicles: 4

Simulation Vehicles

Vehcile Positions

Vehicle communication

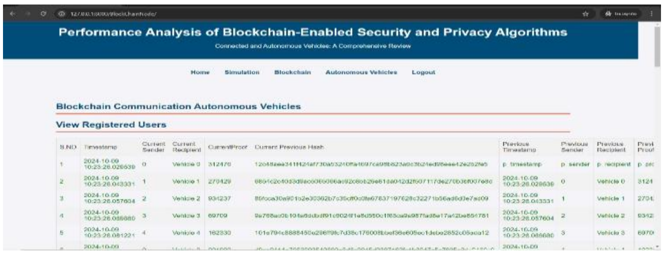
Vehicle Slowdown Vehicles

Applications

CPS represents a new generation for the digital world. It finds its future in almost every domain of life. Some of the practical impacts of CPS on life are mentioned here. Underground Wireless Sensor Network is launched to garner the benefits of CPS for precision agriculture. Smart Pest Control using CPS has been proposed to control

Figure 1: Selecting Vehicles And simulating

Figure 2 shows the interface displays a **blockchain communication log** for autonomous vehicles (AVs). It lists registered users and records transaction details such as timestamp, sender, recipient, proof, and previous hash. Each entry ensures data integrity and traceability, verifying secure communication between AVs. The system maintains a decentralized ledger to prevent data tampering, enhancing the security and privacy of AV interactions.



Performance Analysis of Blockchain-Enabled Security and Privacy Algorithms

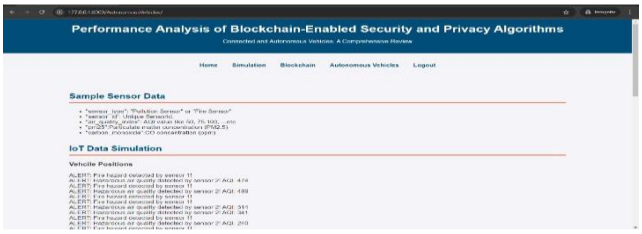
Connected and Autonomous Vehicles: A Comprehensive Review

Blockchain Communication Autonomous Vehicles

View Registered Users

S.NO	Timestamp	Current Sender	Current Recipient	CurrentProof	Current Previous Hash	Previous Timestamp	Previous Sender	Previous Recipient	Previ Proof
1	2024-10-09 10:23:28.028639	0	Vehicle 0	312470	12648aea341f424af730a5324Dffa4697ca98b823a0c3b24ed98eee42e252fe5	p_timestamp	p_sender	p_recipient	p_prc
2	2024-10-09 10:23:28.043331	1	Vehicle 1	270429	6864c2c40d3d8ac6066086ac92c8cb29e61da042d2f607117de270b3bf007e8d	2024-10-09 10:23:28.028639	0	Vehicle 0	3124
3	2024-10-09 10:23:28.057604	2	Vehicle 2	934237	80fcca30a901b2e30392b7c35cff0c0fe67837197628c32271b56ad6d3e7ad09	2024-10-09 10:23:28.043331	1	Vehicle 1	2704
4	2024-10-09 10:23:28.088680	3	Vehicle 3	69709	9e768ac0b104e6ddbdf91c8024f1e8d550c1f63ca9e987fad8e17a12be854781	2024-10-09 10:23:28.057604	2	Vehicle 2	9342
5	2024-10-09 10:23:28.081221	4	Vehicle 4	162330	101e794c8888450e286f9fc7d38c176008bbef36e605ec1debe2852c05ada12	2024-10-09 10:23:28.088680	3	Vehicle 3	6970
6	2024-10-09	[illegible]	[illegible]	[illegible]	[illegible]	2024-10-09	[illegible]	[illegible]	[illegible]

Figure 2: Block Chain Node connectivity with each Vehicle



Performance Analysis of Blockchain-Enabled Security and Privacy Algorithms

Connected and Autonomous Vehicles: A Comprehensive Review

Sample Sensor Data

- "sensor_type": "Pollution Sensor" or "Fire Sensor"
- "sensor_id": Unique SensorId,
- "air_quality_index": AQI value like 50, 75, 100, ...etc
- "pm25":Particulate matter concentration (PM2.5)
- "carbon_monoxide":CO concentration (ppm)

IoT Data Simulation

Vehcile Positions

```
ALERT: Fire hazard detected by sensor 1!
ALERT: Hazardous air quality detected by sensor 2! AQI: 474
ALERT: Fire hazard detected by sensor 1!
ALERT: Hazardous air quality detected by sensor 2! AQI: 488
ALERT: Fire hazard detected by sensor 1!
ALERT: Fire hazard detected by sensor 1!
ALERT: Hazardous air quality detected by sensor 2! AQI: 314
ALERT: Hazardous air quality detected by sensor 2! AQI: 341
ALERT: Fire hazard detected by sensor 1!
ALERT: Hazardous air quality detected by sensor 2! AQI: 240
ALERT: Fire hazard detected by sensor 1!
```

Figure 3: Sensor data and IOT Simulation

Figure 3 shows that the interface displays **sensor data and IoT data simulation** for autonomous vehicles (AVs). It shows sample sensor data such as pollution or fire sensor types, unique IDs, air quality index (AQI), and gas concentration levels. The **IoT Data Simulation** section highlights vehicle positions with real-time alerts about detected hazards, such as fire or poor air quality, ensuring that AVs receive accurate environmental data for safe decision-making.

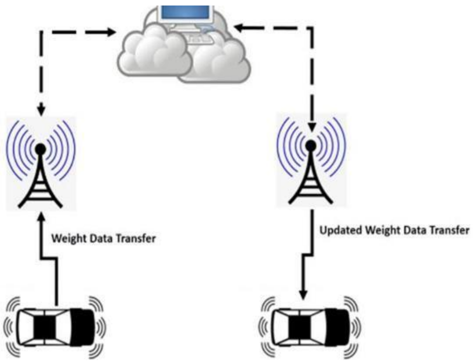


Figure 4: GeFL hybrid model

Figure 4 shows the diagram illustrates **data transfer between autonomous vehicles (AVs) and a central server via wireless communication towers.**

- **Weight Data Transfer:** The initial vehicle sends its data (likely sensor or traffic information) to the central server through a communication tower.
- **Updated Weight Data Transfer:** The server processes and updates the data, then transmits the modified data back to another vehicle through a different tower.

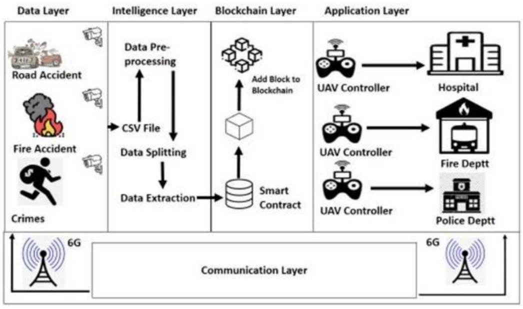


Figure 5: Classification report of ETC

Figure 5 Shows The diagram represents a **multi-layer architecture for emergency response using blockchain and UAVs (Unmanned Aerial Vehicles).**

1. Data Layer:

- Collects incident data such as **road accidents, fire accidents, and crimes.**

2. Intelligence Layer:

- **Data Pre-processing:** Cleans and formats data.
- **CSV File/Data Splitting:** Organizes data for analysis.
- **Data Extraction:** Retrieves relevant information for decision-making.

3. Blockchain Layer:

- **Smart Contracts:** Automates decision-making based on predefined rules.
- **Add Block to Blockchain:** Ensures secure and tamper-proof

storage of incident data.

4. Application Layer:

- **UAV Controllers:** Deploy drones to the appropriate response units.
- **Hospital:** For medical emergencies.
- **Fire Department:** For fire incidents.
- **Police Department:** For crime-related incidents.

5. Communication Layer:

- Uses **6G networks** to ensure fast and reliable communication between layers.

5. CONCLUSION

In this paper, we exhaustively investigated the current research trends in security and privacy of CAVs during 2016-2023 using Blockchain. The paper also investigated attack vectors and vulnerabilities for CAVs. that for record-keeping in different studies. But it is equally important here to mention that Blockchain has not been relied upon independently as a sole secure means of communication. The majority of the literature we investigated during this sur1vey has shown to be heavily dependent on traditional security measures such as trusted third party authorities, pseudonym and key generation algorithms that still bring inefficiencies and delays in providing timely secure communication. The need is to move away from the traditional security and trusted third party techniques and deploy new security algorithms over Blockchain, which are lightweight in their performance and efficient enough to ensure secure communication. Though Blockchain technology is also considered a means of providing security and privacy within CAVs as observed in the literature, it is not investigated independently as stan1dalone security and privacy parameter. Traditional encryption algorithms are being run on Blockchain, which further multi1plies the computational energy consumed by the Blockchain network and ultimately, the solution may not be as effective as it should be. Traditional encryption algorithms are quite heavy-weight, which requires heavy computational energy and takes a lot of time in calculating the results. Suppose traditional algorithms are tied up with Blockchain. In that case, it will maximize the computational energy and time required to generate the results as Blockchain itself utilizes quite a lot of energy in mining and authenticating data on blocks. It is suggested that future security and privacy measures for CAVs be designed around new encryption techniques over Blockchain, which is light enough to reduce the overall computational energy and time consumed. By doing so, the new world of CPS will be ready to face new challenges and threats posed due to cyber-attacks.

REFERENCES

[1] N. Kim, S. Rathore, J. Ryu, J. Park, and J. Park, “A survey on cyber physical system security for IoT: Issues, challenges, threats, solutions,” J. Inf. Process. Syst., vol. 14, no. 6, pp. 1361–1384, 2018, doi: 10.3745/JIPS.03.0105.

[2] M. Mackintosh, G. Epiphaniou, H. Al-Khateeb, K. Burnham, P. Pillai, and M. Hammoudeh, “Preliminaries of orthogonal layered defence using functional and assurance controls in industrial control sys1tems,” J. Sensor Actuator Netw., vol. 8, no. 1, p. 14, Feb. 2019, doi: 10.3390/jsan8010014.

[3] K. Sampigethaya, M. Li, L. Huang, and R. Poovendran, “AMOEBA: Robust location privacy scheme for VANET,” IEEE J. Sel. Areas Commun., vol. 25, no. 8, pp. 1569–1589, Oct. 2007, doi: 10.1109/JSAC. 2007.071007.

[4] M. B. M. Noor and W. H. Hassan, “Current research on Internet of Things (IoT) security: A survey,” Comput. Netw., vol. 148, pp. 283–294, Jan. 2019, doi: 10.1016/j.comnet.2018.11.025.

[5] A. R. Silva and M. C. Vuran, “(CPS)2 : Integration of center pivot systems with wireless underground sensor networks for autonomous precision agriculture,” in Proc. 1st ACM/IEEE Int. Conf. Cyber-Phys. Syst., Apr. 2010, pp. 79–88.

[6] F. Mehdipour, “Smart field monitoring: An application of cyber-physical systems in agriculture (work in progress),” in Proc. IIAI 3rd Int. Conf. Adv. Appl. Informat., Aug. 2014, pp. 181–184.

[7] S. I. Caramihai and I. Dumitrache, “Agricultural enterprise as a com1plex system: A cyber physical systems approach,” in Proc. 20th Int. Conf. Control Syst. Comput. Sci., Bucharest, Romania, May 2015, pp. 659–664.

[8] Y.-T. Li, M. Jacob, G. Akingba, and J. P. Wachs, “A cyber-physical management system for delivering and monitoring surgical instruments in the OR,” Surgical Innov., vol. 20, no. 4, pp. 377–384, Aug. 2013, doi: 10.1177/1553350612459109.

[9] D. I. Dogaru and I. Dumitrache, “Cyber-physical systems in healthcare networks,” in Proc. E-Health Bioeng. Conf. (EHB), Iasi, Romania, Nov. 2015, pp. 1–4.

[10] C.-U. Lei, H.-N. Liang, and K. L. Man, “Building a smart laboratory environment at a university via a cyber-physical system,” in Proc. IEEE Int. Conf. Teaching, Assessment Learn. Eng. (TALE), Bali, Indonesia, Aug. 2013, pp. 243–247.

[11] J. Wan, H. Yan, D. Li, K. Zhou, and L. Zeng, “Cyber-physical sys1tems for optimal energy management scheme of autonomous electric vehicle,” Comput. J., vol. 56, no. 8, pp. 947–956, Aug. 2013, doi: 10.1093/comjnl/bxt043.

[12] S. Jianjun, W. Xu, G. Jizhen, and C. Yangzhou, “The analysis of traffic control cyber-physical systems,” Proc. Social Behav. Sci., vol. 96, pp. 2487–2496, Nov. 2013, doi: 10.1016/j.sbspro.2013.08.278.

[13] H. Singh, “Big data, Industry 4.0 and cyber-physical systems integration: A smart industry context,” Mater. Today, Proc., vol. 46, pp. 157–162, Jan. 2021, doi: 10.1016/j.matpr.2020.07.170.