An Innovative Blockchain-Based Traceability Framework for Industry 4.0 Cyber-Physical Factory

William Davis*[a], Mahnoor Yaqoob*[a], Luke Bennett*[b], Stefan Mihai*[a], Dang Viet Hung*[b], Ramona Trestian*[b], Mehmet Karamanoglu*[b], Balbir Barn*[b], Huan Nguyen*[b]
**London Digital Twin Research Centre, Middlesex University*
The Burroughs, UK.
[a]{WD085, MY365, SM3488}@live.mdx.ac.uk, [b]{L.Bennett, D.VietHung, R.Trestian, M.Karamanoglu, B.Barn, H.Nguyen}@mdx.ac.uk

***Abstract*—Industry 4.0 is currently transforming the industrial landscape through the use of innovative technologies and novel data management approaches. The incorporation of Industry 4.0 brought new dimensions of improvement and autonomy into the existing industrial manufacturing processes which has also led to increased expectations for traceability in manufacturing. Traceability enables the tracking of every part and product of the manufacturing process giving insights into each manufactured component and its full history across each operation step that helps manufacturers improve quality and efficiency. Despite the huge potential in facilitating the optimization of the production lines, product traceability has remained a challenging topic in mass manufacturing. Hence, in this paper, an innovative Blockchain-based framework is proposed to integrate the processes of a real production line using the Industry 4.0 Festo Cyber-Physical Factory located at London Digital Twin Research Centre, Middlesex University. Blockchain technology is a distributed and shared database of events for a product life cycle that is encrypted in blocks or smaller data units. This paper introduces a viable blockchain-based framework implemented within a real smart product assembly for internal traceability within the production process in order to improve the security by preventing counterfeiting, identify specific problems on the production line and provide objective proof for product quality assurance.**

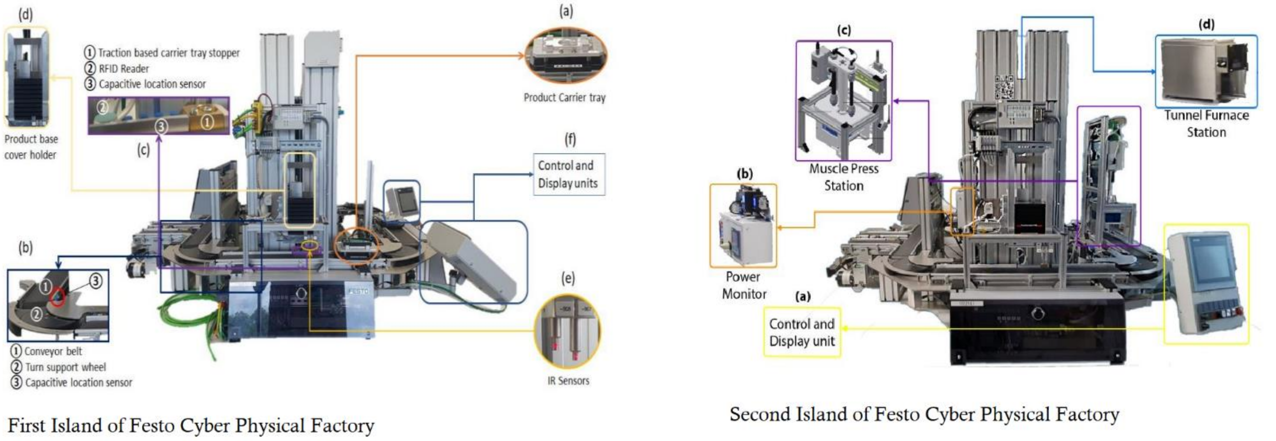
Keywords*—*industry 4.0, blockchain, cyber-physical factory

I. Introduction

The advent of Industrial Internet of Things (IIoT) has led to rapid advancements in manufacturing technologies which in turn enabled the creation of smart factories. A smart factory relies on the intersection of the real and digital worlds within manufacturing involving the full integration of manufacturing technologies and systems to deliver superior quality services along with an overall reduction in the time and cost for manufacturing. Industry 4.0 brings innovative technologies and novel data management approaches leading to increased expectations for traceability in manufacturing. In this regard, the integration of Blockchain technology is seen as a promising solution. Blockchain technology is a distributed and shared database of events for a product life cycle that is encrypted in blocks or smaller data units. These blocks (or ledgers) contain all the events and records shared among all concerned participants, for ease of verification in future. Blockchain can be implemented in any transaction to store and verify the product life cycle. Financial ledgers are the most common use cases for blockchain. Blockchain technology is not limited to supply chain and its applications are diverse, such as: voting, ownership management, energy supply, protecting critical civil infrastructure, electronic health records, etc. In [1], [2] the authors proposed originChain that aims to restructure the current central database systems with blockchain in order to provide transparent and tamper-proof information.

Over the years, the increase in food falsification has caused a lack of customer trust and economic loss. Authentication and tracking of the food supply chain have become a pressing issue for the industry and its stakeholders. Thus, Galvez et al. [3] have reviewed the potential of blockchain technology to ensure traceability, transparency, and legitimacy in the food supply chain. The authors have highlighted that blockchain in a food supply chain can be implemented at several stages: production, processing, storage, distribution, retail, and administration phases. Similarly, Tian et al. [4] have reviewed the utilization and development of Radio-Frequency Identification (RFID) within a blockchain environment and have identified the pros and cons of using RFID and blockchain technology for agriculture and the food supply chain. The authors have proposed a conceptual design for building an agri-food supply-chain traceability system. The study in [5] also introduces blockchain concepts for information security and transparent ledgers for the food supply chain. However, the data gathered is solely based on problems faced by China and its food industry. Motivated by the fact that blockchain technology provides a promising solution to the traceability problem in supply chain management, Liu et al. [6] have introduced a general framework based on blockchain for product traceability in e-commerce supply chain. The framework introduces a multichain structure model for storing all information, data management model, and a block structure model.

One of the latest paradigms in smart technologies is Communicating Things Network (CTN), a network of physical devices that can extract and share digital information. However, within an IIoT framework, it is possible for intruders to breach the devices' security. In this context, Rathee et al. [7] have proposed the integration of blockchain within a hybrid IIoT framework to extract information from IoT devices and store extracted records into the blockchain in order to maintain transparency among various users located at different places. Similarly, the authors in [8] developed a blockchain-based steel



First Island of Festo Cyber Physical Factory

Second Island of Festo Cyber Physical Factory

Fig. 1. Festo Cyber- Physical Factory islands and stations.

IoT quality traceability system using a hyperledger blockchain platform. The experimental results have shown that all stakeholders can participate in information authorization utilizing the system.

For today's complex agricultural supply chain, the task of efficient traceability is of utmost importance. Thus, in [9] the authors have proposed an approach that uses the Ethereum blockchain and smart contracts to accomplish transactions for tracking soybean production and distribution across the agricultural supply chain. This provides businesses with vital information to reduce cost and increase efficiency. Similarly, in [10] the authors have proposed ProvChain, a provenance architecture based on blockchain. The goal of ProvChain is to provide security, privacy and availability of data operations in a cloud storage application. Similarly, the provenance data are stored as records hashed in Merkle tree nodes.

Consequently, the integration of blockchain to enable secure and transparent traceability in the supply chain across different areas within Industry 4.0 is gaining significant importance lately. In this context, this paper introduces a viable blockchain-based framework implemented within a real smart product assembly for internal traceability within the production process in order to improve the security by preventing counterfeiting, identify specific problems on the production line and provide objective proof for product quality assurance.

II. Festo Cyber-Physical Factory

The Festo Cyber-Physical Factory installed at Middlesex University is a dedicated system performing the production assembly line operations [11], [12]. The cyber-physical lab (CP Lab) is composed of two production units called islands. These islands are connected via an Automated Guided Vehicle (AVG). Each island has four stations, and each station performs a dedicated assembly task. Furthermore, each production cell has an abridged station responsible for passing the product to AVG to pass it on to the next island. The stations communicate over two TCP servers running on the Manufacturing Execution System (MES). One server is a state server for simple diagnostics and connection related flags. The other is a messaging server that sends and receives ordering information such as order number, current work plan position, carrier ID, etc. When an order is placed through MES, a carrier tray is assigned to that particular order for the whole duration. The carrier tray moves from station to station through conveyor belt. Each station identifies the carrier, order number and progress using RFID to ensure that every order is processed only once at each module. Figure 1 shows an actual representation of the Festo Cyber-Physical Factory and its islands.

The production process starts at the first station, which is the **Magazine Front station** responsible for placing the lower-plastic casting onto the next available carrier. The carrier is checked using IR sensors. If the carrier is empty, the base cover is dispensed. The second station is the **Manual station**. Here, an operator is required to place the order specific Printed Circuit Board (PCB) onto the base cover at this station. Afterwards, a quality check is performed at **Camera inspection station**, to verify if the correct PCB is chosen. In case of unsuccessful visual inspection, the order is returned to the first island where each station will again verify the progress of the product through RFID and take actions accordingly until a visual inspection is successful. In case of successful visual inspection, the product is passed on to the **Bridge 1 station.**

From the bridging station, AVG transports the carrier to the **Bridge 2 station** on the second production unit. The next station on the second island is the **Magazine Back station**, responsible for placing the upper-plastic casing on top, closing in the PCB. Similarly, IR sensors detect if the product needs a top cover, and dispenses accordingly. The next station is **the Press station** where upper and lower parts of the product are pressed together at the desired pressure and time. With the available Human Machine Interface, the operator decides on the force needed to press the covers together. The time interval for which the pressure needs to be continuously applied is set on the order but can be changed using HMI. The last station is the **Heating station**. Here, the product is kept in the pre-heated furnace for a period which is preset in the order. Similarly, the HMI allows to modify the time, target temperature and monitor the actual temperature registered by the PT100 sensor inside the module and the total time the carrier has spent inside the oven. If the ambient temperature is lower than the target temperature, the heating and cross-flow blower is turned on until the target temperature is achieved. After this point, a countdown clock starts from a time interval picked by the user. When the time is up the carrier is out and it returns to the manual station via the bridge for order packing and freeing the carrier. At this point, the order is complete.

III. Development of Blockchain for Festo Cyber-Physical Factory

Due to the quantity of data being produced in Industry 4.0, it is not easy to properly harness this efficiently and securely whilst promoting anti-counterfeit methods. Therefore, one of the main focuses of this study is the production of blockchain receipts of authenticity for products. The products leave the production line to see their journey through the production process and provide proof of validity. Furthermore, it enables in-built security against computer trespassing and node corruption. The major contributions of the proposed blockchain framework for Festo Cyber-Physical Factory are as follows:

- To develop a system for uploading appropriate data to a decentralized blockchain network.
- To implement the system in an Industry 4.0 production line
- To provide blockchain receipt of authenticity for every product created

A. *Identifying Change in Blockchain*

The main form for a blockchain to take is as a Merkle Tree. A Merkle Tree enables us to hash a block so that it is virtually impossible to compromise and forge data. In most cryptocurrency blockchains, a set of transactions enter the tree; these are individually hashed and concatenated into one string in hexadecimal form. This string is then hashed, producing the root hash of the block.

To make the block secure and confident that it has not been tampered with, a vital piece of ’transaction’ data is time. Time is always changing. The hash of a block created at 17:15:10 is completely different from one created just a second later. For example, if a block claims to have been created at 17:15:10 and has a different hash than expected, the block must have been altered. To identify this change, a classifier named ’Blockchain’, was produced with two inputs: ’previousHash’ and ’transactions’. These were hashed together to create a variable called ’contains’. This process enabled the storage of the intermediary hash of the block before the final hashing. Thus, a block is created with the hash of a previous block.

Robot Operating System (ROS) has been used as a node-based platform to simplify the software on which the blockchain software is written. Furthermore, a listening script has been created to receive the blockchain data. All the nodes have identical data, and all nodes publish to each other.

B. *Dectecting Node Tampering*

If a node has been tampered with, falsifying the data, the block's hash will change. Since the goal is to implement blockchain within MES, the number of stations is finite, meaning only a limited number of nodes is required. As the number and names of nodes to be used are known (NODE1, NODE2, etc.), a 'nodesOnline' Robot Operating System (ROS) module was created, to which a node can publish online. This gives the node 'awareness' of other nodes active on the network. To emit a node name at the frequency of one transmission per second, all other processing continued sequentially each step having a different timestamp. The used threading technique allowed the node discovery function to go a stage further. Using a custom message in the 'emitter' function, the node name is sent in conjunction with the last hash created by the block with all data received from other nodes. If the nodes' previous hashes are the same, all data has been transferred across successfully, and nodes have not been compromised. If the hashes are different, one of the nodes has incorrect data. Figure 2 shows nodes subscribing to block data and publishing their hashes to the last hash.

To find which hashes hold the majority and which hashes are incorrect, an array is created to hold the hashes - with the index of each hash being the number of whichever nodes the hash came from. Once a hash discovered to be a minority – to be changed – it is simple to carry out an array search to find which index matches the offending hash; the index is the same as the node's name and, therefore, reveals the compromised node. While the emitter() function used to broadcast the last hash showed that the data's transmission had not been compromised, it did not prove the node was secure. The emitter() function had to be replaced with a dedicated array to handle the blocks' hashes. This array is fed into a loop and is repeatedly hashed until the end of the array. That hash is then broadcast every five seconds, synchronized to clock time so that every node is published simultaneously. Algorithm 1 demonstrates salt hashing to find the hash of the node.

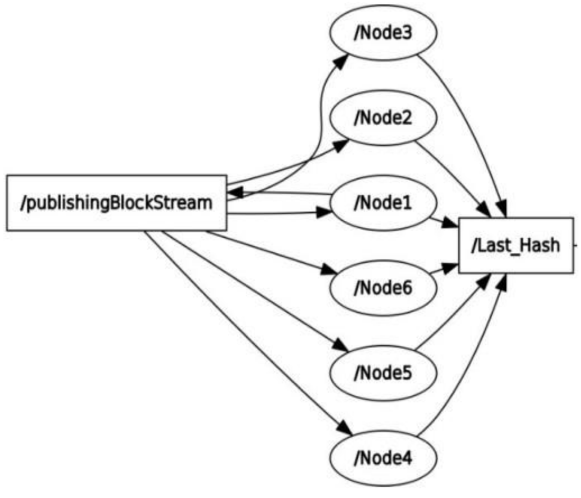


Fig. 2. Nodes subscribing to block data and publishing their hashes to Last Hash.

Algorithm 1: Broadcasting a node’s hash across the network

```
for $i \le orderQuantity$ do
  for $j \le carrierQuantity$ do
    for $z \le blockchainLength$ do
      $MasterHash = generateHash(MasterHash + Blockchain[z])$
BroadcastAcrossNodes(MasterHash)
```

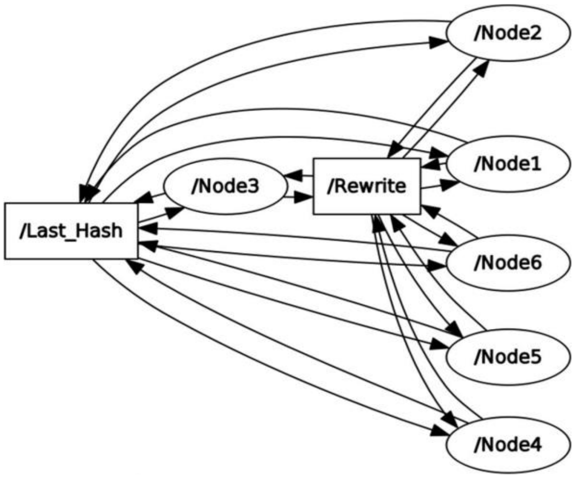


Fig. 3. Nodes publish/subscribe to the rewrite function.

When rewriting a compromised node, all of the array data needs to be transferred to the other node as quickly as possible. However, the compromised node first has to be wiped and then reinitialised. Once the node has been completely rewritten, the emitter() function then broadcasts an updated hash that should be the same as majority hash. Figure 3 demonstrates how the nodes publish and subscribe to the rewrite function.

To communicate with PLCs, TCP server is used. PLCs act as a TCP Client a transmit a data string on every clock cycle. The Python scripts act as TCP Servers and handle data parsing. An example of a PLC string would be: 1,1300,211,3,32,45,02,17,03,2021. This refers respectively to: station name, order number, carrier ID, product number, seconds, minutes, hours, days, months, years.

C. *Linking Created Products to Their Blockchain Receipts*

The final step was to link the created products to their accompanying blockchain receipts. A Raspberry Pi's is equipped with a camera running the OpenCV module, a computer vision package. QR codes were then attached to the top lids of every product. When a QR code is decoded, the user is taken to a file server running on the Raspberry Pi. When a product reaches the manual station for the second time (once it has finished a lap) the QR code is scanned by the camera and the data sent via ROS and written to a global variable. Callback() in Node2 then renames the receipt to say it is completed. This is then copied to the file on the file server at the QR code's address. When a user scans that QR code with their smartphone and connects to the MES System's network, that specific product's blockchain receipt is then revealed.

IV. Blockchain- Based Festo Cyber-Physical Factory Workflow

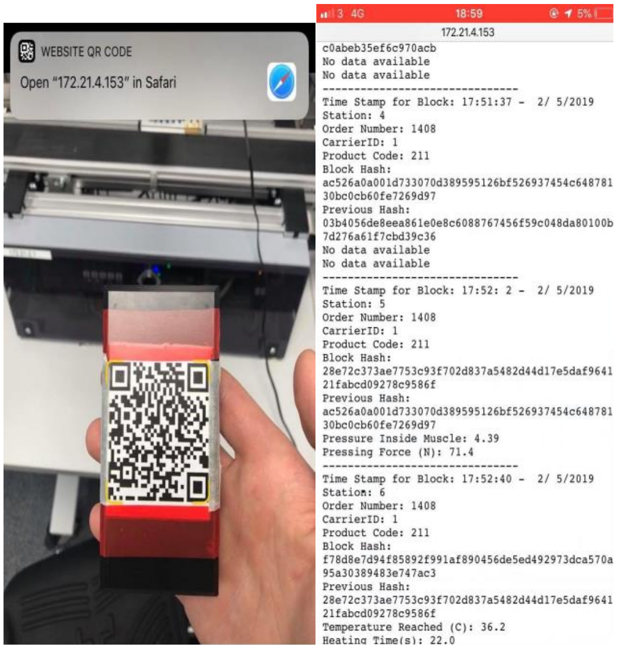
The blockchain solution has been integrated within the production line process of the Cyber-Physical Factory described in Section 2. The workflow of the proposed solution consists of two stages: blockchain initialization and receipt generation.

A. *Blockchain Initialization*

The blockchain system is hosted on three Raspberry Pis. Each Raspberry Pi has two blockchain nodes running on them for a total of six nodes. Each node is in direct communication with one station (the Bridge 1 and 2 stations are excluded) within the CP Lab. Initiating an order on the MES requires a secure hash ('license key') sent to the license server and the customer number and order requirements. The server will check if the key is valid. If successful, the order details will be sent to MES, where an order will be created. The MES will allocate the newly created order to the next available carrier on the CP Lab. It does that via an RFID tag located on the bottom inside edge. The Magazine Front Station is the first station in the work plan thus, the RFID tag first gets populated here. The information written to it includes an order number, product number and current station position. Once the RFID tag has been successfully written to, the station will send the Carrier ID, current order details and status (including a timestamp) to the blockchain system, which will initialize a new blockchain. The node that initialized the blockchain then broadcasts its information across the network to the other five nodes, which in turn create new genesis blocks and their own root hashes. Finally, these root hashes are broadcast through the network. If a root hash is detected to be different to the majority, the connected node will be classed as corrupt, and a re-write operation will be carried out as explained in Section 3.

B. *Receipt Generation*

The Magazine Back Station drops the top casing onto the assembly. Before loading the hopper, all the casings have a QR code mounted on the surface. The QR code acts as a unique link to the blockchain created for this specific product. The last station the carrier will reach is the manual station again. Workers remove the part from the carrier for packing. Above this station, a camera is mounted and scans the QR code, and the RFID is read. The software then links this QR code to the blockchain that was created. A user can then find out the history of the product's production life cycle along with its serial number as proof of authenticity. An example is illustrated in Figure 4.



WEBSITE QR CODE

Open "172.21.4.153" in Safari

172.21.4.153

```
c0abeb35ef6c970acb
No data available
No data available
-------------------------------
Time Stamp for Block: 17:51:37 -  2/ 5/2019
Station: 4
Order Number: 1408
CarrierID: 1
Product Code: 211
Block Hash:
ac526a0a001d733070d389595126bf526937454c648781
30bc0cb60fe7269d97
Previous Hash:
03b4056de8eea861e0e8c6088767456f59c048da80100b
7d276a61f7cbd39c36
No data available
No data available
-------------------------------
Time Stamp for Block: 17:52: 2 -  2/ 5/2019
Station: 5
Order Number: 1408
CarrierID: 1
Product Code: 211
Block Hash:
28e72c373ae7753c93f702d837a5482d44d17e5daf9641
21fabcd09278c9586f
Previous Hash:
ac526a0a001d733070d389595126bf526937454c648781
30bc0cb60fe7269d97
Pressure Inside Muscle: 4.39
Pressing Force (N): 71.4
-------------------------------
Time Stamp for Block: 17:52:40 -  2/ 5/2019
Station: 6
Order Number: 1408
CarrierID: 1
Product Code: 211
Block Hash:
f78d8e7d94f85892f991af890456de5ed492973dca570a
95a30389483e747ac3
Previous Hash:
28e72c373ae7753c93f702d837a5482d44d17e5daf9641
21fabcd09278c9586f
Temperature Reached (C): 36.2
Heating Time(s): 22.0
```

Fig. 4. A demonstration of how the QR Codes can be scanned to reveal the blockchain associated with the connected product.

V. Conclusions

This paper implements a blockchain solution for product traceability within the Festo Cyber-Physical Factory located at Middlesex University. Within the proposed framework, data is harvested effectively, stored and used through a decentralized network to effectively maintain security and prevent breaches. This work demonstrates that blockchain can be integrated within the product's production life cycle to enable proof of authenticity.

Acknowledgment

This work was supported by the UK-India Education and Research Initiative (UKIERI) and the Department of Science and Technology (India) under Grant DST UKIERI-2018-19-011.

References

[1] X. Xu, Q. Lu, Y. Liu, L. Zhu, H. Yao and A. V. Vasilakos, 'Designing blockchain-based applications a case study for imported product traceability', Future generations computer systems, vol. 92, pp. 399–406, 2019.

[2] Q. Lu and X. Xu, "Adaptable Blockchain-Based Systems: A Case Study for Product Traceability," in IEEE Software, vol. 34, no. 6, pp. 21-27, November/December 2017, doi: 10.1109/MS.2017.4121227.

[3] J. F. Galvez, J. C. Mejuto, and J. Simal-Gandara, 'Future challenges on the use of blockchain for food traceability analysis', *TrAC Trends in* Analytical *Chemistry*, vol. 107, pp. 222–232, Oct. 2018, doi: 10.1016/j.trac.2018.08.011.

[4] F. Tian, 'An agri-food supply chain traceability system for China based on RFID & blockchain technology', *2016 13th International Conference on Service Systems and Service Management (ICSSSM)*, 2016, doi: 10.1109/ICSSSM.2016.7538424.

[5] D. Tse, B. Zhang, Y. Yang, C. Cheng and H. Mu, "Blockchain application in food supply information security," 2017 IEEE International Conference on Industrial Engineering and Engineering Management (IEEM), Singapore, 2017, pp. 1357-1361, doi: 10.1109/IEEM.2017.8290114.

[6] Z. Liu and Z. Li, 'A blockchain-based framework of cross-border e-commerce supply chain', International Journal of Information Management, vol. 52, p. 102059, Jun. 2020.

[7] G. Rathee, A. Sharma, R. Kumar, and R. Iqbal, 'A Secure Communicating Things Network Framework for Industrial IoT using Blockchain Technology', *Ad Hoc Networks*, vol. 94, p. 101933, Nov. 2019.

[8] Y. Cao, F. Jia and G. Manogaran, "Efficient Traceability Systems of Steel Products Using Blockchain-Based Industrial Internet of Things," in IEEE Transactions on Industrial Informatics, vol. 16, no. 9, pp. 6004-6012, Sept. 2020, doi: 10.1109/TII.2019.2942211.

[9] K. Salah, N. Nizamuddin, R. Jayaraman and M. Omar, "Blockchain-Based Soybean Traceability in Agricultural Supply Chain," in IEEE Access, vol. 7, pp. 73295-73305, 2019, doi: 10.1109/ACCESS.2019.2918000.

[10] X. Liang, S. Shetty, D. Tosh, C. Kamhoua, K. Kwiat, and L. Njilla, 'ProvChain: A Blockchain-based Data Provenance Architecture in Cloud Environment with Enhanced Privacy and Availability', in *Proceedings of the 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing*, Madrid, Spain, May 2017, pp. 468–477, doi: 10.1109/CCGRID.2017.8.

[11] M. Raza, P. M. Kumar, D. V. Hung, W. Davis, H. Nguyen, and R. Trestian, 'A Digital Twin Framework for Industry 4.0 Enabling Next-Gen Manufacturing', in *2020 9th International Conference on Industrial Technology and Management (ICITM)*, Feb. 2020, pp. 73–77.

[12] Mihai S, Davis W, Hung DV, Trestian R, Karamanoglu M, Barn B, Prasad R, Venkataraman H, Nguyen HX. "A digital twin framework for predictive maintenance in industry 4.0", presented at the HPCS 2020, Barcelona, Spain (Online Virtual Conference), March. 2021.