International Journal of Multidisciplinary Engineering in Current Research
ISSN: 2456-4265, Volume 6, Issue 7, July 2021, http://ijmec.com/

ORIGIN DISTRIBUTED LEDGER FOR ENSURING IT SECURITY IN CLOUD MANUFACTURING

Dr. Bhargav Gangadhara,
[1]*Senior Technical lead/Director, Jack Henry and Associates, USA*
[1] *bhargavmtechmem@gmail.com*

ABSTARCT: Origin distributed ledger is an evolving concept for protection of production, logistics, and supply chain networks from rogue Industrial Internet of Things (IIoT) devices. Such rogue IIoT devices are a recognized threat in the cloud manufacturing networks. In extreme cases, they can be used to cause industrial accidents. A brief version of origin is about end-to-end tracking and tracing of data and the nodes involved in creating, modifying, transmitting, storing, and deleting it at specific times and locations. It providesan end-to-end verifiable and controlled computation for ensuring trustworthiness, quality, reliability, and validity of data. Origin has existed in computing using logging software systems. This research is focused on threats to food supply chains between two countries. A scenario for protecting food supply chain from India to UAE has been modeled. This research recognized the threat of harmful food items getting mixed with flow of genuine products in a supply chain. The IIoT devices used to control the flow can be authenticated using the evolving origin distributed ledger technology. With the help of recent design recommendations in the literature, a model design has been created and simulated in this research. Observations from the simulation revealed that TCP congestions and unpredictable turnaround time for assigning cryptographic keys to IIoT device sessions may have to be explored in future. A collaborative design between the two nations has been proposed. All IIoT devices not supporting cryptography will be eliminated from the cloud manufacturing and supply chain networks. Currently, this design may be used for one time registration only. Future studies may provide improved versions in which, repeated authentication and keysreplacements may be implemented.

KEYWORDS: industry 4.0, logistics 4.0, block chain, IT security, cloud manufacturing

I. INTRODUCTION

The global manufacturing industry is gradually entering the era of highly competitive, personalized, and complex demands from the customers, and hyper-automation, flexible, and responsive solutions for developing dynamic capabilities to meet those demands (Akdil et al., 2018; Eruvural and Eruvural, 2018; Salkin et al., 2018; Felsberger et al., 2022). Customers have better power and influence through socialization of products, processes, and services delivered through social networking of manufacturing processes and systems having high emphasis on systemic learning and experiencing (Ajayi and Laseinde, 2023; Atieh et al., 2023). In this new era, the information technology, systems, and communication (ITSC)

infrastructure is closely integrated with the operations infrastructure of manufacturing organizations under a new framework called Industry 4.0 (Lemstra and de Mesquita, 2023). Machines, machine tools, and robots have been digitalized for operating them in the servitisation mode (Liu et al., 2023). Modern technologies involving Industrial Internet of Things (IIoT), autonomous and adaptive robotics and machines, big data analytics, vertical and horizontal integration, machine learning, augmented reality, cyber-physical production, distributed

ledgers, cloud manufacturing, additive manufacturing, human-robots collaborative systems, have been adopted by manufacturing organizations to adapt with the changing dynamism of markets, consumer demands, and business environments (Lemstra and de Mesquita, 2023).

The production, logistics, and supply chain engineering systems are interconnected and Internet enabled using IIoT (Lemstra and de Mesquita, 2023). The legacy networks of these engineering systems were formed using programmable logic controllers, and supervisory/ distributed control systems (Wollschlaeger et al., 2017). These physical systems were always present and later digitally transformed using IIoT to support TCP/IP in addition to their traditional proprietary protocols (such as LONWORKS and BACNET). With proprietary protocols, these networks formed islands of connectivity, but IIoT-enabled digital transformation using open protocol TCP/IP caused comprehensive connectivity among all the engineering systems used by manufacturing organizations. Thus, industrial systems capable of sensing the process parameters can collaborate cognitively and send their data/reports to big data servers on the cloud computing (Aileni et al., 2020). The manufacturing controllers are deployed on cloud computing over big data servers for making judgments based on collective analysis of sensory data and send back commands for actuation, tuning, or disabling of process-governing parameters to the field-level engineering systems (Ghomi et al., 2019). The engineering systems integrated using IIoT form the perception layer, which is the primary addition in the Industry 4.0 framework as compared with its predecessor (Industry 3.0).

The layers above the perception layer are modern versions of the traditional IT infrastructure deployed on cloud computing. The perception layer caused digital enablement of the engineering systems using open protocol TCP/IP, and hence caused the IT vulnerabilities to enter the production shop floors, logistics systems, and supply chain networks (Eruvural and Eruvural, 2018).

One of the most significant vulnerabilities is related to compromise of IIoT devices in the engineering systems, which can be used remotely by attackers as the entry points for their exploits causing process anomalies or even physical disasters (Yazdinejad et al., 2023a). IIoT devices are increasingly deployed in critical industrial systems (such as temperature and pressure monitoring and control) in smart factories (Yazdinejad et al., 2023b). Collecting, storing, and analyzing industrial monitoring data may offer critical safety services. However, if their security and privacy are compromised, they can be exploited to cause breakdowns in critical industrial systems. If a mechanism for ensuring authentication, authorization, and accounting of IIoT devices in the perception layer can be developed, this vulnerability can be reduced significantly. Recently, an approach actively discussed in academic studies is origin data capturing and storing in controlled block chains in cloud computing to reliably authenticate, authorize, and account the IIoT devices deployed in action in cloud manufacturing and supply chain networks (Ali et al., 2018; Ramachandran and Kantarcioglu, 2018; Ruan et al., 2019; Kaaniche et al., 2020; Tang et al., 2019; Siddiqui et al., 2020). This is the primary focus of this research. Fundamentally, this approach involves certification and monitoring of IIoT devices deployed within a manufacturing and supply chain networking using Distributed ledger technology to enhance reliability and reduce chances of entry of malicious actors in such networks. Conceptually, this approach appears to be promising, but its realization in practice is still an open research domain. This research investigates a realistic scenario for realizing the approach in practice using modeling and simulation in a networking simulation software. The scenario is to monitor a packaging and forwarding network of packaged food products in Western India supplying directly to the

International Journal of Multidisciplinary Engineering in Current Research
ISSN: 2456-4265, Volume 6, Issue 7, July 2021, http://ijmec.com/

customers in GCC countries employing a Distributed ledger controlled by GCC. The IIoT devices in action are used in the cloud manufacturing network of those products comprising authorized manufacturers by the GCC. A block chain control algorithm is investigated for authentication, authorization, and accounting of IIoT devices deployed in the facilities of the authorized cloud manufacturers. In this context, the research questions formulated for the investigation are the following:

a) What threats exist in the IIoT-enabled perception layer of cloud manufacturing?
b) How can origin data system in block chain ledgers be used for mitigating the risks arising from threats to IIoT network in cloud manufacturing?
c) What are the theoretical and practical implications in implementing and operating a block chain with origin data system to secure packaged food supplies from India to GCC countries?

Highlights of this research are the following:

a) A focused review of recent literature on threats and solutions built upon origin block chain in the perception layer of cloud manufacturing;
b) A detailed network model of origin architecture within the block chain technology;
c) Design of an algorithm for authentication, authorization, and accounting of IIoT devices deployed in the facilities of the authorized cloud manufacturers in Western India supplying packaged food products directly to the customers in GCC countries;
d) Simulation of the algorithm in the network model and its analysis;
e) A discussion on the theoretical and practical implications in implementing and operating a block chain with origin data system to secure packaged food supplies citing the literature studied and the simulation results;

The literature review has been conducted following the sequence outlined below:

Section 2: a brief review to understand cloud manufacturing is presented in this section. Cloud manufacturing is a sophisticated and highly technical subject. Hence, it has been touched to the extent this research can gain relevant guidance and quickly delve into its main focus area.

Section 3: this section presents a deep review of the problem ofthreats in cloud manufacturing's perception layer analyzed in this research. This section provides inputs to the reader to understand the problem and also appreciate the effectiveness of solutionsevolving.

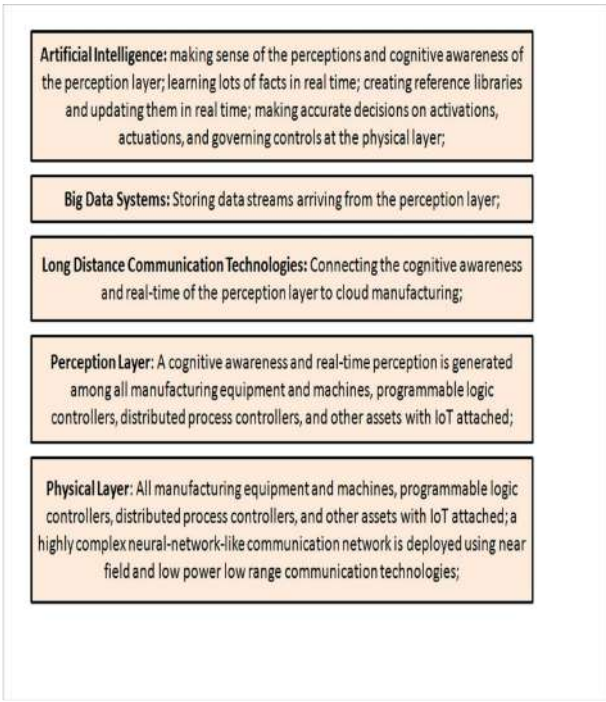
Section 4: this section presents a deep review of origin block chain that is one of the solutions researched in the recent past. Origin block chain is the main focus of this research and hence its design details have been reviewed deeply to build required knowledge for designing the origin algorithm, modeling a block chain in a network modeler and investigating it in its network simulation.

II. UNDERSTANDING CLOUD MANUFACTURING–A BRIEF REVIEW

This section presents a brief yet deep review of cloud manufacturing (C-MFG). C-MFG is a new innovation that allows multiple manufacturers to form a network to service common demand streams irrespective of their physical locations. The manufacturing design is component-based instead of the older assembly line designs. The individual components are integrated through cloud computing forming virtual assembly lines operating on a network of manufacturing contributors (Lim et al., 2021). The cloud C-MFG apps on cloud computing are configured to register individual components map them with individual services thus forming a pool of manufacturing services, such as

International Journal of Multidisciplinary Engineering in Current Research
ISSN: 2456-4265, Volume 6, Issue 7, July 2021, http://ijmec.com/

design, simulation analysis, production, testing, quality control, packaging, and shipping. A manufacturing package is offered to customers in the form of composite cloud services (CCS). A simplified representation of C-MFG layers is presented in Figure 1. The capability to contribute to C-MFG requires several changes in the physical manufacturing plants. At the core is the IIoT attached with manufacturing systems causing a paradigm shift to the ways sensing and actuation was done in manufacturing environments (Aileni et al., 2020; Tiwari and Khan, 2020). IoT has the capability of capturing continuous data on movements, and data on operating parameters of running machines and equipment, machine tools, and robots with spatial and location-based information in a dynamic manufacturing environment (Haghnegahdar et al., 2022; Shrivastava et al., 2023). With the conceptualization of privacy protected distributed ledgers for cloud manufacturing, efficiencies in data collection, storage, and transactions can improve significantly thus paving way to services-oriented networked manufacturing offered through cloud computing platforms (Hasan et al., 2021; Barenji, 2022).



Data streams to big data systems supporting manufacturing controllers on cloud computing are generated automatically without need for field-level validation. The automated data streams from the IIoT devices constitute real-time visibility of manufacturing processes forming a virtual perception layer with cognitive abilities of an entire physical layer of manufacturing plants (Aileni et al., 2020; Tiwari and Khan, 2020). The cognitive perceptions formed by the IIoT devices internetworked at the perception layer (fitted exactly over the physical layer) may be visualized as a neural network of manufacturing systems having their own communication mechanisms and protocols to form an industry wide consciousness (Ojha et al., 2021). The manufacturing components attached with IIoTs can enter peer-to-peer and group communications to participate in collaborative tasks, such as real-time synchronization of production and logistics.

At the layers above big data systems, artificial intelligence systems are deployed to make sense of the perceptions captured by the perception layer, and make accurate actuation, activation and governing decisions using semantic visualization, search and validation algorithms, and matching (Ojha et al., 2021; Tiwari and Khan, 2021). Machine Learning is expected to build its reference libraries of knowledge ontologies, various execution case scenarios developed through real-time deep learning or through simulations, and all available services resources with their real-time tracking of allocations and utilizations (Simeone et al., 2019; Zhang et al., 2022).

C-MFG is a significantly large subject requiring numerous books and articles to be covered. This research covers it at the level required to understand the perception layer threats such that the research can now delve deeply into the problem investigated.

International Journal of Multidisciplinary Engineering in Current Research
ISSN: 2456-4265, Volume 6, Issue 7, July 2021, http://ijmec.com/

III. CYBER SECURITY THREATS IN PERCEPTION LAYER OF CLOUD MANUFACTURING–PROBLEM ANALYSIS

Cyber security threats in cloud manufacturing system need to be visualized with a different perspective as compared with those threats in self-hosted manufacturing and supply chain computerized control systems (Yazdinejad et al., 2023a; Yazdinejad et al., 2023b; Gupta et al., 2021). The perspective should visualize digital cyber security threats transforming into physical impacts by carefully scrutinizing the sensing and actuation anomalies caused by the malicious actors. Network telescopes and Darknets can direct malicious payload traffic towards the manufacturing networks by sneaking their owned IIoT devices and cause poisoned data injections in running IIoT- enabled industrial sensors (Shaikh, 2019). Data poisoning in IIoT- enabled network sensors can change the perceptions captured by the big data and machine learning layers from the perception layer through continuous injection of anomalies by advanced persistent threats causing deviations from on-the-ground realities (Gan et al.,2023). For example, the human-robot or robot-robot messaging for collaborations can be broken to cause automation failures resulting in process anomalies, production failures and even industrial accidents. Normally, protection against remote code execution tactics is robust but rogue IIoT devices installed by insiders can cause a major loophole (Shaikh, 2019). The more worrying trend is about insiders creating deliberate loopholes. The activity is roughly speculated to be about 30% of the overall number of attacks (Sobers, 2021). The extent to which unsolicited IIoT devices can be sneaked into manufacturing networks has not been estimated yet. However, there is a chance that such devices are already entering manufacturing systems because of lack of regulated manufacturing of IIoT devices causing ineffective security controls and absence of regular patch updates in those devices available in the market (Gan et al., 2023). This is because the emphasis is on designing for ease of user acceptance, deployment and usage (Gan et al., 2023). With increasing number of such devices getting inside manufacturing networks,the dark net can become much bigger threat in future as global attackers try their remote code execution skills using malicious power shell binaries causing logic flow corruption or compromise the communication channels (Shaikh, 2019; Barrere et al., 2020; Gan et al., 2023). Their advanced persistent threats can be slow acting, progressive, long lasting, and very difficult to detect (Gan et al., 2023). Attacks on IIoT devices can be carried out through their data interface structure designed on Message Queue Telemetry Transport (MQTT) protocol (Hintaw et al., 2019; Hintaw et al., 2023). MQTTis the most used machine-to-machine communication protocol (Shilpa et al., 2022). It is represented by an ISO standard ISO 20922: 2016, which can be combined with Public Key Infrastructure (PKI) standard to secure command and control messages flow using the MQTT protocol (Hastings et al., 2020). Given its popularity and standardization, security of the MQTT protocol is now gaining interest of researchers. MQTT is used for billions of devices controlled remotely by smart phones and tablets (Mishra and Kertesz, 2020). MQTT interactions are very simple “publish and subscribe” sessions (Hintaw et al., 2019). All interactions pass through running MQTT broker software. The IIoT devices communicate through the broker to “publish” their readings using PUT programs and the computers, tablets, or mobile smart phones receiving the data “subscribe” to the readings using GET programs. PUSH programs are used to send commands to the IIoT devices. Several open source MQTT broker software are available to deploy the broker instances (Hintaw et al., 2019; Mishra and Kertesz, 2020). Examples are: Mosquitto, EMQX, ActiveMQ, HiveMQ CE, RabbitMQ, and VerneMQ. The MQTT communications are standardized through interactions. However, the broker instances have specific flags allowing additional features, such as multiple

International Journal of Multidisciplinary Engineering in Current Research
ISSN: 2456-4265, Volume 6, Issue 7, July 2021, http://ijmec.com/

clients sharing a single subscription, persistent connections transferred between brokers, and retention of messages exchanges. The brokers are deployable on cloud computing using Dockers acting as micro services virtual machines.

The MQTT brokers offer in-built cipher suites for SSL and TLS with SHA hash codes up to 256 bits for encryption of messaging (Hintaw et al., 2019). However, the encryption may not be end-to- end requiring additional layer of PKI for devices that support its integration (Hastings et al., 2020). The traffic between subscribers and brokers may be encrypted but the traffic between IIoT devices and the brokers may not be encrypted always because not all IIoT hardware support SSL and TLS cipher suites. The clear text message transfers can be interrupted by malicious actors. Further, the current systems do not have checks to ensure that either the publishers or the subscribers are authenticated. Additional layers for authenticating human subscribers may be created but IIoT devices are authenticated using device ids and passwords entered in the system configuration files of the brokers and the devices (Hintaw et al., 2023). The devices send the credentials as a part of the payloads that can be interrupted by the hackers. Thereafter, a hacker can replace the device with a counterfeit using the same credentials. Every IIoT device may not be protected using PKI integration given the high cost of implementation. Hence, corporations may focus on identifying and replacing compromised devices. The next section presents this solution that is the focus of this research.

IV. ORIGIN DISTRIBUTED LEDGER FOR ENSURING IT SECURITY IN CLOUD MANUFACTURING–ANALYSIS OF THE SOLUTION IN FOCUS

As discussed in the previous section, the most popular communication protocol for machine-to-machine communications is MQTT. However, it has flaws in its authentication, authorization, and accounting system controlledthrough MQTT brokers. Given that devices do not seek authentication like human users, their login credentials are stored in their configuration files, which can be accessed by hackers because of lack of encryption support in many IIoT devices. Further, devicescan be easily replaced by counterfeits by insider workers maintaining them at the ground level. An improved framework of authentication, authorization, and accounting (AAA) of cyber physical devices is required to identify them and record them for validation using their origin information. The framework is different than traditionalIT security controls of human users.

The AAA controls shall require additional capabilities of

tracking and tracing movements, locations, and usage of devices, anti-counterfeit controls, and data quality controls, which are not followed in controlling human-accessed systems. The cyber physical devices security requires a new mechanism of AAA called origin. In this research, the solution in focus is origin using distributed ledger, which is capable of securing thousands of cyber physical manufacturing devices in a cloud manufacturing framework.

Origin is about end-to-end tracking and tracing of data and the nodes involved in creating, modifying, transmitting, storing, and deleting it at specific times and locations (Hu et al., 2020). It provides an end-to-end verifiable and controlled computation for ensuring trustworthiness, quality, reliability, and validity of data. Origin has existed in computing using logging software systems. However, logging is not effective as it has a lag caused by log filtering and analysis. Further, it does not provide instantaneous AAA administration to prevent the threats immediately at their incidence. These limitations are perceived to be eliminated in the origin distributed ledgers conceptualized and designed recently by several research studies, such as Javaid et al. (2018), Kaaniche et al. (2020), Ramchandran and Kantarcioglu (2018), Ruan et al. (2019) and Sigwart et al. (2020).

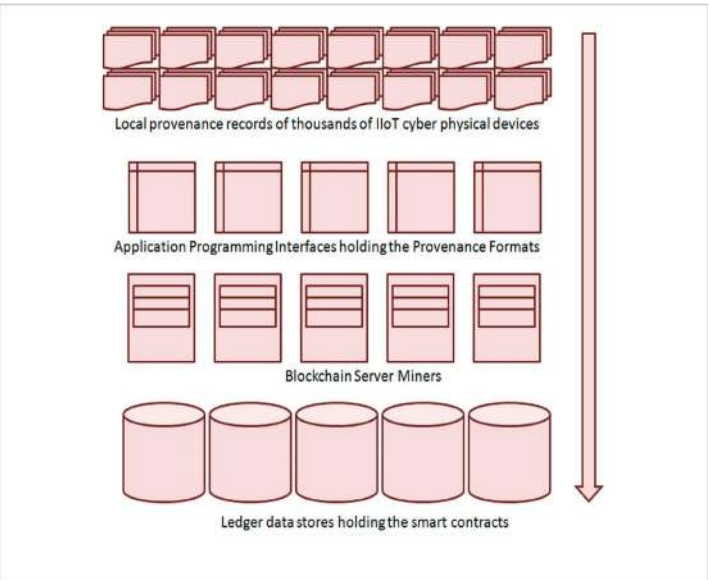
The designs evolving in recent academic studies comprise

of origin distributed ledgers institutionalized as AAA authority for recognizing, registering, recording, and controlling IIoT cyber physical devices. The distributed ledgers are designed to provide origin data confidentiality, integrity, verifiability, auditability, accountability, and privacy preservability (Kaaniche et al., 2020; Sigwart et al., 2020). Some of the key distributed ledger roles may be: data owner, data user, origin auditor, and origin validator. The distributed ledgers may be orchestrated nodes deployed in a multi-cloud design. This is the infrastructure part. The services require integrated strategic consensus modeling, data modeling, and block structure (Ruan et al., 2019). The block structure may comprise of block hash, transaction digest, and state digest. Both the transaction and state digests in a block need to be executed to match the results with the values stored in the digests of a specific block with a block hash. If results match, the block will be considered as non-tampered and will be allowed to get entered into the ledger linked with the smart contracts seeking the origin data feed.

The actual infrastructure design has been presented referring to the

papers by Sun et al. (2022), Popovic et al. (2022), and Jyoti and Chauhan (2022). The block records will be transmitted over encrypted links in the form of block files (preferably in JavaScript Object Notation format), which can be parsed by parsers written in Core Java and then encrypted before storing as read only records. All distributed ledgers will be front ended by Application Programming Interfaces (APIs) with predefined file structures to secure transactions related to fetch data, post data, and lock (encrypt) data. The file structures will be visible only to the authenticated APIs. The blocks received in the API should be compatible with the file structures defined by the distributed ledger APIs. The structure will be validated and tested before the distributed ledger will validate and store the blocks in the ledgers. Thus each distributed ledger will have respective localized storage on the hosting cloud. The distributed ledgers can be hosted on single as well as multiple clouds. In multi-cloud architecture, the distributed ledger will need APIs deployed on each cloud acting as network peers. All traffic shall be encrypted using TLS and SSL ciphers. A simplified diagram is presented in Figure 3 combining the architectures recommended by Sun et al. (2022), Popovic et al. (2022), and Jyoti and Chauhan (2022): Figure 2 shows the IIoT cyber physical devices sending their local origin records to the APIs of the distributed ledgers server miners. As per the MQTT design discussed in the previous section, these APIs may be MQTT brokers but with advanced features such as standardized block formats. As the first level of control, origin records not received in the standard block format will be rejected by the APIs. As the origin records are visible only to authenticated APIs, it will be impossible for a malicious actor to install an IIoT device outside an authenticated network and push it into a cloud manufacturing network. Hence, the first hurdle faced by the attacker will be to poach into an organization to hire an insider trader. When the insider trader tries to sneak an external IIoT device into the cloud manufacturing network, the next hurdle will be to prepare its internal block format exactly the way defined by the distributed ledger APIs. Many variables will require active feeds from the APIs of the manufacturers of the devices. The origin distributed ledger will also have a validation function that can connect to the multiple parties for validation before allowing the IIoT device into the cloud manufacturing network. In practice, an attacker may have to break through multiple validations before sneaking the IIoT device into the network making their job tougher. Many devices will come preloaded with authenticated origin block formats those will download several variables from their APIs before attempting to connect to the network.

International Journal of Multidisciplinary Engineering in Current Research
ISSN: 2456-4265, Volume 6, Issue 7, July 2021, http://ijmec.com/



The interaction topology and algorithm was presented referringto the designs by Jyoti and Chauhan (2022) in their secure origin-based smart contracting architecture, and by Malik et al. (2022) in their PrivChain architecture. A simplified representation of the secure origin-based smart contracting architecture is presented in Figure 3 and PrivChain architecture is presented in Figure 4. Both the studies recommend the architecture comprising the origin distributed ledger as the trust third party that is tasked to attest about the "secret information" using cryptographic verification without knowing the content of the secret information.For this design, these two studies recommended storage of origin data at the origin distributed ledger and storage of the cryptographic keys at the storage of the attester. The origin data is stored at two locations: at the cloud service provider in the space provided for the data owner, and on the distributed ledger comprising the smart contracts linked with origin information. Whenever a new user requests for registration of a data for this purpose (using a temporary key generated by the key generation centre), it makes a request to the cloud hosted application by uploading the data to be verified. A cycle of validation is triggered to validate the data from the distributed ledger. The cloud hosted application allows temporary storage of origin data in the origin data store and also publishes it to the distributed ledger. In the next step, the user requests the origin auditor to validate the origin information of the data. The origin auditor requests the origin distributed ledger to validate the data. Based on the verification by the distributed ledger, the validation status is shared back with the user.

The cycle shown in Figure 3 by Jyoti and Chauhan. (2022) can be used for validating origin of any product received from a supply chain by simply scanning its data on its QR code sticker. The same concept is presented by Malik et al. (2022) in their secure origin-based smart contracting architecture replicated in Figure 4. The differences between the flows of Figures 3, 4 are that in the latter the consumer directly contacts the distributed ledger for origin validation, the bank is involved with the distributed ledger such that the payments are made only after verification and commitment of origin records, and there is no auditor for origin validation. In this design, the origin data is stored only on the distributed ledger and there is no temporary storage of origin data for validation.

The origin distributed ledger solution proposed by the recent

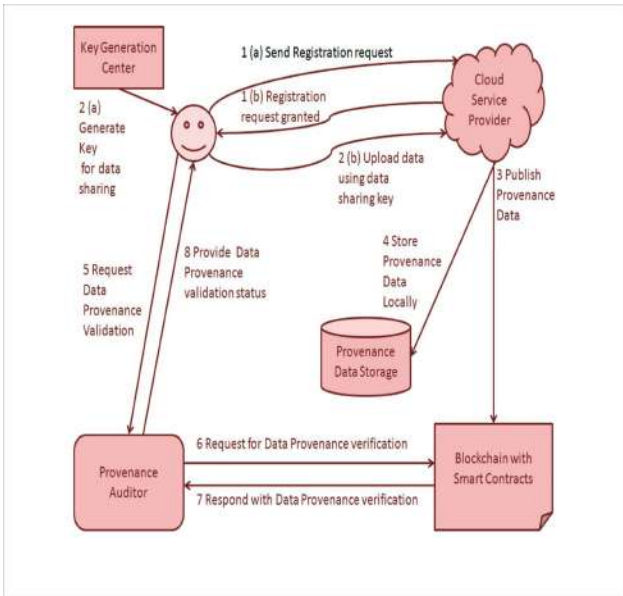
research studies is not yet evaluated as an IT security infrastructure for securing IIoT devices in cloud manufacturing. This requires modeling the solution and simulating it in a modeling and simulation tool capable of simulating application in a computer network. For this purpose, OPNET was selected for this research. The next section presents how the methodology of this research was executed.

V. METHODOLOGY

The secure origin-based smart contracting architecture presented in Figure 3 and the PrivChain architecture

International Journal of Multidisciplinary Engineering in Current Research
ISSN: 2456-4265, Volume 6, Issue 7, July 2021, http://ijmec.com/

presented in Figure 4 are defined for theoretical representation. This research presents a design of a practical scenario in which, the origin distributed ledger is integrated between two countries: UAE and India. The supplies from India consumed at UAE and vice versa are validated through a common distributed ledger having a joint authority between the two nations as the common origin data owner. Origin data can be created at the time of preparing an IIoT to be connected with the supply chain network. In this design the data is proposed to be stored in a distributed ledger having multiple server nodes. The server nodes may be deployed on cloud computing with local administrators at UAE and India. However, the origin data is proposed to be owned by a joint authority having centralized power to approve or reject activation of an IIoT to the supply chain network. The design proposed is outlined in Figure 5. The users of this design are connected with the cloud of cloud manufacturing apps (or simply cloud manufacturing: CM). The main service providers to this cloud are connected with the IIoT cloud (physical asset owners of manufacturing plants, logistics, and supply chains). The other clouds are proposed to facilitate reliable handshake between the CM users and the IIoT cloud providers.



The firewall cloud is the main gateway to process all origin validation requests. Whenever an IIoT device is added to the IIoT cloud or an existing IIoT device is prepared to be used by the CM users, it is programmed with several origin identifiers. The origin identifiers are stored in the origin distributed ledger (PBC) cloud through one of its processors. The authority controlling the origin data are connected with the origin data owner's (PDO) cloud.

The algorithm sequence designed for the proposed modified version of PrivChain and the secure origin-based smart contracting architecture is explained as the following:

a) Application starts–a CM cloud member requests an IIoT to jointhe cloud;
b) IIoT to Industrial Monitor–The IIoT makes a request for providing a valid session key for connecting to the CM cloud:
c) Industrial Monitor to IIoT (in three interactions)–The IndustrialMonitor randomly selects any three mandatory attributes (fromthe list of mandatory attributes approved by the origin Data Owner) and requests the IIoT to provide them serially in three interactions:
d) IIoT to Industrial Monitor (in three interactions)–The IIoT responds to the Industrial Monitor with the three requested attributes serially in three interactions:
e) Industrial Monitor to Distributed ledger Firewall–The Industrial Monitor requests the Distributed ledger Firewall to provide the session key for an IIoT device that reported the attached mandatory attributes (to be encapsulated within the request packet).Distributed ledger Firewall to origin distributed ledger cloud–After receiving the request from the Industrial Monitor attached with the mandatory attributes encapsulated in a packet, the Firewall shall locate one of the accessible distributed ledger members of the origin distributed ledger cloud (PBC) and forward the request.
f) Origin distributed ledger cloud member to origin data

International Journal of Multidisciplinary Engineering in Current Research
ISSN: 2456-4265, Volume 6, Issue 7, July 2021, http://ijmec.com/

owner: The PBC member can recognize the three attributes forwarded by the distributed ledger firewall because all the attributes assigned to any IIoT are stored in the PBC. However, the PBC does not have the valid session keys needed to connect the IIoT with the CM cloud. Hence, the PBC member forwards the request to the origin data owner (PDO). However, this request does not comprise of the three attributes as the PDO need not know about them. The PDO may only seek a Boolean state confirming if the process of validating attributes was completed. In fact, there is no need to forward a non- validated request to the PDO as the PBC can reject the request if validation is failed. A Boolean may be needed to ensure that the final rejection comes from the PDO such that it can track the requests registered. This research has defined the PDO as a combination of authorities from UAE and Indian governments. Hence, the need for tracking has been enabled.

g) Origin data owner to origin distributed ledger cloud member–The PDO responds to the PBC with a valid Session key. It may be a 256 bits long hash key that can be used by an IIoT device for all future sessions till the key expires.

h) Origin distributed ledger cloud member to distributed ledger firewall–The PBC member forwards the key to the Distributed ledger Firewall.

i) Distributed ledger firewall to IIoT–The distributed ledger firewall provides the key to the IIoT (Cloud monitor had already assigned a temporary address to the IIoT and provided its detail to the Distributed ledger Firewall) and maintains a local cache entry of the key in an event if the IIoT might have lost it in future.

The above steps were configured inside a customer application flow in the OPNET's Application Characterization Engine (ACE). The full modeling and simulation report is presented in the next section.

VI. MODELING AND SIMULATION

The scenario modeled in OPNET is presented in Figure 6. The OPNET version used was academic and hence, the model has been kept simple focusing on investigating the algorithmic interactions defined in the previous section. In reality, the model would be a complex cloud computing infrastructure quite difficult to realize in an academic network modeling software. In the model, the red lines indicate 10 Mbps Internet connections to a centralized Distributed ledger Switch. The Distributed ledger switch may be a cloud-based virtual switching hub accessible to IIoT devices through Internet. It may be a complex Application Programmable Interface (API) server used for accepting and processing machine-to-machine calls for authentication and authorization, and also to connect to the application servers. The actual realization of this networking shall be much more complex and is out of scope of this research. This research established 10 Mbps Ethernet transceiver connections to the Distributed ledger Switch and each IIoT devices getting an average throughput of 5 Mbps (to simulate a realistic Internet for field IIoT devices). In this scenario, eight IIoT devices are lined up to be authorized and assigned session keys such that they can establish production connectivity with the CM cloud. Without the production connectivity, they are merely network layer client devices assigned temporary connections without any application access.

The model comprises of the following components:

BC_SW: Distributed ledger switch allowing data connections to the Industrial Internet of Things (IIoT) devices communicating over the Internet;

FWn: One of members of the distributed ledger firewall cloud;

CMm: One of the members of the cloud of cloud manufacturing applications that is requesting session access tokens for eight IIoT devices;

International Journal of Multidisciplinary Engineering in Current Research
ISSN: 2456-4265, Volume 6, Issue 7, July 2021, http://ijmec.com/

IMm: One of the members of the industrial monitoring cloud; this may be private cloud owned by a consortium of industries in a country or region; The cloud manufacturing cloud is a subscriber to this cloud and expects it to provide access to only validated IIoT devices deployed by individual manufacturers;

PBCm: One of the members of the origin block chain cloud that holds origin data of all the IIoT devices deployed and configured by individual manufacturers;

PDOm: One of the members of the origin data owners that owns the origin data captured and provides valid session hashkeys for the IIoT devices recording their origin data on the PBC; The PDO members also provide access to the hash keys to the CM cloud members such that each validated IIoT member can be authenticated by them;

BC_Algorithm: The algorithm configuration and controller utility built on OPNET ACE that operates all the steps and interactions of this design;

BC_Profile: The profile configuration utility that is used to package all the interactions of the algorithm as a reusable resource (similar to the application packages used in application design);

BC_Application: The application runtime used for running the application on the network designed (one may visualize it as an EXE or JAR file used for running the application); IIoTn_0 to IIoTn (eight devices): The eight IIoT devices waiting to be validated in the scenario modeled; Figure 7 shows the implementation of the steps in the algorithm in the OPNET ACE. The steps are called "Phases" in OPNET. In every phase, the source and destination classes need to be defined. Every class is later mapped with the actual physical components of the model design. The interactions between the source and destination classes in the algorithmic sequence designed in the previous section are defined as phases, which are sequenced using the "Start Phase After" column. The source to destination and the destination to source traffic is defined based on the design of exchanges. In this algorithm, the exchange of a request and response is sized as 1,024 Bytes (1 KB) and the attributes exchange is sized as 1,024 Bytes (1 KB), as well. The simulation was executed for 8,000 s (about 2 h and 22 s). The reports were generated for each phase in the algorithm separately and also of the entire custom application runtime as a package. This research did not use any industrial benchmarks for performance evaluation. Hence, analysis of detailed response times and amount of data exchanged has been avoided. The main emphasis has been given on the behavioral evidences in the simulation results. The first result analyzed in this context is the TCP congestion view (Figure 8). It is a rarely discussed parameter in network studies, but holds an important value in this research. TCP congestion window is not merely a parameter but is a behavioral reflection of TCP sessions. It follows the IETF 1981 standard for Transmission Control Protocol (Medhi and Ramasamy, 2018).

In a congestion window, a transmitter breaks a packet into small segments, which are transmitted one by one in a connection-oriented mode (next segment transmitted only after receiving acknowledgement of the previous segment) to the receiver (Medhi and Ramasamy, 2018). The receiver reassembles the segments using the sequence numbering of each segment. The size of the segments is calculated automatically by the transmitter based on information about the available throughput to the receiver. As throughput is a stochastic variable, the size of segments also is stochastic.

Figure 8 shows the congestion window behaviors by seven IIoT devices and the rest of components on the cloud. OPNET generates hundreds of TCP connections and hence, this figure shows only one sample each for each of the device. The size of segments is varying from 3,000 to 6,000 bytes for sampled TCP connections of the transmitting devices throughout the simulation period. The transmission may be longer than the session length needed for the algorithmic connections because of the Ethernet keep-alive packets flowing apart from the packets containing the data. This observation indicates the behavior of TCP

International Journal of Multidisciplinary Engineering in Current Research
ISSN: 2456-4265, Volume 6, Issue 7, July 2021, http://ijmec.com/

congestion windows generated by transmitting devices. Keeping this observation in context, a real world scenario having link bandwidth fluctuations may return longer TCP congestion windows with segment sizes much lesser than the lowest value of this sample: 3,000 bytes. In this research, one IIoT (IIoTn) was assigned a higher QoS guarantee whereas others were left at the default state. As explained above, the IIoT devices were connected to the cloud switch at 10 Mbps with an average IP processing throughput of 5 Mbps. The result in Figure 8 shows its effect as IIoT devices not only faced the shortest segment sizes (3,000 bytes) but also shorter TCP congestion windows. This observation has a significant practical implication, as revealed from the next three statistics and the critical analysis in the next section. Figure 9 shows the TCP delays experienced by the Industrial Monitoring Distributed ledger, which is the main role player in the algorithm (takes all requests, forwards to origin Distributed ledger cloud and finally provides the received session keys to the IIoT devices for connecting with the Cloud manufacturing cloud).

VII. CRITICAL ANALYSIS OF IMPLICATIONS FOR THEORY AND PRACTICE

The findings of this research are analyzed in the context of the packaged food industry of Western India supplying to consumers in the UAE. The packaged food industry in India may be governed by the regulations of the Government of India. However, this research has shown how a layer of origin security can be implemented and controlled for all the packaged food companies in India to counter the risks of counterfeits or harmful products sneaking into the supply chain. The controls projected in this research can ensure that every existing and new IIoT device used for controlling the ground processes in packaged food supply chains shall be authenticated and validated by distributed ledger authorities.

To visualize the concept of monitoring and control by distributed ledger authorities, the theory of "virtual perception layer with cognitive abilities" of the physical layer of manufacturing plants is revisited here (Aileni et al., 2020; Tiwari and Khan, 2020). The virtual perception layer is also referred to as "neural network of manufacturing systems" (Ojha et al., 2021). The solution demonstrated in this research through simulation is possible only when the "virtual perception" or the "neural network" is in place forming an industry wide consciousness through specially designed communications and collaborations protocols (Ojha et al., 2021) such as the MQTT protocol described in Section 3 for machine-to-machine communications (Hintaw et al., 2019; Hintaw et al., 2023). MQTT has been reviewed in detail in Section 3 because of its industry-wide acceptance as the standard machine-to-machine communication protocol (Hintaw et al., 2019; Hastings et al., 2020; Shilpa et al., 2022; Hintaw et al., 2023). Several open source and commercial MQTT broker software packages are now available, such as Mosquitto, EMQX, ActiveMQ, HiveMQ CE, RabbitMQ, and VerneMQ (Hintaw et al., 2019; Mishra and Kertesz, 2020; Hintaw et al., 2023). All MQTT broker software packages offer SSL and TLS encryption but several IIoT devices are ready with them at their firmware levels (Hintaw et al., 2019; Hintaw et al., 2023). Hence, SSL and TLS encryption may be optional in many installations leading to clear text transmission of device credentials thus making the network vulnerable to counterfeit IIoT devices.

The solution designed and demonstrated in this research works on the foundation of cryptography enablement in all the IIoT devices. This means that all the IIoT devices not supporting cryptography are to be eliminated in this solution. This may be a major change but may ensure better IIoT security in the packaged food supply networks between India and UAE. This will also enable the validation, control and monitoring protocol introduced in this research. MQTT protocol supports SSL and TLS in basic implementation. They can be useful in preventing masquerading attacks on running

International Journal of Multidisciplinary Engineering in Current Research
ISSN: 2456-4265, Volume 6, Issue 7, July 2021, http://ijmec.com/

sessions. However, they do not ensure authentication of all the IIoT devices. Hence, the additional layer of origin security and assignment of cryptographic keys for origin authentication is essential, especially in protecting a critical supply chain network such as international food supply chains. This layer needs a governance cloud network. This research presented an example configuration of the cloud network between India and UAE. The Industrial Firewalls may be deployed in both the countries with secured peering overlooked by the Industrial Monitoring distributed ledger operated by authorities at both the nations. The origin distributed ledger may comprise of every authorized supply chain member interested in plugging an authorized IIoT to the network. The origin Data Owner may comprise of a registrar of every authorized manufacturer of IIoT devices in India and UAE.

The time taken in origin authorization and assignment of keys and the stochastic TCP window sizes are two concerns observed in this research. IIoT devices cannot be assigned priority quality of service queuing given their volumes. This means that there will be no control on TCP windows sizes. However, other actors on the cloud network require quality of service guarantees. This strategy has been demonstrated in Figure 8. All IIoT devices except IIoTn do not have any QoS guarantees thus facing stochastic variation in the TCP window lengths. However, TCP windows of all other actors have been assigned equal sizes surviving the entire simulation period. This strategy is essential to ensure that any volume of requests for the session key can be processed within an acceptable time period. In practice, India and UAE will need a dedicated self-hosted It infrastructure and network for operating their quality of service guarantees.

The limitation of this study is that it has attempted to design and
simulate a network in an academic environment, which may take a massive size if implemented in reality for corporate applications. Hence, the performance and behavioral statistics should be followed for making academic estimations and not be used as benchmark referencing. The challenges reflected from the simulation may be valid in the real world environment as well but the scales may be much larger than shown in the simulations. The simulations were conducted in a powerful laptop but better hardware will be needed for future studies. The banking integration (similar to the origin flow by Malik et al., 2022) was kept out of the design because of this limitation. However, in practice it is expected to be an essential component integrated with the origin distributed ledger.

Future studies may attempt to conduct the simulations on large hardware pools (preferably virtualized) to get more practical insight closer to the expected performance and behavior. The future studies may also simulate banking integration to see how payment gateways can perform parallel to the origin distributed ledger architecture.

VIII. CONCLUSION

IIoT and its rapid evolvement with cloud computing integration have caused integration of information and flow of controls among production, logistics, and supply chain engineering systems. However, rogue IIoT devices are recognized as threats to physical industrial environments as they can be used by malicious elements to cause industrial accidents. In food supply chains, risks of counterfeit harmful products getting mixed with genuine products in a supply chain are recognized. As IIoT devices are used to automate several processes in the supply chains, they need to be recognized, authenticated, authorized, and accounted ensuring that no counterfeit gets online connectivity within the system. The mechanism of origin distributed ledger has gained significant research interest to solve this problem. This research has explored the architecture of origin distributed ledger between two countries: India and UAE. The architecture has been conceptualized with the help of recent literature and modeled in OPNET Modeler to simulate its operations and make performance and behavioral observations.

These observations provided some useful results beneficial for practical realization of the origin distributed ledger network between the two countries. First of all, the two countries needto collaborate for creating common distributed ledgers for cloud monitoring, peering of industrial firewalls, origin control, and registration of origin data owners. Thereafter, the mechanisms for making requests for IIoT device registration and assignment of cryptographic access keys as designed in the algorithm should be established. Network simulations showed challenges related to TCP congestions and waiting time for assignment of keys. Hence, in its current form this architecture may be useful for one time authentication of IIoT devices only. In future, repeated authentication may have to be conducted during the lifetimes of the IIoT devices in the system. Repeated architecture will require more robust ICT clouds ensuring guaranteed quality of service for every IIoT device.

References

[1] Cao, Y.; Wu, Z.; Liu, T.; Gao, Z.; Yang, J. Multivariate process capability evaluation of cloud manufacturing resource based on intuitionistic fuzzy set. Int. J. Adv. Manuf. Technol. 2016, 84, 227–237. [CrossRef]

[2] Fu, J. A practical resource-searching method for manufacturing grid. Int. J. Adv. Manuf. Technol. 2014, 74, 335–340. [CrossRef]

[3] Hu, Y.J.; Chang, X.F.; Wang, Y.; Wang, Z.L.; Shi, C.; Wu, L.Z. Cloud manufacturing resources fuzzy classification based on genetic simulated annealing algorithm. Mater. Manuf. Process. 2017, 32, 1109–1115. [CrossRef]

[4] Dr. Bhargav Gangadhara, "Optimize utility in cloud-Based manufacturing systems using service models and development models", Presented and published at International Journal of Innovative Research in Advanced Engineering.IJIRAE Editorial Board, August 11 - 12, 2016.

[5] Li, B.H.; Zhang, L.; Wang, S.L.; Tao, F.; Cao, J.W.; Jiang, X.D.; Song, X.; Chai, X.D. Cloud manufacturing: A new service-oriented networked manufacturing model. Comput. Integr. Manuf. Syst. 2010, 16, 1–7. (In Chinese) [CrossRef]

[6] Dr. Bhargav Gangadhara, "Optimize Utility in Computing-Based Manufacturing Systems Using Service Models and Development Models", Presented and published at International Journal of Computer Science and Information Security, IJCSIS Editorial Board, Vol -14, Page 5 , 2016.

[7] Zhang, L.; Luo, Y.L.; Tao, F.; Ren, L.; Guo, H. Key technologies for the construction of manufacturing cloud. Comput. Integr. Manuf. Syst. 2010, 16, 2510–2520. (In Chinese) [CrossRef]

[8] Tao, F.; Li, C.; Liao, T.W.; Laili, Y. BGM-BLA: A New Algorithm for Dynamic Migration of Virtual Machines in Cloud Computing. IEEE Trans. Serv. Comput. 2016, 9, 910–925. [CrossRef]

[9] Zhou, J.; Wang, M. Cloud Manufacturing Service Paradigm for Group Manufacturing Companies. Adv. Mech. Eng. 2014, 6, 740725. [CrossRef].

[10] Tasgetiren, M.F.; Pan, Q.K. A discrete artificial bee colony algorithm for the total flowtime minimization in permutation flow shops. Inf. Sci. 2011, 181, 3459–3475. [CrossRef]