The management of information security in Industrial IoT systems

Hari Shankar kumar[1], Dr Shajahan Basheer[2,] Dr E.Rajesh[3],

[1]PG Scholar, School of Computing Science and Engineering, Galgotias University, Greater Noida, India.
[2,3]Professor, School of Computing Science and Engineering, Galgotias University-Greater Noida, India

Abstract—
With the aid of fundamental information protection techniques and tools, many methods of securing enterprise IIoT systems are demonstrated.
The potential applications of various structural variants, network technologies, and cryptographic techniques are illustrated.
The solutions provided in the article are used in a variety of ways.
The findings may be helpful to IIoT system designers and managers.
Keywords—Cloud computing, edge computing, information security , cryptographic protection, industrial internet of things, and device protection

I. INTRODUCTION

The Internet of Things (IoT) is used frequently when developing sophisticated systems for data collection,data processing, decision-making, and object management in a variety of human endeavours.

The industrial Internet of Things(IoT) is one of the key uses of Internet of Things technologies (IIoT). The manufacturing and process control equipment are the "things" in this context. Numerous publications gives study on the use of Industrial Internet of Things(IIoT) in various industries. But they mostly focus on the technical and software parts of this issue, ignoring its crucial aspect: the security of the commercial Internet of Things(IoT) [1, 2, 3, 4, 5].

II. THEPROBLEMDESCRIPTION

The following are the biggest risks when implementing the Internet of Things(IoT) in industrial application.

- • Unauthorized access to the data handled by the Internet of Things(IoT) results in the following effects.
  - falsification of actual information on how the machinery is being used and the business as a whole;
  - effect on the enterprise's and the equipment's operations;
  - device malfunctions brought on by data corruption or overflowing;
  - Unauthorised use of the company’s information for malevolent purposes;
- Unauthorized access to the data that governs how the business is run via the system of the devices of the
Internetofthings (IoT),which cause equipment to operate incorrectly , charges in how equipment interacts with one another and the production cycle as a whole, and the introduction of imperfect products;
- A negative effect on the Internet of Things(IoT) communication device system could cause equipment to interact incorrectly , lose production information, and even stop production process;
- Detrimental effect on the Internet of Things(IoT) system’s configuration , leading to modification I the functioning of the interacting equipment and unauthorized transfer of control functions to other system;

- misuse of Internet of Things(IoT) devices and its application to malicious system attacks;
- negative impact on the software of Internet of Things(IoT) devices, leading to effects like modifications to the equipment's operating modes, the emergence of defect in the performance of technological operations, the creation of delay in the equipment's interaction, and incorrect management decisions regarding the equipment's, the entire production system, as well as specific subsystems;
- Unintentional malfunction of the Internet of Things communication infrastructure and individual devices, together with external variables linked to equipment breakdown and the emergence of flaws in the executions of technological process;

If any of these threats are carried out, the firm will suffer financial and reputational consequences. It will require a lot of money and effort to update the Internet of Things system's architecture in order to eliminate the effects of these dangers.

Threat study reveals that in IIOT systems, data management and device access control frequently take precedence over actual ownership of the information the system processes.

The industrial Internet of things must have an acceptable level of security in order tominimise the risks brought on by these threats. Informational and operational security should both be offered concurrently.

Figure 1 displays the fundamental safeguards for the IIoT system's security.

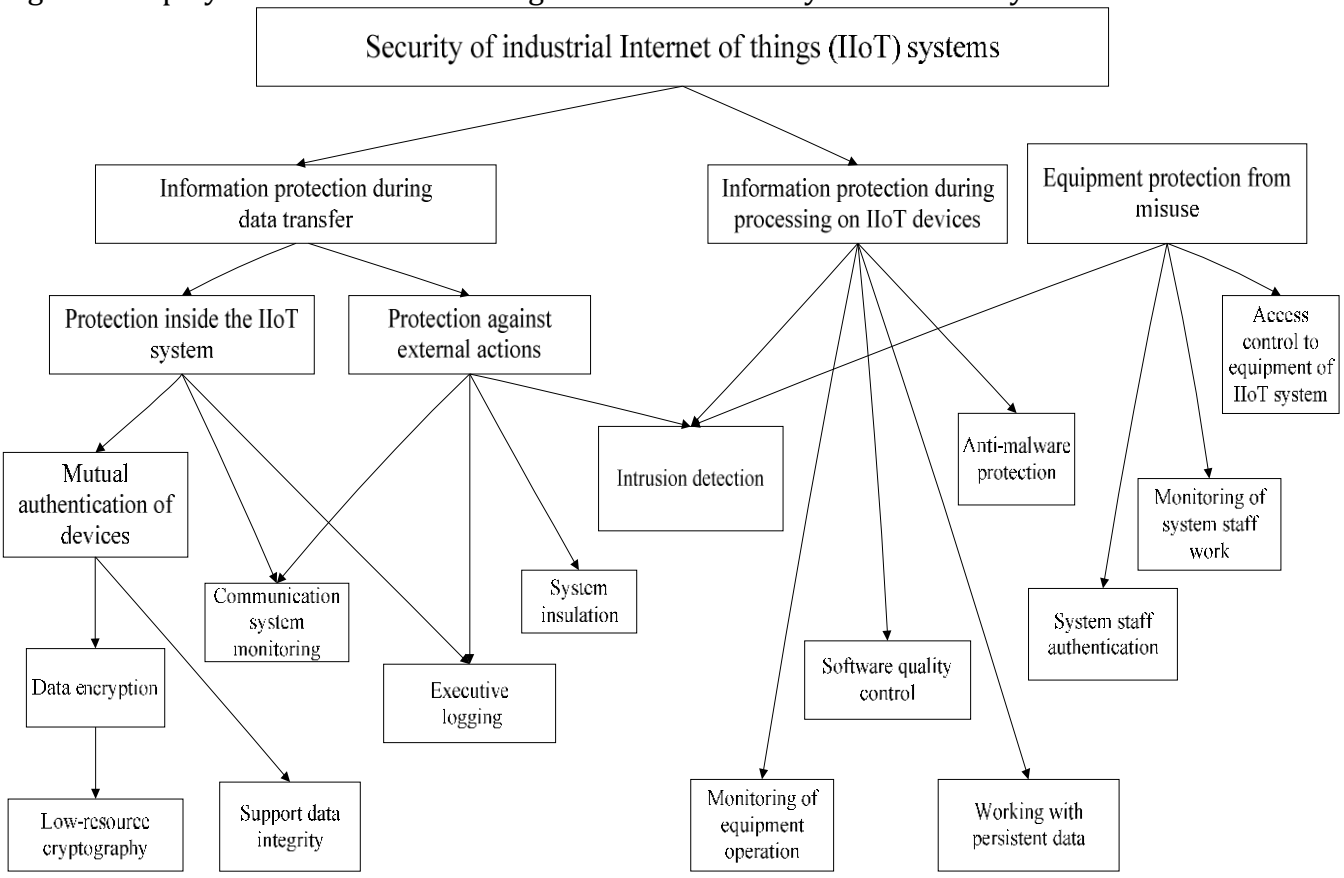

Figure.1.Basic security mechanisms of IoT systems

III. Like y Solution

1. We will then think about potential remedies to lessen the impact of these dangers. As seen in figure 1, all solutions may be broken down into those that deal with system structure development, communication organisation, information organisation for cryptographic protection, and device organisation for protection.

2. Using edge computing and cloud technologies

At the IoT World Forum (IWF), this strategy was presented as a reference model in 2014. Cloudgycomputing is becoming a key component of Internet of Things(IoT) system , which can be seen of as a potential replacemt for Fog computing[6,7,8]

IoT systems divide grouping of “things” into discrete , hazy network structure, where basic computations, data processing and storage are done.

Some of the system’s overall outputs are then sent to the cloud and made accessible to the other user groups. This strategy is well –suited to the organizational structure of many business, where production processes(units) that operate independently of one another and are only connected through the transfer of their production related outputs are distinguishable.

Edge computing is a more innovative method of organising auxiliary computing. In this scenario, IIoT devices attached to the "things" process data that is received from them rather than sending it to a higher level of processing. Each IIoT device only interacts with its respective "thing," and each "thing" with its respective "device."

Figure 2 depicts the Industrial IoT of things system's organisational structure with cloud and edge computing..

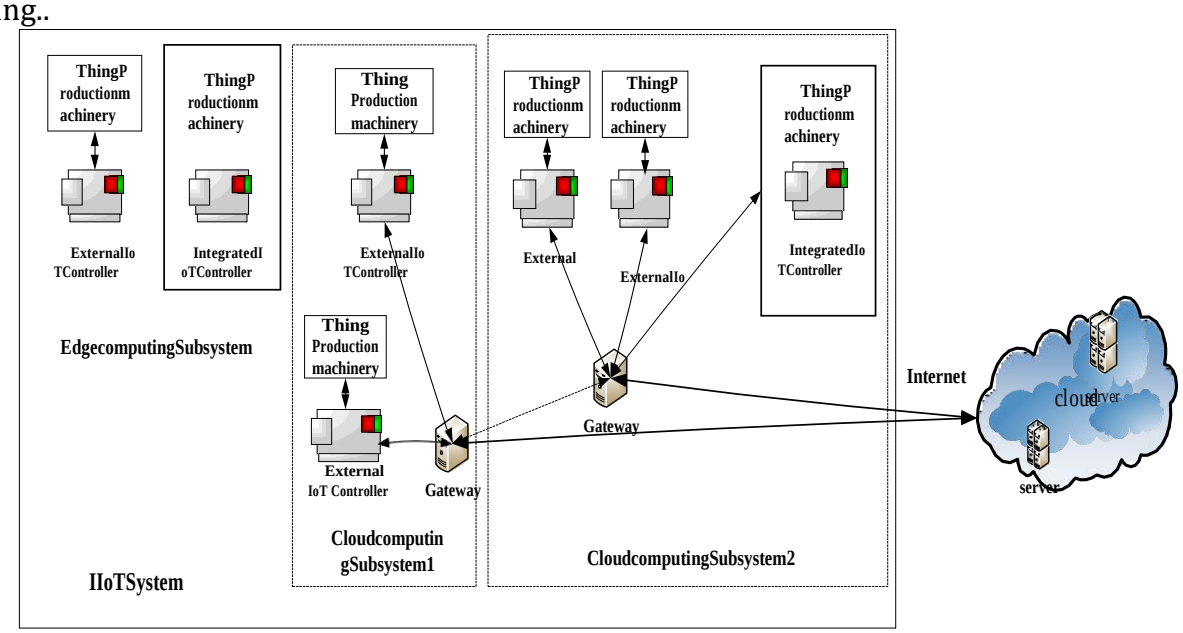

Figure.2.Example of the structure of the IIoT of things system with cloud and edge computing

By localising information flows inside the fog and edge subsystems, the use of fog and edge computing technologies makes it possible to create the IIoT system structure that best matches the production structure of the organisation and lowers the risk of unwanted access to the data. Thus, a complicated and multifaceted IIoT system of a specific organisation, which may include thousands of IoT devices, may be broken down.

Reduced processing times for production information are also achievable thanks to the utilisation of edge computing and fog. Generally speaking, using fog and edge computing can significantly lessen the impact of security threats like unauthorised access to information by intercepting transmitted data, unauthorised information interactions between IIoT devices (respectively production equipment), and unauthorised access to IIoT devices.

The works[11,12,13] contains the findings of calculations made to determine the parameters of cloudgy systems.

3. The application of various data transfer techniques

The practical application of IIoT can occasionally be limited by elements like the lifespan of devices powered by autonomous power supplies, communication ranges, the difficulty of communicating with moving objects, the necessary data rate, and the requirement to use various standards and communication medium types.

These issues contribute to the development of novel communication-related technological solutions, which have since been employed extensively in reality to build IIoT systems.

Examples of many widely used technologies (standards) for creating data networks that best satisfy IIoT criteria and lessen the impact of some security threats for IIoT systems are shown below.

A. Power grids are used for information sharing in PLC(Power Line Communication) technology, a type of telecommunication. The G3-PLC Protocol is a low –frequency narrow –band standard built on OFDM that is approved by the International Telecommunications Union (International Telecommunications Union) for data transmission over electrical networks (NB-PLC) .The requirements for systems that use OFDM modulation for narrow-band PLC technology have been established with the capacity to adapt to the parameters of the physical transmission environment , allowing the data rate to be increased to 128 Kbits/s . A technique known as Standard G3-PLC that works with IPv6 allows for the development of robust systems that can be managed online[15]

B. B.Low-Power Wide-Area Network (LPWAN) technology, an energy-efficient long-range network, was introduced in 2015 [16]. It is a wireless technology that has a variety of advantages over Wi-Fi and cellular networks for sending little amounts of data over great distances. This technology covers the network physical layer (NPL) technology and modulation mechanism for LoRa; LoRaWAN is an open protocol designed for networks with high capacity (up to 1,000,000 devices in one network), a range of up to 10-15 km in open space, and low power consumption. The connected system's dependability and security are ensured by this protocol, which offers unique encryption techniques. End devices (nodes) in the LoRaWAN network provide encrypted data to gateways (hubs), which subsequently send it to the network server of the service. .

The Protocol is perfect for Industrial IoT applications and systems because they don't have high requirements for data transfer rates or volume.

C. The 3GPP group built the NB-IoT Technology on top of current mobile (cellular) standards [17]. The network must be synced with all devices connected to it. Sending or receiving messages would be impossible in that case. Each synchronisation session, however , depletes the device’s betterly.

NB-IoT networks typically transmit data at a rate of 200 Kbps. While network performance will be redundant in suburban or rural locations, NB-IoT performs best in complicated urban environments. The Protocol works best for applications that demand regular message sending and receiving.

Figure 3 illustrates one potential use for telecommunications technology. The backup communication lines and subsystem servers are not depicted in the diagram.

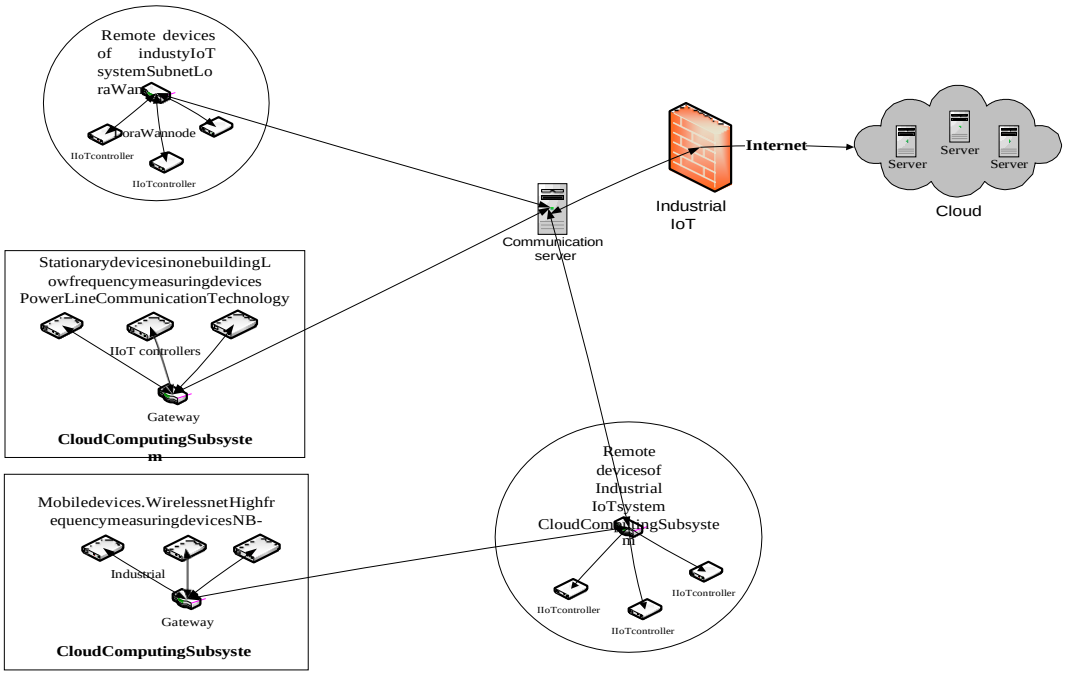

Figure.3.An example of possible application of telecommunication technologies

D.The fifth generation (5G) network might be regarded as the most promising and adaptable option for developing IIoT networks [18].

The maximum data transmission rate has significantly increased to up to 25 Gigabit/s (from the Real speed of 10 Gigabit/s), which is the most advantageous outcome of the 5G implementation. The signal delay is lowered to 1 msec with 5G. (in 4G and 3G 10 milisec and 100 milisec). Up to 100 million connections are feasible per square kilometre in 5G networks, which enables the development of IIoT systems for both major businesses and complicated industry-wide production cluster and system. The technology will also allow for the integration of staff gadgets.

For IIoT systems, 5G's primary benefits are:

- Network slicing technology, which allows the physical architecture of the 5G network to be divided into numerous virtual networks. As a result, industrial businesses now have the option to set up conceptually separate networks, each of which will be tailored to the unique requirements of the productions process.
- The Device-to-devicetechnologyenables close-by devices to share data directly, which is crucial for the transmission of data among various equipment positioned in confined space and the enterprise's staff.

The information provided regarding the capabilities of 5G will enable nearly all issues related to real-time production management and remote control of mobile objects to be resolved.

As a result, there are currently a number of potential options for communication organisations available to Industrial IoT system developers. These technologies allow for the encryption of traffic, the separation of multiple applications' and business units' communications, and the creation of additional communication channels. All of this lessens how much security concerns affect Industrial IoT systems.

4. Information protection with cryptography

The use of encryption in information transmission and storage is crucial, especially in IndustrialInternet of Things systems, as it makes it more difficult for data to be misused for use against the company and maintains the security of product information, documentation, and data.

However, using information encryption causes some issues with how the IndustrialIoT system is set up. Whenit been processed for calculations and equipment management, for instance, it must be presented in an open format,

necessitating frequent data encryption and decryption. As a result, processing times are delayed, there are significant overhead costs, and it is challenging to synchronise incoming data.

Here, it's important to consider the capabilities of IoT devices while analysing and defending the usage of protocols and the selection of encryption methods in various system locations and for various types of data. Standard encryption (hashing) techniques demand a lot of processing power to use. IoT devices can perform encryption and decryption functions on their own or with the assistance of additional specialised processors. The price of the IndustrialIoT system may rise in either scenario. In this regard, the adoption of low-resource (lightweight) encryption algorithms in Industrial Internt of ThingsIIoT systems—algorithms whose creation and analysis have received a lot of attention [19]—may be acceptable.

When it's important to verify the accuracy of the selection of the source and recipient of the data, as well as the accuracy of the communicated message, protection techniques include ways to authenticate both the devices and the transmitted messages. In a system with many IoT devices, this process becomes very challenging and calls for specialised equipment.

Thus, the employment of cryptographic protection techniques and tools can stop the illegal acquisition of production information and shield the business from losses brought on by the exposure of production information and goods.

5. protection for IIoT devices

There has been a lot of material recently about instances of IoT device misuse involving unauthorised access and administration. Due to modifications in the equipment's operation, for instance, this can result in large losses in the context of the IIoT. Intrusion detection systems (IDS - Intrusion Detection Systems) are techniques that can be used to protect devices but do not prohibit access because they only respond to the fait accompli.

It is important to authenticate the subjects who are permitted access to the devices in order to prohibit access to IIoT devices. In order to interact with the huge number of devices in the Industrial Internt of Things(IIoT) system, it is advisable to develop an identity users system - Management system (IdM - Identity Management). Access control utilising authentication servers could be a potential remedy (similar to the "Kerberos"system). These methods for addressing the issue of access control to IIoT system devices are relatively widespread, but they must be customised for each unique situation.

*6. **B**lockchain technology used for data storage*

In IIoT systems, the way production information is organised for storage is crucial. To guard against hardware and software failures, the storage system must offer data modification protection, data access control, and redundancy [20].

The possible solutions isblockchaintechnology.

It should be highlighted, nonetheless, that with IIoT system, there is no needs to compete for the privilege to record a block of data;

instead, specific algorithms can create and record blocks without the involvement of enterprise staff.

The characteristics of the enterprise's operational units determine the rules of the setup and the block composition. Finding the necessary data in the chain that has been formed is fairly challenging.

IV. CONCLUSION

The supplied data can primarily address the informational and functional level security issues in IIoT systems.

The administration of shared Industrial Internet of Things(IIoT) devices, system reconfiguration for new duties, and the selection of security measures are only a few of the many topics that are currently left unaddressed by this study. These issues must be resolved in each instance in accordance with their configuration because they are intricately linked to the unique characteristics of each production.

REFERENCES

[1] Gilchrist A. industry 4.0: The industrial internet of Things(IoT). Bangken,nonthaburi:apress,2016.–250p.

[2] J.Stankovic,"ResearchDirectionsfortheInternetofThings(IoT)", *InternetofThingsJournal,*Vol. 1,No.1,2014.

[3] W.Stallings,"TheInternetofThings:NetworkandSecurityArchitecture",*TheInternetProtocolJournal,* Vol.18,No4.2017.

[4] A.McEwen,andH.Cassimally,*"Designing the InternetofThings(IoT)",* ISBN-13:978-1118430620,Wiley,2013.

[5] R. Khan, et al., "Future Internet: The Internet of Things(IoT) Architecture,Possible Applications and Key Challenges"*, Frontiers of InformationTechnology (FIT),* 2012 10th International Conference on, 2012, pp.257-260.

[6] Cisco Systems, "The Internet of Things Reference Model," WhitePaper,2014.Availableat:*http://www.iotwf.com/*.

[7] ITU-T,"OverviewoftheInternetofThings,"RecommendationY.2060,June2012.

[8] ITU-T, "Common Requirements and Capabilities of a Gateway forInternetofThingsApplications,"RecommendationY.2067,June2014.

[9] Retatna A., Slice D., White R. Advanced IP Network Design. M.,Wiliams, 2002.–368p.(inRussian)

[10] Tanenbaum E., M. van Steen. Distributed systems. *Principles andparadigms*.Pearson PrenticeHall,2007.686p.

[11] V.N.Azarov;E.A.Saksonov;Yu.L.Leokhin,"AnalysisofInformationStructureoftheCorporateNetworkofEnterprise",*QualityManagement,TransportandInformationSecurity,Information Technologies,* 2018 IEEE International Conference on,(IT&QM&IS)2018,pp.9–12.DOI:0.1109/ITMQIS.2018.8524906.

[12] R.Y. Ivanyushkin, E.A. Saksonov, Y.L. Leokhin, V.A. Netes, M.A.Bykhovsky,"Analysisofhierarchicalstructureofthecorporatenetwork", *Quality Management, Transport and Information Security,InformationTechnologies,*Proceedingsofthe2017InternationalConference on, (IT&QM&IS) 2017, pp.196-198.DOI:10.1109/ITMQIS.2017.8085795.

[13] E.A.Saksonov, Yu.L. Leokhin, P.V. Panfilov" Structural Synthesisof the IoT System for the Cloud Computing", *2019 24th Conference ofOpen Innovations Association (FRUCT)*, Proceedings of the 2019InternationalConferenceon,(FRUCT)2019,pp.381-387.DOI:10.23919/FRUCT.2019.8711934.

[14] https://compuzilla.ru/plc-tekhnologiia/

[15] N. R. Murphy, D. Malone, "IPv6 Network Administration",O'REILY, 2005.260p.

[16] https://www.lora-alliance.org

[17] https://networkguru.ru/tekhnologiia-nb-iot-osobennostirazvertyvaniia

[18] https://www.huawei.com/minisite/russia/5g/about.html

[19] ISO/IEC 29192-3:2012 Information technology – Securitytechniques–Lightweight cryptography

[20] https://tutdenegki.com/crypta/blockchain.html

[21] Murty, A., M. Satyanarayana, And I. Devi. "Compressor Health Monitoring Using Iot." *International Journal Of Mechanical And Production Engineering Research And Development* 8.3 (2019): 117-124.

[22] Kumar, A. Senthil, And Easwaran Iyer. "An Industrial Iot In Engineering And Manufacturing Industries—Benefits And Challenges." *International Journal Of Mechanical And Production Engineering Research And Dvelopment (Ijmperd)* 9.2 (2019): 151-160.

[23] Singh, Yuvraj. "Conceptual Study On Network Security And Its Types." *International Journal Of General Engineering And Technology (Ijget)* 6.5: 37-42.

[24] Patel, Preeti. "Security Of Information With Biometric Applications." *Iaset: International Journal Of Library & Educational Science (Iaset: Ijles)* 2.2: 81-88.

[25] Babu, R. Hemanth, T. Raja Reddy, And N. Giri Babu. "Role Of Information Technology And Analysis Of Various Frameworks In Customer Relationship Management." *International Journal Of Sales & Marketing Management (Ijsmm) 5.3 (2016)* 1 (2016): 6.

[26] Nallusamy, S., Et Al. "Implementation Of Total Productive Maintenance To Enhance The Overall Equipment Effectiveness In Medium Scale Industries." *International Journal Of Mechanical And Production Engineering Research And Development* 8.1 (2018): 1027-1038.