Adaptive Cyber Security Performance in Manufacturing Execution System

Vivekraj M[1] and Thirumalai R[2]

[1] *Program Manager, Faurecia Interior Systems India Pvt Ltd,*

Research Scholar, Anna University, Tamil Nadu, India.
[2] *Department of Mechanical Engineering, Dr. N.G.P. Institute of Technology, Anna University,*
Coimbatore, 641048, Tamil Nadu, India

[1] *vivekrajmannayee@gmail.com,* [2] *vkrthirumalai@gmail.com*

Abstract

The Manufacturing Execution System environment provides the potentiality to collect and communicate real-time data within the plant floor manufacturing execution systems, thereby achieving dynamic data collection and optimization and control of production operation management. This helps to develop a more intelligent manufacturing execution system with higher flexibility and visibility plant floor area. By extending Industrial Internet of Things technologies based robotic cell to manufacture field. Manufacturing Execution System is a key element of the broader thrust towards Industry 4.0, and trusts on the formation of a bridge between Industrial system and Robotic system environments through Industrial Internet of Things (IIoT) tools, coupled with enhancements to those plant floor systems through greater use of cloud manufacturing systems. Whilst these advanced tools have been in progress for some time, their integration with industrial systems and plant floor systems leads to new challenges as well as potential benefits and security threats. In this paper proposes and develops secure communication an overall architecture and solution for Robot security systems.

Graphical Abstract

Keywords: *Industry 4.0, Cyber Physical Systems, Cyber Physical System Security, Cryptography, Adaptive Security Performance.*

1. Introduction

Smart industries are changing their activities inside and over their flat collaborators by receiving Industrial Internet of Things, Edge computing, Cloud Manufacturing, Artificial Intelligence, Manufacturing Automation, Manufacturing execution system, variant management and Big data analytics. The outcome is an exceptionally associated 'Cyber physical' manufacturing execution system, named Industry 4.0 that will expand productivity and consumer loyalty. Not exclusively does Industry 4.0 guarantee to change the client experience, it will likewise improve creation (Ahmad et al., 2019, Vincent et al., 2015, Wu et al., 2019 and Ji et al., 2019). Smart industries, AI will drive process enhancement and issue remedy through distributed participation and the peer-to-peer of gadgets at the smart industry edge. This new 'shrewd activities' condition will interface everything- - human administrators, mechanical production system robots, electrical keen meters, stockrooms and conveyance trucks - to everything else. By coordinating sensor-based, correspondence empowered frameworks at the smart industry edge, Industry 4.0 vows to convey all the more rapidly, deftly and inexpensively the exceptionally modified, items and administrations that clients need (Babiceanu et al., 2017 and Taylor et al., 2019). In any case, there are inborn security hazards in systems administration and incorporating these new innovations over the operational environment. To understand the guarantee of Industry 4.0, security should be woven into this self-governing, any-to-any, edge-substantial eco- system. The security layer of this texture should be as disseminated, repetitive, adaptable and versatile as the frameworks it is entrusted to guard. Current concentrated security frameworks just aren't intended to deal with the extension, nature or intricacy of the Industry 4.0 operating system. The dangers of depending on conventional security models are extraordinary. While the expenses of these prominent cyber-attacks have been tremendous, an assault on an Industry 4.0 smart industry (Hughes et al., 2017 and Zarco et al., 2019). A cyber-security framework that ensures confirmation and data trade is the fundamental prerequisite of Industry 4.0. Huge numbers of the present innovations, ideas and conventions utilized in customary venture security originate before Industry 4.0. These security arrangements are overseen by focal IT offices that are answerable for keeping up firewalls and verifying each individual, application, and gadget that gets to them. Be that as it may, the intruders aren't leaving (Stock and Schel ., 2019 and Komend et al., 2019). In this paper incorporates adaptive security innovation, which carefully fulfills the difficult security condition of Industry 4.0. By implementing changeless records and appropriating and sharing indistinguishable security information over the hubs in its system, adaptive security is carefully designed and performance also investigated, repetitive and self-recuperating. Through a procedure of ceaseless compromise, agreement between gadgets makes sure about the system when new or irregularly associated gadgets go along with it. Through the adaptive security, gadgets set up agreement to distinguish and segregate awful gadgets and applications. This adaptive security ability conveys the information, honesty and excesses that Industry 4.0 requirement to flourish.

2. Related Work

Cyber-physical system as the name implies, affects the physical components of the system and go beyond just intellectual property theft. Cyber-attacks in manufacturing could also go beyond accessing the system for the sake of intellectual property theft and could alternatively affect the physical component itself within the production environment (Ahmad E et al., 2019). The edge manufacturing execution system

analytics, data routing components and hyper ledger services are already available as open source software components. The indicated platform design is a work in progress and the implementation provides a basis for further research and experimentation on edge computing and blockchains for digital automation in the industry, while at the same time improving relevant implementations (Vincent et al., 2015). An aware correlation technique based totally on temporal and attribute-based totally similarity analyses are done. In this evaluation test has been finished with a CMS safety tested. SQL injection and Nmap scanning device are used for cyber – assaults and interferences; CNC milling and heat- treatment strategies are followed as bodily assault targets (Wu et al., 2019). The evolutionary footprint of smart manufacturing is used from the perspective of HCPSs, and the implications, features, technical frame, and key technologies of HCPSs for new-generation intelligent manufacturing (NGIM). Finally, a result of the major encounters of HCPSs for NGIM is planned (Ji et al., 2019). A simulation-based totally model is used to get entry to the repercussions on production execution gadget presentation underneath the possible presence of cyber-threats. The effect of cyber-attacks on production bodily operation may be condensed through different safety guidelines inclusive of growing capacity of assets on the plant ground and making use of more traditional reorder techniques for sure situation (Bracho et al., 2018). The layout of a cloud-based totally cyber-bodily framework for 3D printing contexts is used alongside the advent of a 3-D Shape Modification App runs on the Android platform. There is a need to layout and expand person friendly ‘apps’ that will permit engineers and non-engineers to create target designs using form modification strategies and then ultimately manufacture execution system (Cecil et al., 2019). The opportunities concerning industrial network safety and secure identity for Cyber-Physical Production System (CPPS). OS fingerprinting, bio-metrical respectively hyper metrical strategies and self-descriptive skills of CPPS components, To construct a hybrid fingerprint for CPPS, to increase protection and construct a secure identification for CPPS (Stock and Schel.,2019). A cyber-physical system vulnerability effect analysis using decision trees, then offers the manufacturing execution system with a stoplight scale between low, medium, and high stages of cyber- physical system vulnerability for each analyzed production execution process. The stoplight scale allows a manufacturing execution system to interpret assessment effects in an intuitive way (Smit et al., 2016). The trustworthiness answers are used for integrated manufacturing execution system with cyber physical worlds, where trustworthiness is utilized in complement device dependability supplies with cyber security necessities, such that the resulting production cyber-physical gadget promises services that could justifiably be trusted (Smit et al., 2016). The integration of complex smart production technology massively increases the scope for an assault from adversaries aiming at business espionage and sabotage, the potential outcome of these attacks tiers from financial damage and misplaced production. These demanding situations are faced by those who wishing to secure smart manufacturing execution systems (Tuptuk and Hailes ., 2018). The Robot Operating System and the Point cloud library to process statistics from 3-d cameras monitoring the workspace and phase the human from the registered point clouds of the robot. While the human hand position is monitored through a local positioning gadget the use of ultrasonic sensors, the robot motion records are received from the robot controller (Komend et al., 2019). The IoT an AI which came due to the extensive distribution and usage of computer systems and the Internet will be known as the 1/3 revolution and subsequently, technological advances led to the connectivity among things and connecting amongst people, things, spaces. Currently, beyond the IoT and IoE, the hyperlinked society in which 'the actual world and cyberspace are linked and

intelligentization becomes possible is expected to be found out gradually. In order to apply CPS era to manufacturing system, it's far ore important to set the course of IoT implementation that can be connected with CPS and to expand and fortify the IoT infrastructure(Kim, and Park., 2017). Blockchain has turned out to be one of the most frequently discussed techniques for securing records storage and transfer through decentralized, trustless peer-to-peer systems. This study identifies peer-reviewed literature that seeks to utilize blockchain for cyber protection purposes and affords a systematic evaluation of the most frequently followed blockchain security applications (Taylor et al., 2019). The charges include industrial network security spending, the impact of unfavorable cyber events, and opportunities foregone if the era is underutilized. Authors has surveyed a lot of the present literature and records on the advantages and fees of ICT and their variant throughout time and countries. Observed that, in general, the greatest advantages of ICT come from its compounding contributions to boom and productivity across all sectors of the economy, similar to earlier general-purpose technologies like power production, at the same time as the greatest costs are those related to a hit unfavorable cyber event (Hughes et al., 2017). Modular cyber-physical robot, which in turn, considered a module and, therefore, a demonstrator of the fractal factory. "Based on the demonstrator of a cyber-bodily robot, the necessities for the modelling of an ultra-flexible and adaptable CPS have been determined. They also examined the requirements of encryption & description of the useful unit and the consumer interface definition have been advanced for the IFF Robot (Zarco et al., 2019).

3. IIOT shakes up plant floors

Industrial internet of things is connecting every stage of the manufacturing process, including end –to- end process system, IIot altering plant floor operations, and making plant floors infinitely more multifarious than before. Bringing to IIoT into a plant floor means deploying technology through connected devices, such as manufacturing execution system, scanners, RFID tags, and smart sensors. Manufacturing execution system is inclined to attack due to their inability to recognize, protect and retort to threats mechanism. Intruders get honor with the help of access point that allow them to damage the systems of the cyber physical device as well as pose security threats to IIot network, manufacturing execution system and Robotic cell, etc. The main idea of this paper explores about the manufacturing execution system and addressing issues in real time hacking problems towards industrial network. Moreover, in this paper address for formative how blockchain can improve the cybersecure manufacturing execution system.Manufacturing Execution System and Industrial Internet of Things both facilitate information sharing by connecting industrial facilities and business processing systems. This maximizes productivity, improves industrial visibility and minimizes bottleneck movements. Generally, the manufacturing execution systems are connected with Industrial controllers and microcontrollers that enable them to share data with the other facility's system and the control center. Industrial systems are well connected using either a network protocol, a Wi-Fi network system, or IEEE standard protocols for the purpose of transfer the information using a specific communications protocol.

4. Manufacturing execution system

Figure 1 demonstrates assembling an execution framework. This framework is firmly incorporated with substantial numbers and sorts of Programmable Logic Control frameworks that drive gathering forms this level of coordination can't be successfully be

obliged with current cloud advances. Further, producing execution framework accessibility in the present condition of distributed computing would convey the gathering framework procedure to a stop.

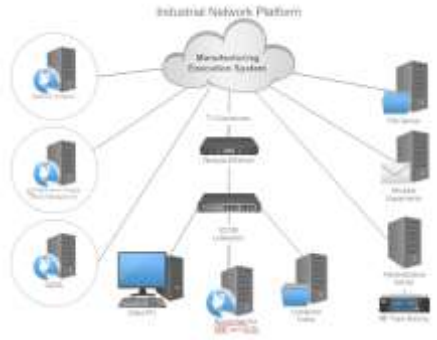

Fig. 1. Industrial Network System

Fig. 2. Manufacturing Execution System Setup

Most manufacturing organizations disconnect their industrial facility systems from their business arranges in order to not uncover their get together process control frameworks and manufacturing assets for the public clouds. The MES system that focused on mechanical programming and hardware is a case of such hazard. We can imagine an on-preface MES inter-operating with cloud-based applications. In fact, We think the truth for most assembling firms is that their endeavor IT engineering will be a half breed of on-commence and cloud-based applications. Intermediate documents are open from different gadgets like tablet, portability devices.

4.1 Manufacturing execution system experimental setup

Figure 2 demonstrates the exploratory setup for one of the cloud based get together the framework. In this get together station comprises of different stages like item sorting, and gathering forms that can be controlled by programmable logic controller. The upper and the lower transports are driven by the turning actuator 1 and the lower transport revolving actuator 2 separately. From the lot random selection choice of metallic pegs and plastic construct rings are put in light of the upper transport. The rings and pegs should be distinguished and isolated. This is finished by two nearness sensors, a closeness sensor1 and an infra-red intelligent sensor 2. By utilizing these two sensors a refinement can be made between the metallic and nonmetallic pegs and the ring. By method for the sort straight actuator by 3, plastic rings can be shot out/dismisses down the get together chute, which can have up to plastic rings. Metallic segment, then, proceed on the upper transport and are absconded down the feeder chute. The feeder chute naturally sustains latches onto the lower transport. An infrared sensor is utilized to figure out if or not the gathering range is stacked state of exhaustion. In the event that the condition is unfilled, the get together solenoid base rotational actuator is utilized to administer a ring from the get together channel into the gathering territory. The get together territory is situated quite recently over the lower transport and, when a metallic product passes, the latch draws in with the opening in the ring and the two parts are collected. The lower transport is utilized to convey finished parts into the accumulation plate. A printing module interfaced with the programmable logic controller, recovers information from the framework and print over the segment with applicable parameters, similar to make, permit no, bunch no, Mfg. Date, expiry date and so forth... In this work, a Siemens S7-300 programmable logic controller is utilized to control the procedure and programming called "Simatic Manager" is utilized to program the programmable logic controller. On MES based assembling floor have numerous MES based hardware. These

MES apparatuses create transitional records. These middle of the road archives created with the assistance of programmable rationale controllers. Be that as it may, these cloud based MES information are effectively hacked or changed by interlopers. With a specific end goal to ensure a sort of halfway archives by encryption calculations. Encryption calculations additionally select element nature, in addition, keeping in mind the end goal to expand open or private key verification too. The figures [3,4] indicates cloud based MES information.

4.2 The Manufacturing Network Simulation and Experimental Results and Analysis

There are a great number of network simulation tools that can be used in this paper, however, We had two primary criterion while we were selecting the optimal tool to use, they were: Flexibility and availability of descriptive and comprehensive resources for self learning and practical real world translation. We also considered the platform on which the tool would run, preferring windows above Linux and Mac OS as well as the availability of the resource open source being the most preferred. We thus Shortlisted 3 simulation software, they are being GNS3, NS3 and OMNET++. All of them were open source softwares however the 2 latter softwares had limited resources and lacked the flexibility and robustness we were looking for so we chose the GNS3 which is the graphical network simulator version 3.2.1.5. This tool specifically is an emulator i.e. instead of just simulating the network nodes, it actually emulates the real IOS binary files and images to provide a much more practical and real world scenario for the simulation and thus creates more authentic results. We used the Cisco C7200 router's IOS image and configured it with different routing protocols, and privilege levels providing varying levels of security.

4.3 The Manufacturing Execution System Network Topology

The basic network as of now consists of three C7200 routers connected to each other through Fast Ethernet connections which are the gateways to individual networks consisting of virtual machines connected to each other through an ethernet switch. Figure 3 shows the network topology employing manufacturing execution system. The various MES set up connected with network topology as shown fig. 3

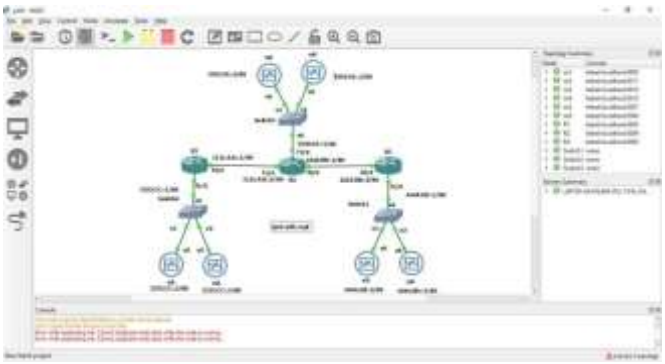

Fig. 3. The basic network topology employing IPV6 with OSPF routing

4.4 Enhanced Interior Gateway routing protocol

EIGRP (Enhanced Interior Gateway routing protocol) is a dynamic routing protocol, which automatically assigns the destinations in the routing table of the individual routers. This allows for easy and efficient routing as compared to protocols such as static routing

in which a network administrator must assign each of the IP routes individually. Furthermore, it provides additional security features by using dissimilar authentication passwords at different times. The following are the IP routes and standard ping round trip times for EIGRP routing protocol. Figure [4, 5] Pings sent and receive a pair of MES devices.

Fig. 4. Pings sent from 1.1.1.2 /24 to various other networks

Fig. 5. IP routes for router 1 in EIGRP network

4.5 Open Shortest Path First algorithm

OSPF is a shortest path first algorithm and routes data through the shortest path in a network that is determined through djiskstra's algorithm. Thus, it can be considered to be a dynamic routing protocol that determines the optimal route by calculating the cost of routing while using factors like bandwidth delay and load. This allows the network administrator to have an overview of the optimal routes. Figure [6,7] shows routing protocol in an open shortest path first algorithm and ping send from other MES network.

Fig. 6. The routing protocol in an OSPF network

Fig. 7. Ping sent from 33.33.33.5/24 to other networks

4.6 Routing Information Protocol

The router Information protocol is one of the earliest distance vector routing protocols. It uses the hop count, ie the changes in the network segments, as a routing metric. It creates efficient networks by limiting hop counts to prevent routing loops, however the maximum number of hop counts allowed is 15 this somewhat limits the size of the network. Figure [8, 9] shows routing information protocol and pings established other manufacturing execution system devices.

Fig. 8. The IP routes in a RIP routing network

Fig. 9. Pings sent from 1.1.1.2/24 to other networks

4.6.1 Static routing

Static routing is unlike dynamic routing and it involves the manual entry of the IP routes between different networks into the routing table. This makes the process of adding new nodes to the network tedious and time consuming. Figure 10 shows static routing and MES nodes pings. Static routing is usually used in combination with dynamic routing to provide a backup plan in case the dynamic routing fails. It's also used as a routing redistribution, i.e. to send information from one protocol to the other.

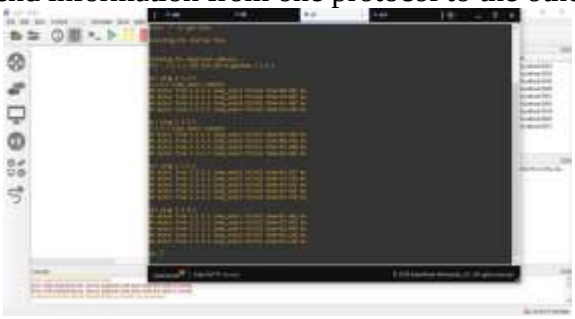

Fig. 10. Pings sent from 1.1.1.2/24 to other network nodes

4.7 Internet Protocol version 6

The IPv6 is the most recent version of the Internet of the protocol which provides the ability to identify and locate network nodes across the internet. It replaced IPv4, as it was realized that IPv4 simply didn't have the required address space needed to cope with the commercialization of the internet in 1998. It is an internet layer protocol that provides packet switched internet working which involves the transmission of data in specific bundles called packets having a header and a payload from one network host to the other. Figure [11, 12] shows pings status and password authentication for accessing the router console. Further the simulation in this case was made even more secure by using the maximum level of privilege in the Cisco C7200 router and enabling a service password encryption on the router. This provided an additional layer of security.

Fig. 11. Ping sent from 3333:CC::2/80 to other

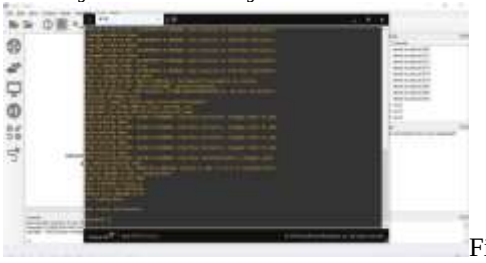

Fig. 12. The password authentication for accessing the router console

networks

4.8 Implementation of honeypot in manufacturing execution system

A honeypot emulatesa part of a network by creating a number of simulated ports. These in turn are used to lure an attack away from the actual system by tricking it to believe that the simulated port is the real system. There are two kinds of Honeypots; high interaction and low interaction. We have chosen a low interaction system as they are lightweight and highly flexible and are thereby ideal for use in the Machine to machine communication system. Figure [13-15] shows implementation of honeypot in smart manufacturing execution system. We have chosen two honeypot systems: the Honeybot and KF sensor, the former being an open source platform and the latter being a paid tool. Both the honeypots are low interaction and detect malicious scans and maintain logs of the attacks. An attack was simulated by using Filezilla and was recorded on both systems and an alert was sent out.

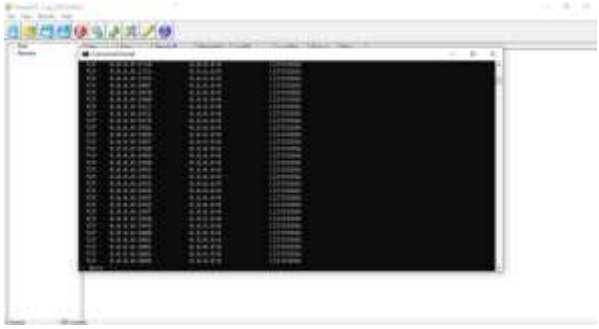

Fig. 13. The fake portsa as generated by Honeybot

The following images describe the logs recorded by the honeypot showing the data sent and received as well as the address of the scan the protocol used and in the case of KF sensor the relative severity is also displayed. This kind of a low interaction honeypot can be used in a manufacturing network by implementing it in the network host placed in the Demilitarized zone of the network thereby it intercepts attackers before they reach the inner network hosts.

Fig. 14. The scan log showing the details of the simulated attack in KF sensor

Fig. 15. The scan log showing the details of the simulated attack in Honeybot

4.9 Security in Manufacturing Execution Systems

Encryption refers to the use of a key or a system of keys to coding information so that only authorized parties who have access to the keys or a corresponding key can only access the information. We have chosen 2 sets of encryption algorithms for scrutiny to judge whether they can be used in the M2M communication field. They are:

4.9.1 Advanced Encryption Standard

The advanced encryption system is a highly secure symmetric encryption algorithm. They can be used for securing the communications between the machines as well securing the files stored in resource intensive network hosts. They work on a system of substitution permutation network that inputs a block of plain text and the keys, Then they make it undergo a series or layers of substitution and permutation boxes that are operations that scramble the input into the final ciphertext box. Fig 16 shows Simplified implementation of the AES encryption algorithm implementation of MES device environment. The main criteria for the AES algorithm was high speed and a low ram requirement, which it satisfied efficiently works extremely well in both high and low resource devices, even showing satisfactory results in 8-bit smart cards.

Fig.16. Simplified implementation of the AES encryption algorithm

Fig. 17. Simplified implementation of the RSA encryption algorithm

4.9.2 Rivest–Shamir–Adleman algorithm

The Rivest-Shamir Adleman algorithm is the most widely used asymmetric encryption algorithms. The RSA encryption algorithm uses two sets of keys, one private and one public. The public key is used by the transmitter of data to encrypt the data and the private key is used by the recipient. The algorithm works on the principle that it is very difficult to factorize a large prime number if its factors are known thereby, the encryption can be done by using the public key, but to find the private key by using the public key is a process that takes a very long time provided that a sufficiently large number is chosen. Figure 17 shows test result of the RSA encryption algorithm MES device. RSA can be employed on low processing devices, especially if the 1024 bit RSA algo is used and thereby is useful for application for securing machine to machine communication.

4.9.3 Veracrypt Using MES

Veracrypt is an open source encryption tool that allows us to create a virtually secure drive of arbitrary space. It uses a variety of Encryption algorithms, including AES. It can be used for the secure storage and transfer of sensitive data such as manufacturing process parameters, production data, Inventory locations and stock, files for firmware updates and other sensitive data. It can be easily be installed onto a resource intensive network host that acts as a central hub and a can securely record and store data.

4.9.4 Blockchain using Manufacturing Execution Systems

Blockchain is a chain of blocks which contains information / transactions. This is basically a data structure to ensure data integrity so that information will be protected and cannot be changed with permission. Each block has a unique digital fingerprint for blocks based on the previous blocks, hash / fingerprint, which implies that any change in a single block will affect other block's operation. We import block object as it is into

a new file for easy understanding. Genesis block is the first block in the blockchain. Figure [18-23] shows the blockchain implemnetation of machine to machine communication stages. The random arbitrary message in this genesis block The text implies transaction between the blocks We get unique hash/fingerprint even if we change an individual text If we change from genesis block also it will get a different hash. Note - In reality this will not be strings and it will be transaction objects. Figure [24 -25] shows M2M A .csv report sharing from an MES to MES device environment. CODE -1

Fig. 18 . Blockchain using M2M

Fig.19. Blockchain using M2M

Fig. 20. Blockchain using M2M

Fig. 21. Blockchain using M2M

When we change a character from the second block the following changes can be observed in the hash. Similarly, changing any block's data will give a different hash value.

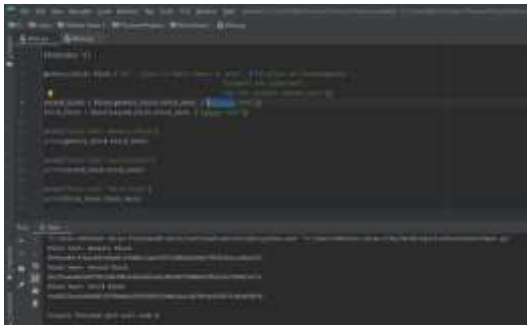

Fig. 22. Blockchain using M2M

Fig. 23. Blockchain using M2M

This is how we can get to know that someone has messed with a block. It shows the mechanism of data integrity.

4.11 Blockchain with implementation of Manufacturing Execution System

We use the time stamp to synchronize all the blockchains. The code contains two classes. This is storing strings as an example, in which each block has different hashes from genesis block to n number of blocks. In the case we have considered 10 blocks in total.

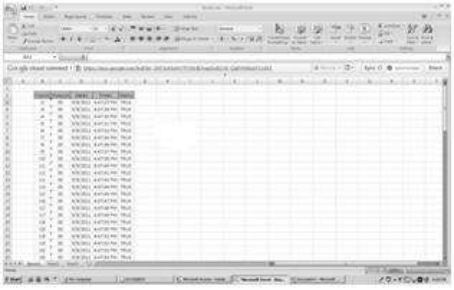

Fig. 24 Blockchain using M2M A report MES_01

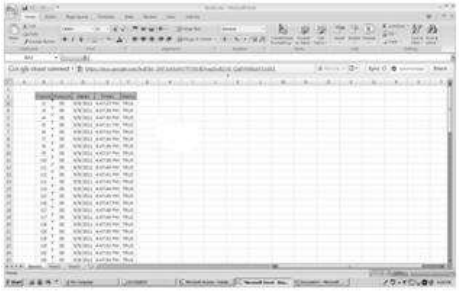

Fig. 25. Blockchain using M2M A report MES_02

4.12 Encryption selection methods for Securing meter data

In this paper work the kinds of existing encryption calculations and presents a relative examination on DES, AES, Blowfish, RSA and Hash capacities. These have been actualized on an assembling execution framework dataset which comprises of different hubs and server from where the master framework gets to the information. This information from the assembling execution framework is moved to the server, which put away in an encoded structure. The calculations are looked at based on execution time (Fig 26-30 shows An examination of DES, AES, Blowfish, RSA and HASH calculations VS Without encryption Average time to move a message digest). A calculation which requires low vitality and force is supported. Blowfish has almost 9.38 % decline in the estimation of intensity contrast with DES and AES algorithm.This is again a parameter to check the degree of security of a calculation. Blowfish calculation changes the plain content totally. Subsequently, it very well may be reasoned that blowfish calculation is secure and effective than the rest of the calculations for MES to MES communication purpose. Though significant level information hash calculation is secure and productive. (Table 1 shows time to transfer a message digest)

Table 1 Time to transfer a message digest

M	Location	Without Encryption (Avg. Time ms)	DES (Avg. Time ms)	AES (Avg. Time ms)	Blowfish (Avg. Time ms)	RSA (Avg. Time ms)	Hash (Avg.Time ms)
M1	2.2.2.2	26.821	491.09251	394.2687	251.58098	844.862	1134.53
M1	2.2.2.2	25.8333	473.00772	379.74951	242.316354	813.749	1092.75
M1	2.2.2.2	41.616	761.98896	611.7552	390.35808	1310.9	1760.36
M1	3.3.3.3	62.744	1148.8426	922.3368	588.53872	1976.44	2654.07
M1	3.3.3.3	58.745	1075.621	863.5515	551.0281	1850.47	2484.91
M1	3.3.3.3	64.439	1179.8781	947.2533	604.43782	2029.83	2725.77
M1	2.2.2.2	37.554	687.61374	552.0438	352.25652	1182.95	1588.53
M1	2.2.2.2	43.476	796.04556	639.0972	407.80488	1369.49	1839.03

M1	2.2.2.2	24.468	448.00908	359.6796	229.50984	770.742	1035
M1	2.2.2.2	34.598	633.48938	508.5906	324.52924	1089.84	1463.5
M1	2.2.2.2	36.57	669.5967	537.579	343.0266	1151.96	1546.91
M1	3.3.3.3	45.401	831.29231	667.3947	425.86138	1430.13	1920.46
M1	3.3.3.3	48.355	885.38005	710.8185	453.5699	1523.18	2045.42
M1	3.3.3.3	60.548	1108.6339	890.0556	567.94024	1907.26	2561.18
M1	3.3.3.3	55.517	1016.5163	816.0999	520.74946	1748.79	2348.37
M1	3.3.3.3	49.351	903.61681	725.4597	462.91238	1554.56	2087.55
M1	3.3.3.2	56.366	1032.0615	828.5802	528.71308	1775.53	2384.28
M1	3.3.3.2	57.376	1050.5546	843.4272	538.18688	1807.34	2427
M1	3.3.3.2	53.407	977.88217	785.0829	500.95766	1682.32	2259.12
M1	3.3.3.2	56.42	1033.0502	829.374	529.2196	1777.23	2386.57
M1	3.3.3.2	64.406	1179.2739	946.7682	604.12828	2028.79	2724.37
M1	3.3.3.2	61.785	1131.2834	908.2395	579.5433	1946.23	2613.51
M1	3.3.3.2	63.497	1162.6301	933.4059	595.60186	2000.16	2685.92
M1	1.1.1.2	0.001	0.01831	0.0147	0.00938	0.0315	0.0423
M1	1.1.1.2	0.001	0.01831	0.0147	0.00938	0.0315	0.0423
M1	1.1.1.2	0.001	0.01831	0.0147	0.00938	0.0315	0.0423
M1	1.1.1.2	0.001	0.01831	0.0147	0.00938	0.0315	0.0423
M1	1.1.1.2	0.001	0.01831	0.0147	0.00938	0.0315	0.0423
M1	1.1.1.2	0.001	0.01831	0.0147	0.00938	0.0315	0.0423
M1	4.4.4.2	40.668	744.63108	597.8196	381.46584	1281.04	1720.26
M1	4.4.4.2	40.451	740.65781	594.6297	379.43038	1274.21	1711.08
M1	4.4.4.2	37.448	685.67288	550.4856	351.26224	1179.61	1584.05
M1	4.4.4.2	38.516	705.22796	566.1852	361.28008	1213.25	1629.23
M1	4.4.4.2	42.467	777.57077	624.2649	398.34046	1337.71	1796.35
M1	11.11.11.1	34.489	631.49359	506.9883	323.50682	1086.4	1458.88
M1	11.11.11.1	44.422	813.36682	653.0034	416.67836	1399.29	1879.05
M1	11.11.11.1	35.486	649.74866	521.6442	332.85868	1117.81	1501.06
M1	11.11.11.1	41.454	759.02274	609.3738	388.83852	1305.8	1753.5
M1	11.11.11.1	34.375	629.40625	505.3125	322.4375	1082.81	1454.06
M1	11.11.11.1	36.395	666.39245	535.0065	341.3851	1146.44	1539.51
M1	11.11.11.1	35.606	651.94586	523.4082	333.98428	1121.59	1506.13
M1	11.11.11.1	38.481	704.58711	565.6707	360.95178	1212.15	1627.75
M1	11.11.11.1	34.555	632.70205	507.9585	324.1259	1088.48	1461.68
M1	22.22.22.4	37.326	683.43906	548.6922	350.11788	1175.77	1578.89
M1	22.22.22.4	41.46	759.1326	609.462	388.8948	1305.99	1753.76
M1	22.22.22.4	41.393	757.90583	608.4771	388.26634	1303.88	1750.92
M1	22.22.22.4	35.488	649.78528	521.6736	332.87744	1117.87	1501.14
M1	2.2.2.2	40.563	742.70853	596.2761	380.48094	1277.73	1715.81
M1	2.2.2.2	35.881	656.98111	527.4507	336.56378	1130.25	1517.77
M1	2.2.2.2	43.482	796.15542	639.1854	407.86116	1369.68	1839.29
M1	2.2.2.2	36.526	668.79106	536.9322	342.61388	1150.57	1545.05
M1	3.3..3.3	59.486	1089.1887	874.4442	557.97868	1873.81	2516.26

M1	3.3..3.3	60.334	1104.7155	886.9098	565.93292	1900.52	2552.13
M1	3.3..3.3	63.44	1161.5864	932.568	595.0672	1998.36	2683.51
M1	3.3..3.3	53.425	978.21175	785.3475	501.1265	1682.89	2259.88
M1	2.2.2.2	41.427	758.52837	608.9769	388.58526	1304.95	1752.36
M1	2.2.2.2	32.524	595.51444	478.1028	305.07512	1024.51	1375.77
M1	2.2.2.2	34.432	630.44992	506.1504	322.97216	1084.61	1456.47
M1	2.2.2.2	43.351	793.75681	637.2597	406.63238	1365.56	1833.75
M1	2.2.2.2	41.378	757.63118	608.2566	388.12564	1303.41	1750.29
M1	444:DD::2	58.286	1067.2167	856.8042	546.72268	1836.01	2465.5
M1	444:DD::2	63.4	1160.854	931.98	594.692	1997.1	2681.82
M1	444:DD::2	63.536	1163.3442	933.9792	595.96768	2001.38	2687.57
M1	444:DD::2	51.349	940.20019	754.8303	481.65362	1617.49	2172.06
M1	444:DD::2	65.447	1198.3346	962.0709	613.89286	2061.58	2768.41
M1	555:EE::2	62.374	1142.0679	916.8978	585.06812	1964.78	2638.42
M1	555:EE::2	42.429	776.87499	623.7063	397.98402	1336.51	1794.75
M1	555:EE::2	42.526	778.65106	625.1322	398.89388	1339.57	1798.85
M1	555:EE::2	41.534	760.48754	610.5498	389.58892	1308.32	1756.89
M1	555:EE::2	40.437	740.40147	594.4239	379.29906	1273.77	1710.49

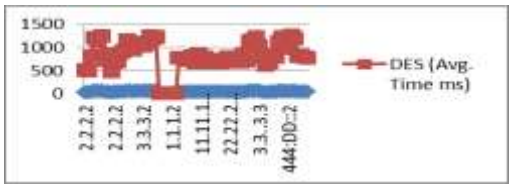

Fig. 26. A comparison of DES algorithms VS Without encryption Average time to transfer a message digest

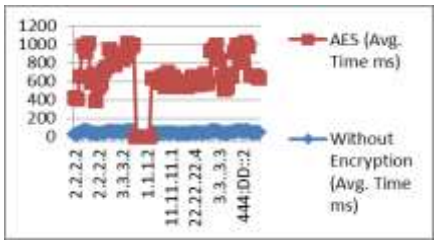

Fig. 27. A comparison of AES algorithms VS Without encryption Average time to transfer a message digest

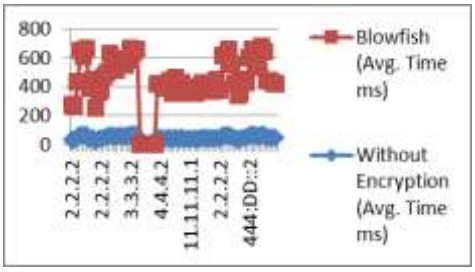

Fig. 28. A comparison of Blowfish algorithms VS Without encryption Average time to transfer a message digest

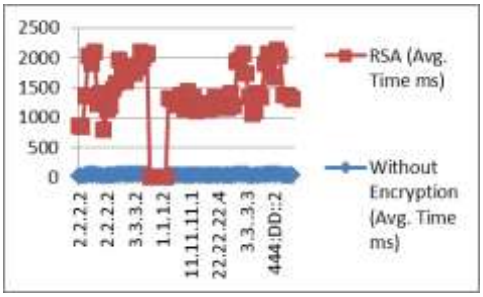

Fig. 29. A comparison of RSA algorithms VS Without encryption Average time to transfer a message digest

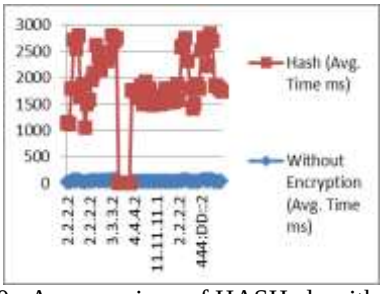

Fig. 30. A comparison of HASH algorithms VS Without encryption Average time to transfer a message digest

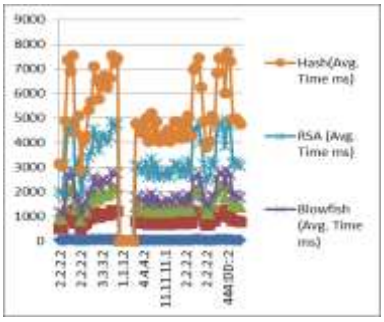

Fig 31. A comparison of DES, AES, Blowfish, RSA and HASH algorithms VS Without encryption Average time to transfer a message digest

5. Conclusion

The " blockchain mixed MES as administration" model for MES producing has risen with the ascent of the web advancements, in which, a specialist organization can give MES as a support of numerous customers over the Internet. Be that as it may, not at all like different administrations. Manufacturing Execution and mixed of Blockchain technology is still in its growing and its possible impact on the factory floor area is yet to be clearly understood. The integration of MES with the blockchain, especially robotics based automation and Industry 4.0, is still in an early infant stage. This means that many advancements and improvements are being realized on separate application blockchains. There is no rich 'implementation' technologies hitherto to develop, most of the OEM's participants are not aware of many of the novel technologies, and they sometimes lack implementation knowledge in the sturdiness of these proposals. Proposed strategies are ample, communication standards are missing, and the combination of these tactics with Industry 4.0 or MES based robotics, e.g., is so far to be achieved. In this paper, we overview of the existing methods and proposals for MES based block chain technologies that either use MES and robotics or leverage peer to peer services that can improve industrial network systems. As the block chain application is growing, it will interact with many other standards, such as robotics and machine learning and industrial Big data applications, to yield improved MES higher living standards for our automation world.

References

[1] *Ahmad, E. Elhabashy, and Lee J. Wells and Jamine A. Camelio, Cyber-Physical Security Research Efforts in Manufacturing - A literature Review," Procedia Manufacturing, vol. 34, No.1 (2019) pp.921–931.*

[2] *Alejandro Bracho, Can Saygin, HungDa Wan, Yooneun Lee and Alireza Zarreh, A Simulation-Based Platform for Assessing the Impact of Cyberthreats on Smart Manufacturing Systems." Procedia Manufacturing, vol. 26, No. 1(2018) pp. 1116–1127.*

[3] *Barry B. Hughes, David Bohl, Mohammod Irfan, Eli Margolese-Malin, and José R. Solórzano, ICT / Cyber Benefits and Costs: Reconciling Competing Perspectives on the Current and Future Balance." Technological Forecasting & Social Change, vol. 115, No. 1 (2017) pp. 117–130.*

[4] *Daniel Stock and Daniel Schel, Cyber-Physical Production System Fingerprinting, Procedia CIRP, vol. 81, No. 1, (2019) pp. 393–398.*

[5] *Hannah Vincent, Lee Wells, Pablo Tarazaga and Jaime Camelio, Trojan Detection and Side-Channel Analyses for Cyber-Security in Cyber-Physical Manufacturing Systems, Procedia Manufacturing, vol.1, (2015), pp.77–85.*

[6] *J. Cecil, P.Ramanathan, and H. Huynhc, A Shape Modification App and Cyber-Physical Framework for Collaborative Manufacturing." Procedia Manufacturing, vol. 34, No. 1 (2019), pp. 932–939.*

[7] *Zarco, Liliana & Siegert, Jörg & Bauernhansl, Thomas, Software Model Requirements Applied to a Cyber-Physical, Modular Robot in a Production Environment, Proceidia CIRP, vol. 81, No. 1 (2019), pp. 352–357.*

[8] *Mingtao Wu, and Young Moon, Alert Correlation for Cyber-Manufacturing Intrusion Detection." Procedia Manufacturing, Vol. 34, No. 1 (2019), pp. 820–831.*

[9] *Nilufer Tuptuk, and Stephen Hailes, Security of Smart Manufacturing Systems, Journal of Manufacturing Systems, vol. 47, No. 1(2018), pp. 93–106.*

[10] *Paul J.Taylor , TooskaDargahi, AliDehghantanha, Reza M.Parizi and Kim-Kwang Raymond Chood, A Systematic Literature Review of Blockchain Cyber Security, Digital Communications and Networks, (online), available from, (accessed on 19 February 2019)*

[11] *Radu F. Babiceanu, and Remzi Seker, Trustworthiness Requirements for Manufacturing Cyber-Physical Systems, Procedia Manufacturing, vol. 11, No. 1 (2017), pp. 973–981.*

[12] *SungHyun Kim, and Sungbum Park, CPS (Cyber Physical System) Based Manufacturing System Optimization, Procedia Computer Science, Vol. 122 (2017), pp. 518–524*

[13] *Titanilla Komenda, Gerhard Reisinger and Wilfried Sihn, A Practical Approach of Teaching Digitalization and Safety Strategies in Cyber-Physical Production Systems, Procedia Manufacturing, vol. 31, No. 1(2019), pp. 296–301.*

[14] *Zach DeSmit, Ahmad E. Elhabashy, Lee J. Wells and Jaime A. Camelio, Cyber-physical Vulnerability Assessment in Manufacturing Systems, vol. 5, No. 1(2016), pp. 1060–1074.*

[15] *Ji Zhou, Yanhong Zhou, Baicun Wang and Jiyuan Zang, Human–Cyber–Physical Systems (HCPSs) in the Context of New-Generation Intelligent Manufacturing, Engineering, vol. 5, No. 1 (2019), pp. 624–636.*