iJRASET
International Journal For Research in Applied Science and Engineering Technology

# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

**Volume:** 10 **Issue:** X **Month of publication:** October 2022

**DOI:** https://doi.org/10.22214/ijraset.2022.46981

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
*ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538*
*Volume 10 Issue X Oct 2022- Available at www.ijraset.com*

# Cyber Security for Internet of Things

Dr. Shikha Gupta[1], Vaama Nikam[2], Tanay Mukadam[3], Prathmesh Deshmukh[4], Prathamesh Bhanse[5]
[1, 2, 3, 4, 5]*Department of Computer Science Lokmanya Tilak College of EngineeringNavi Mumbai, India*

***Abstract:*** ***The Internet of things has gained intense popularity in the past few years. It has become one of the most important technologies. However along with gaining popularity, threats related to cyber security have increased. As the name suggests, Internet of Things, it is completely based on the internet which means a hacker can find a weaklink in the network and exfiltrate data to the cloud and threaten to keep, delete or make the data public. This includes sensitive data, personally identifiable information (PII), protected health information (PHI), personal information, intellectual property, data, and governmental and industry information systems. Cybersecurity is a set of processes, tools and frameworks to protect networks, devices, programs and data from cyber attacks.This paper highlights the different types of Cyber attacks possible on IoT and suggests few mitigations towards it.***

***Keywords: IoT, Industry4.0, IIoT, Cyber Security, Cyber Attacks***

## I. INTRODUCTION

Nowadays technology changes rapidly day by day and affects our lives in many ways. Internet connectivity is easily available everywhere. Security plays a vital role when IoT devices are near to us and send their data over the network. IoT devices are also extensively used in industries. Therefore, it is important to consider the risk of cyber vulnerabilities & attacksin the IoT environment and implement recommendation steps to secure the IoT environment to some extent.

The Industrial IoT is a network of physical objects that are connected to each other, and the data generated by these objects is collected and analyzed. The smart industries use thousands of smart sensors and devices in their automation processes. The Internet of Things (IoT) connects different IoTsmart objects around people to make their life easier by connecting them with the internet, which leads IoT environments vulnerable to many attacks.

The ever-growing demand for Internet of Things (IoT)devices is providing a promising opportunity not only for the development of various home automation systems but also for different industrial purposes. Earlier only computers and mobile devices were connected to the internet but now due to advancement in technology other devices like televisions, air conditioners, cars cameras and other equipment are connected to the internet.

It's estimated that the number of active IoT devices will surpass 25.4 billion in 2030. The Industrial IoT is one of the most predominant technologies in the world today. There are many risks associated with this new technology, but cyber security is one of the most important issues to be taken care of.

## II. LITERATURE SURVEY

[1]This paper focuses on the research work to secure IoT solutions from the security challenges like Device cloning attacks and Sensitive data exposure. Successful securitysolutions have been provided for the two types of attacks. [2]In this paper we learnt about the Cisco IoT architecture. Itattempts to provide us with a list of security threats and issueson the cloud-side layer of IoT which normally consists of abstraction levels and data accumulation. [3]This paper refers to the peculiarities that have been hampering the Industrial Internet of Things for which a survey analysis has been conducted in order to safeguard the exchanged information of the distributed devices. [7]This paper focuses on the cyber risk analysis and artificial intelligence in the industrial internet of things and shows us how we must incorporate the right strategies and tools to anticipate, prevent and overcome common edge computing security risks.[9]In order to provide aguideline to researchers, this survey primarily attempts to classify the attacks based on the objects of vulnerability in IoT. It gives us a detailed description about the cyber-attacks taking place in the IoT.[11]

In this paper we learnt about thorough description of attacks against Industrial IoT systems as well asanalysis of indicative solutions against these vulnerabilities.

| Sr.No | Years | Authors | Focus |
|---|---|---|---|
| 1. | 2017 | Swapnil Naik, Vikas Maral | Cyber Security - IoT |
| 2. | 2018 | Zeinab Bakhshi1, Ali Balador2,3 and Jawad Mustafa2, | Industrial IoT Security Threats and Concerns by Considering Cisco and Microsoft IoT reference Models |
| 3. | 2018 | Haralambos Mouratidis,Vasiliki Diamantopoulou, | A Security Analysis Method for Industrial Internet of Things |
| 4. | 2019 | C. Vijayakumaran1 , B. Muthusenthil2, B.Manickavasagam3 | A reliable next generation cyber security architecture for industrial internet of things environment |
| 5. | 2019 | Bjorn Leander , Aida Causevic´and Hans Hansson | Cybersecurity Challenges in Large Industrial IoT Systems |
| 6. | 2020 | USMAN TARIQ 1, AHMAD O. ASEERI ,MOHAMMED SAEED ALKATHEIRI3 , AND YU ZHUANG4 | Context-Aware Autonomous SecurityAssertion for Industrial IoT |
| 7. | 2020 | Petar Radanliev1*, David De Roure1 , Kevin, Jason R. C. Nurse2, Rafael Mantilla Montalvo3, Omar Santos3, La'Treall Maddox3 and Pete Burnap4 | Cyber risk at the edge |
| 8. | 2020 | Sidi Boubacar ElMamy 1, Hichem Mrabet 2, Hassen Gharbi 3, Abderrazak Jemai 4 and Damien Trentesaux | A Survey on the Usage of Blockchain Technologyfor Cyber-Threats in the Context of Industry 4.0 |
| 9. | 2020 | Yash Shah, Shamik Sengupta | A survey on Classification of Cyber-attacks on IoT and IIoT devices |
| 10. | 2021 | Henry Vargas , Carlos Lozano-Garzon * , Germán A. Montoya * and Yezid Donoso | Detection of Security Attacks in Industrial IoT Networks: A Blockchain and Machine Learning Approach |
| 11. | 2021 | Kostantinos Demertzis, Konstantinos Demertzis | Cyber Threats to Industrial IoT: A Survey on Attacks and Countermeasures |
| 12. | 2021 | Lubna Luxmi Dhirani 1,2,*, Eddie Armstrong 3 and Thomas Newe | Industrial IoT, Cyber Threats, and Standards Landscape: Evaluation and Roadmap |

## III. IOT DEVICES

IoT devices can classified into different categories

1) *Smart Homes:* Smart devices allow users to control their homes and offices using apps and voicecommands. These devices are connected to the internet. Devices such as smart bulbs, switches, air conditioners, gates etc which are used in our daily lives.
2) *Wearable Devices:* These are the most common type of IoT devices available. These devices are worn by humans which track individual movements or actions,are commonly connected to smartphones via Bluetooth and, from there, to the Internet. They help us track our daily activities, give us health insights andhelp in communication. As of now our market is ruledby fitness devices especially during the covid-19 pandemic.
3) *M2M (Machine to Machine) Devices:* These are deviceswhich allow data to be transferred and execute variousoperations without any human interference. These machines receive and execute tasks with the help of the Internet thus eliminating the need to hire a human to watch them 24/7. Apart from this, these devices are also used M2M devices play a pivotal role in remote control, the automotive industry, robotics, traffic control, and fleet control. Such devices are also used in the medical field for real time monitoring of patients and tracking other healthcare assets. The M2M architecture can be classified into three categories such as M2M domain, network domain, and application domain.

### A. *IIOT (Industrial Internet of Things )*

1) *Data Accumulation Layer :* This layer captures data and stores it so it is usable by applications when necessary. Converts event-based data to query-based processing. It allows the storage of application data in files, databases, or preferences, in internal or removable storage. Data Accumulation Networkingsystems are built to authentically move data. The data is in motion. Prior to Level 4, data is moving through the network atthe rate and organization determined by the devices generatingthe data.

2) *Data Abstraction Layer:* The IoT Connectivity is extremely fragmented. There are now a multitude of competing standards organizations that lay claim to being the IoT universal interconnect standard.[11] This puts developers of applications and devices for the Internet of Things in an impossible position that will ironically result in a sub-optimal outcome for the ecosystem. The Data Abstraction layer tackles these issues by providing a single abstract data model to all devices of the same service, allowing connectivity to be implemented in a vendor, API and protocol agnostic fashion. This approach also allows the seamless and dynamic integration of new devices into your existing ecosystem. The Data abstraction layer to define the translation rules uses language binding scripts required for a specific device connectivity. These scripts are text files writtenin a very clear and simple JSON model. [11]These scripts are hosted in Weaving Things cloud service and are used upon device detection and dynamically loaded. Integrators might choose to use their own abstract language. In this case a language abstraction script can be configured to allow thecomplete translation.

*B. Classification of Attacks*

*1) Data Accumulation Layer*

*a) SQL Injection:* In an SQL injection attack, the attacker tries to insert malicious SQL (Structured Query Language) commands for execution and hamper the contents of the database. The SQL injection attack allows the user to spoof, identify, disturb the existing data, make it unavailable or deletethe data. An SQL injection attack works when the hackerimpersonates someone who is allowed to execute a finite set ofrequests: the attacker inputs a valid request and interchanges it with the new instructions which also get executed. IOT devicesare difficult to secure for various reasons. One of the biggest concerns is that these devices need to be able to be accessed remotely, which means they cannot be guarded with a firewall which indeed leaves IOT devices exposed to many types of attacks that would easily be circumvented by desktop or mobiledevices.

*b) Ransomware:* Ransomware attacks threaten to deny access to the computer system, usually by using cryptographic encryption techniques. Ransomware is a malicious software. It uses malwares and malicious codes to encrypt the data. In numerous cases, the ransom demand comes with a deadline. If the victim doesn't pay, the ransom is gone forever or the ransom increases. It is an IoT environment which is able to shut off the entire network of physical devices, because it is easy for such powerful malware to take the control of devices with constrained resources. Ransomware is capable of affecting all the security aspects of IoT, which include integrity, authentication, and availability.

*c) Malicious Attack:* A malware attack is a common cyberattack where malware executes prohibited actions on the victim's system. The malicious software confines many specific types of attacks such as spyware, ransomware, command and control, and more. Some malware attacks end up with mainstream news coverage due to their appalling impact. An example of a famous malware attack is the Operation Prowli ransomware attack.

Best practices against malware attacks:

- Ensure Your Network is Secure
- Use of proven technology and methodologies—such as usinga firewall, IDS, IPS, and remote access only through VPN.
- Create regular and verified backups
- Having a regular offline backup can be the difference betweenswiftly recovering from a destructive virus or ransomwareattack and stressful, frantic scrambling with costly downtime/data-loss.

*2) Data Abstraction Layer*

*a) DDOS:* A Denial of Service attack is a vicious attempt to affect the vacuity of a targeted system, similar as a website or operation, to licit end druggies.[11] Generally, bushwhackers induce large volumes of packets or requests eventually overwhelming the target system. In case of a Distributed Denialof Service attack, the bushwhacker uses multiple compromisedor controlled sources to induce the attack. In general, DDoS attacks can be insulated by which subcaste of the Open Systems Interconnection(OSI) model they attack.[6] They're most common at the Network(subcaste 3), Transport( Subcaste 4), donation(Subcaste 6) and operation( Subcaste 7) Layers. [9]

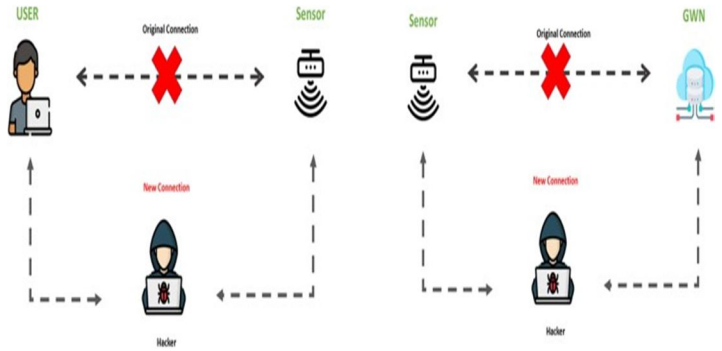
- *Reduce Attack Surface Area:* One of the first ways to alleviate DDoS attacks is to minimize the face area that can be attacked thereby limiting the options for bushwhackers and allowing you to make protections in a single place. [11] We want to ensure that we don't expose our operation or coffers to anchorages, protocols or operations from where they don't anticipate any communication. therefore, minimizing the possible points of attack and letting us concentrate our mitigation sweats.[3] In some cases, you can do this by placing your calculation coffers behind Content Distribution Networks( CDNs) or cargo Balancers and confining direct Internet business to certain corridors of your structure like your database waiters.

- *Know what's Normal and Abnormal Business:* Whenever we describe elevated situations of business hitting a host, the veritable birth is to be suitable only to accept as important business as our host can handle without affecting vacuity. Thisconception is called rate limiting.[6] More advanced protectionways can go one step further and intelligently only accept business that's licit by analyzing the individual packets themselves.[9] To do this, you need to understand the characteristics of good business that the target generally receives and be suitable to compare each packet against this birth.
- *Emplace Firewalls for Sophisticated Operation Attacks:* A good practice is to use a Web operation Firewall(WAF) against attacks, similar to SQL injection cross-site request phony , that attempt to exploit a vulnerability in your operation itself. also, due to the unique nature of these attacks, you should be suitable to fluently produce customized mitigations against illegitimate requests which could have characteristics like disguising as good business or coming from bad IPs, unanticipated topographies, etc. At times it might also be helpful in mollifying attacks as they are to get educated support to study business patterns and produce customized protections.

b) *Man in The Middle Attack:* A man- in- the- middle (MITM) attack is a type of cyberattack where bushwhackers block a discussion or data transfer, either by wiretapping or by pretending to be a licit party.[11] To the victim, it'll appear as though a standard exchange of information is underway but by fitting themselves into the “middle” of the discussion or data transfer, the bushwhacker can still commandeer information.[3] The thing of a MITM attack is to recoup nonpublic data similar to bank account details, credit card figures, or login credentials, which may be used to carry out further crimes like identity theft or illegal fund transfers. Because MITM attacks are carried out in real time, they frequently go undetected until it’s too late.

Prevention of Main in the Middle Attack:

- While being apprehensive of how to describe an implicit MITM attack is important, the stylish way to cover against them is by precluding them in the first place. Be sure to follow these stylish practices
- Avoid Wi- Fi networks that are n’t word- defended, and no way use a public Wi- Fi network for sensitive deals that bear your particular information.
- Use a Virtual Private Network — especially when connecting to the internet in a public place. VPNs cipher your online exertion and help an bushwhacker from being suitable to read your private data, like watchwords or bank regard information.
- Log out of sensitive websites (like an online banking website) as soon as you ’re finished to avoid session kidnapping.
- Maintain proper word habits, similar as no way reusing watchwords for different accounts, and use a word director to ensure your watchwords are as strongas possible.
- Use Multi-factor authentication for all of yourwatchwords.
- Use a firewall to ensure safe internet connections.
- Use antivirus software to cover your bias from malware.




Man in the Middle Attack

c) *Buffer Overflow:* Buffer overflow occurs when a program or process attempts to write further data to a fixed- length block of memory, or buffer, than the buffer is allocated to hold, the redundant data overflows into conterminous memory locales and corrupts or overwrites the data in those locales.[11] The redundant data occasionally holds specific instructions for conduct intended by a hacker or vicious stoner, this data could spark a response that damages lines, changes data or unveils private information.[3] Hackers use buffer overflows to preempt system’s database information and to intrude prosecution of system programs. Best way to avoid Buffer Overflow is to write secure law.

*d)* *Botnet:* Botnet Attack happens when a group of internet- connected bias is infected by malware that's under control by avicious hacker.[3] It generally involve transferring spam, data theft, exploiting sensitive information, or launching vicious DDoS attacks. Botnets use your bias to fiddle other people or beget dislocations each without your concurrence.[11] The botsserve as a tool to automate mass attacks similar as data theft, garçon crashing and malware distribution. This attack targets database services which substantially includes MySql waiters

Prevention of Botnet Attacks:

- Ensure all systems are streamlined
- Maintain good cybersecurity hygiene
- Establish control access to machines and systems
- Continuously cover network business
- Bear cybersecurity training for workers

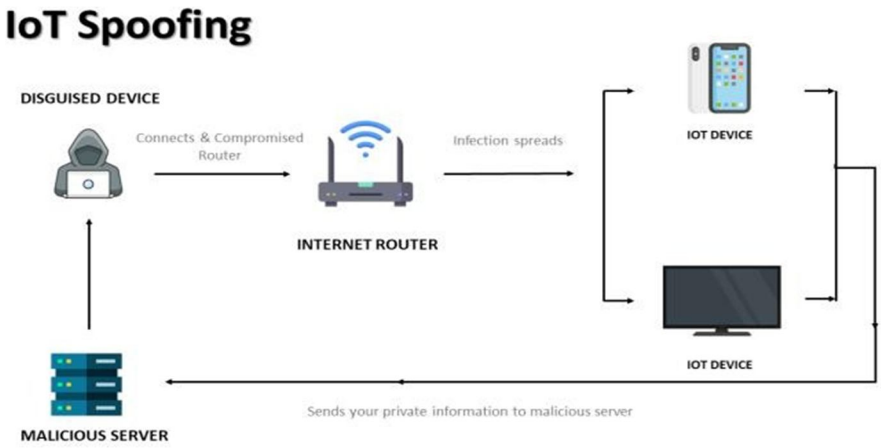
*e)* *Reverse Engineering:* Reverse- Engineering is the act of dismembering an object to see how it works. A Reverse Engineering attack is a person- to- person attack in which a bushwhacker convinces the target that he or she has a problemor might have a certain problem in the future and that he, the bushwhacker, is ready to help break the problem.[3] The hackerestablishes contact with the target through emails and social media platforms, using multiple schemes and pretending to be a donator or professed security labor force to move them to giveaccess to their system network. Though this fashion may feel outdated and ridiculous, it has proved largely effective, especially when the victim's system/ network shows signs of being compromised. Hackers use the information to attack an operation, and they take piecemeal programs to produce viciousperformances of them.[6] Although rear engineering presents aserious threat to operations, numerous apps are reaching the request without any safeguards against the practice. In a study of 30 mobile fiscal apps, 97 suffered from a lack of double protection, making it possible to decompile the apps and reviewthe source law.

*f)* *Brute Force Attack:* A Brute Force Attack is a trial-and- error method. It is used to decode sensitive data. The most common applications for such attacks are cracking passwords and cracking encryption keys. It uses trial and error to crack passwords, login credentials, and encryption keys. It is a simpleyet reliable tactic for gaining unauthorized access to individualaccounts and organizations' systems and networks.[6] Different types of brute force attacks use different methods to reveal sensitive data.

Some of the popular types of brute force attacks are as follows:

- Simple Brute Force Attacks
- Dictionary Attacks
- Hybrid Brute Force Attacks
- Reverse Brute Force Attacks
- Credentials Stuffing Prevention Brute Force Attack:

➢ *Account Lockouts After Failed Attempts:* Accountlockouts with progressive delays lock an account onlyfor a set amount of time after a designated number of unsuccessful login attempts.
➢ *Use Strong Passwords.*
➢ *Monitor IP Addresses:* IP Address icon in relation to the second tactic, you should limit login attempts to users coming from a specified IP address or range. This is especially important if you have a hybrid workenvironment or most of your employees work remotely.
➢ *Use CAPTCHAs:* Captchas are a good way of preventing bots and automated tools from doing actions on your website by giving them challenges before they even can attempt a login.




## IV. IOT SPOOFING

### A. *Attack Mitigation*

Hackers often target weak or vulnerable links that exist in networks or security systems employed to manage these devices. Attackers are actively looking to exploit these weaknesses to their benefit. Nowadays, every device that is connected to the internet is prone to cyber-attacks. The interconnection of IoT/IIoT devices benefits attackers as all they are required to do is find one vulnerability and they can access data from all of the connected devices. In this section, some of the most common methods used to protect the system against Cyberattacks are discussed.

1) *Use Strong Passwords:* A strong password is the main barrier keeping most of your IIoT device from being hacked. Without up-to-date practices, you might be using passwords that attackers can easily guess within hours. Exposing yourself to identity theft and extortion is a risk you should never take. You will need to create passwords that can fight modern password theft methods.[9] It is a smart way to fight data theft. A hacker would use any information they could find about you and use common patterns in passwords to guess yours.
2) *Keep your Software, Firmware Updated:* Latest update keeps you protected with the latest security patches and reduces the chances of cyber-attacks. Any vulnerabilities or exploits can be fixed and secure your IoT devices. IoT devices have no other layer of protection and updating regularly is crucial for their security.[7] The majority of IoT manufacturers send regular updates to your device and for checking new updates you should visit their website.. The system clean up helps to fix the security flaws of older software versions. Hackers are constantly improving their plans to invade your privacy. So it is better to keep your device updated and save it from getting hacked.
3) *Protect Against Physical Tampering:* With IoT, we are installing millions of devices within hand's reach, opening a new opportunity for hackers to tamper with the device and get control of it. Tampering can be done in a lot of different ways. It involves anything from connecting to exposed ports, to interrupting the device's power, device theft, removing parts, etc.[9] You can prevent those attacks by ensuring your device has no exposed ports or connectors. Implement locks or other ways to ensure that only authorized people can get access to your device.
4) *Use Multi-Factor Authentication:* Multi-factor authentication (MFA) requires that, any time you try to log in to a device, you also have another credential on hand to prove if it's really you. Typically, this means the device will send a 6 digit code to your email or smartphone. [9]Providing this code will allow you to log in to the device. There are many cases where MFA isn't suited for IoT devices at the user level, but a good argument for implementing MFA can always be made at the admin level. Like a strong password, this provides some additional measures to protect IoT devices and helps ensure unauthorized users can't easily log in.
5) *Apply Network Segmentation for Stronger Defense:* The security goal of network segmentation is to reduce the attack surface. Network segmentation divides a network into two or more subsections to enable granular control over lateral movement of traffic between devices and workloads. In an unsegmented network, when a large number of endpoints communicate directly with one another without any partitioning in place, there is a greater chance that a single compromise event will spread laterally to become a contagion. In contrast, the more a network is segmented, the harder it is for hackers to endanger a device as a single point of compromise for launching exploits laterally. Use of virtual local area network (VLAN) configurations and next-generation firewall policies to implement network segments that keep IoT devices separate from IT assets

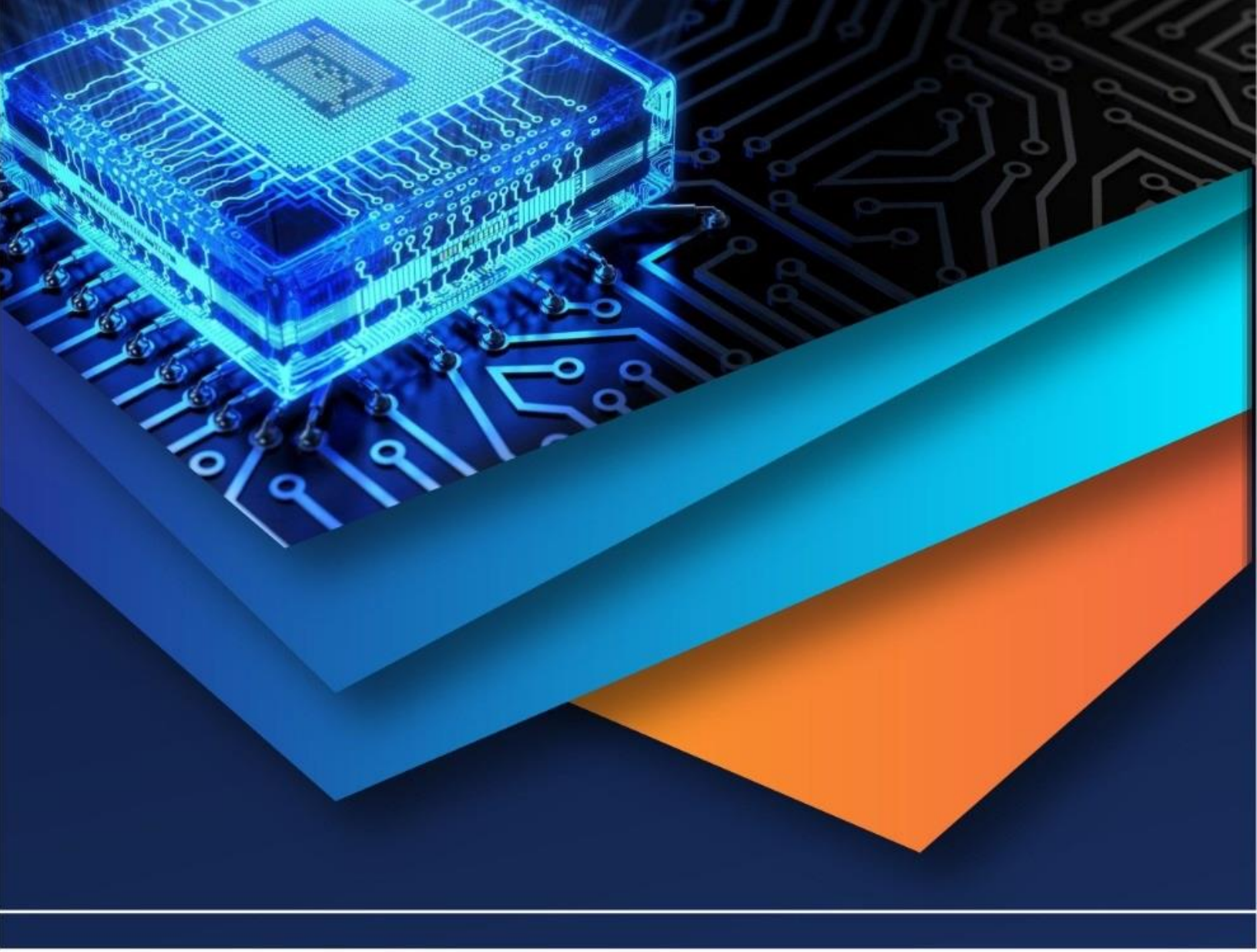
6) *Generate Backups:* Every device generates data that is analyzed to improve performance. However, attacks similar to ransomware can prevent users or data analysis applications from accessing that data. Creating an automatic backup schedule can ensure that the operations can be easily resumed. Multiple copies of the backup must be created in case a backupis affected. Along with the creation of backups, one needs to ensure that they are accurate and up-to-date to prevent the loss of critical data.
7) *VPN (Virtual Private Network):* Multiple IoT projects have begun implementing security measures. One of the most popular solutions is implementing a VPN. A VPN (Virtual Private Network) is a network technology that extends a local area network to a public one like the internet. This process allows users to send and receive data across public networks as if their computers were directly connected to the private network. A point-to-point connection is established with tunneling protocols. This means that your project's IP address,the number that identifies any device's place in a network, canchange to reflect the new one used with the VPN. When connecting a device to the VPN server, a new IP address is assigned in order to leave the devices in the new virtual network. Just an IP address can give away a device's real-worldlocation, so hiding it (or changing it) by accessing a VPN, can change your real-world location to any place you wish to, giving you an extra bit of security.

## V. CONCLUSION

In this study, a thorough description of attacks against Industrial IoT systems was carried out, considering the most important features and vulnerabilities that they incorporate, at the same time a thorough analysis of indicative solutions against these vulnerabilities, as proposed in the most recent literature.[6] As future scope, we aim to analyze more IoT Systems in detail and focus on the cyber security aspects identified in this paper to provide solutions for the same.The aim is to analyze solutions that can be applied to a truly modular infrastructure that scales well with respect to large scale IoT systems.[9]

## REFERENCES

[1] Swapnil Naik, Vikas Maral, 'Cyber Security -IoT' in 2017
[2] Zeinab Bakhshi1, Ali Balador2,3 and Jawad Mustafa2, 'Industrial IoT Security Threats and Concerns by Considering Cisco and Microsoft IoT reference Models' in 2018
[3] Haralambos Mouratidis,Vasiliki Diamantopoulou, 'A Security Analysis Method for Industrial Internet of Things ' in2018
[4] C. Vijayakumaran, B. Muthusenthil, B.Manickavasagam3 'A reliable next generation cyber security architecture for industrial internet of things environment' in 2019
[5] Bjorn Leander , Aida Causevic´and HansHanssonCybersecurity Challenges in Large Industrial IoT Systems in 2019.
[6] USMAN TARIQ 1, AHMAD O. ASEERI , MOHAMMEDSAEED ALKATHEIRI3 , AND YU ZHUANG4, 'Context- Aware Autonomous Security Assertion for Industrial IoT' in 2020
[7] Petar Radanliev1*, David De Roure1, Kevin Page1, Jason R. C. Nurse2, Rafael Mantilla Montalvo3, Omar Santos3, La'Treall Maddox3 and Pete Burnap4, 'Cyber risk at the edge' in 2020
[8] Sidi Boubacar ElMamy 1, Hichem Mrabet 2 , Hassen Gharbi 3 , Abderrazak Jemai 4 and Damien Trentesaux, 'A Survey on the Usage of Blockchain Technology for Cyber-Threats in the Context of Industry 4.0' in 2020
[9] Yash Shah, Shamik Sengupta, 'A survey on Classification ofCyber-attacks on IoT and IIoT devices' in 2020
[10] Henry Vargas , Carlos Lozano-Garzon * , Germán A.Montoya * and Yezid Donoso, 'Detection of Security Attacks in Industrial IoT Networks: A Blockchain and Machine Learning Approach'
[11] Konstantinos Demertzis, 'Cyber Threats to Industrial IoT: A Survey on Attacks and Countermeasures'
[12] Lubna Luxmi Dhirani 1,2,*, Eddie Armstrong 3 and Thomas Newe, 'Industrial IoT, Cyber Threats, and Standards Landscape: Evaluation and Roadmap'
[13] Ghazi Abdalla Abdalrahman, Hacer Varol ,'Defending Against Cyber-Attacks on the Internet of Things ', 2019



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY