International Journal of Computer and Organization Trends
ISSN: 2249 – 2593 / https://doi.org/10.14445/22492593/IJCOT-V12I1P306

Volume 12 Issue 1, 27-36, Jan-Apr 2022


*Review Article*

# Cybersecurity Considerations for Industrial IoT in Critical Infrastructure Sector

Neha Priya[1]

[1]*Department of Educational Studies, Jamia Millia Islamia, Delhi, India.*

Received Date: 18 March 2022
Revised Date: 27 April 2022
Accepted Date: 29 April 2022

***Abstract*** *- There is an increasing demand for Internet of Things (IoT) technology in industries, especially in nations with large populations but limited resources. Critical infrastructure is one such industrial sector on which the population depends for sustainable development. Industrial IoT or IIoT has the potential to drive growth in critical infrastructures. However, technology transformation is time-consuming before large-scale investment and deployment can occur. Besides research and standardization, adequate business assessment, planning, and decision-making are required to leverage IoT technology's advantages. IIoT environment consists of cyber-physical systems in Industry 4.0 applications. Therefore, cybersecurity is a major challenge that critical infrastructures have to deal with while implementing IIoT solutions; this paper discusses cybersecurity considerations for Industrial Automation and Control systems that can be adopted in the critical infrastructure sector to implement IIoT security. To ensure safeguard from threats and adversaries and reliable operation of critical infrastructures, there are three focus areas of the proposed framework: security objectives, security standards, and enabling technologies in the IIoT environment.*

***Keywords*** *- Critical infrastructure, Cybersecurity, Cyber-physical system, Industrial Automation, Control System, Industrial IoT.*

## I. INTRODUCTION

The Internet of Things (IoT) technology enables a heterogeneous wireless internetwork of Things connected in real-time over the internet, i.e., cyberspace. The Things in IoT are nodes that compute, communicate and store data with programs and protocols, just like any network device connected to the internet [1]. No Thing can standalone demonstrate IoT technology, and rather it is part of a collection of devices. For example, electronic devices, sensors, actuators, and relays are connected to network devices to form an IoT system within the energy infrastructure [2]. Each Thing in IoT has well-defined individual functions as well as collective goals. Such systems are also known as Cyber-Physical Systems (CPS), which bring multidisciplinary physical processes to cyberspace. This can form a system-of-systems (SoS) based on points of interest catering to each system sub-goal. Thus, IoT presents an avenue for real-time system integration [3]. The key advantages of IoT systems are real-time communication, process control, monitoring and surveillance, ease of integration, and efficient utilization of resources.

The estimates of connected devices that will come under the manifolds of IoT will be around 18 billion by 2022 due to the increasing diversity of IoT application areas and reduction in the cost of IoT devices [4]. Table 1 gives some applications of IoT-based products and services. These application areas can be broadly classified based on their deployments goals, such as Industrial IoT, Home or Personal IoT, Social or Community IoT, and Cognitive IoT.

The Industrial IoT (IIoT) has gathered major research thrust since it involves large-scale business. The projected market share of IoT applications with large size investment includes key critical infrastructures such as Healthcare (41%), Electricity (7%), Agriculture (4%), Urban Infrastructure (4%), and Security (4%) [5]. Any investment in technology transformation needs profit and risk assessments backed by research confidence. For example, key technology aspects for smart manufacturing involve IoT with cybersecurity [6]. The adoption of IoT in critical infrastructures is a potential challenge. It requires a digital transformation. The value added by the IoT ecosystem is not just technical or economic in perspective but also societal [7]. Social trust could be vital for critical infrastructure sectors as pillars of a country's growth and development. Huge investment capital is required to build them. Any loss or damage to them may risk people's lives and safety, national security, economic vitality, societal well-being, and preservation. So, information over the IoT platform needs to be secured for critical infrastructures.

Fig. 1 shows important critical infrastructure sectors where the adoption of IIoT has added to the growing complexity of such systems [8]. For example, healthcare infrastructure is integrated with emergency handling, ambient assisted living, water, environment quality control, telemedicine infrastructure, patient diagnosis, and monitoring [9]. Power generation infrastructure has sub-systems like plant control, smart grid, Heating, Ventilation and Air Conditioning (HVAC), water treatment, pollution control, fire protection, disaster monitoring, physical security, surveillance, etc. One or more sub-systems can be built-in IoT environments, each having its outcome and interdependencies. Any failure in one component or system can affect another and may cause cascading failures [10].

With IoT-led digital transformation, the physical system is accessible on the cyber platform. Therefore, physical security is accompanied by cybersecurity risks [11]. The critical information in these infrastructures makes both safety and security interchangeable. Any compromise of information security may lead to unsafe, adverse operations since information is the most common cyber attackers target [12]. Cyber threats may range from smaller malware attacks to more serious cyber warfare [13] or even cyber terrorism [14]. Assessment of threats and vulnerabilities is integral to the security planning process for deploying IoT technology.

The emergence of CPS has given rise to new vulnerabilities in a critical infrastructure network. A preliminary approach is to assess the resilience of critical infrastructure before taking key decisions on resource allocation [15]. For taking benefits of the IoT, IoT architecture not just comprises hardware, software, and communications but also security components as proposed in [16].

This work presents the cybersecurity considerations within the IIoT framework for critical infrastructures. In section II, we review the related literature to understand the cybersecurity aspects of IIoT in protecting critical infrastructures. Section III identifies various IoT challenges for Industrial Automation and Control Systems (IACS). Section IV is a comparative analysis of the cybersecurity considerations for IoT deployment in IACS. Finally, we discuss the results and suggest cybersecurity considerations to gain the advantage of the IoT technology in critical infrastructures.

**Table 1. Applications of IoT [1] [5]**

| **Technology** | **Radio Frequency Identification (RFID)** | **Near Field Communication (NFC)** | **Machine-to-Machine (M2M)** | **Mobile-to-Mobile** |
|---|---|---|---|---|
| **Product-based Application** | Smart Homes and Offices | Smart cards | Industrial Control | Smart Cars |
| | Smart Parking | Personal Healthcare devices | Smart Agriculture | Wearables |
| **Services based application** | Logistics | Inventory management | Smart Grid | Intelligent Transport systems |
| | Smart Water Supply | Tracking security and Emergencies | Smart Cities | Tele-communications |

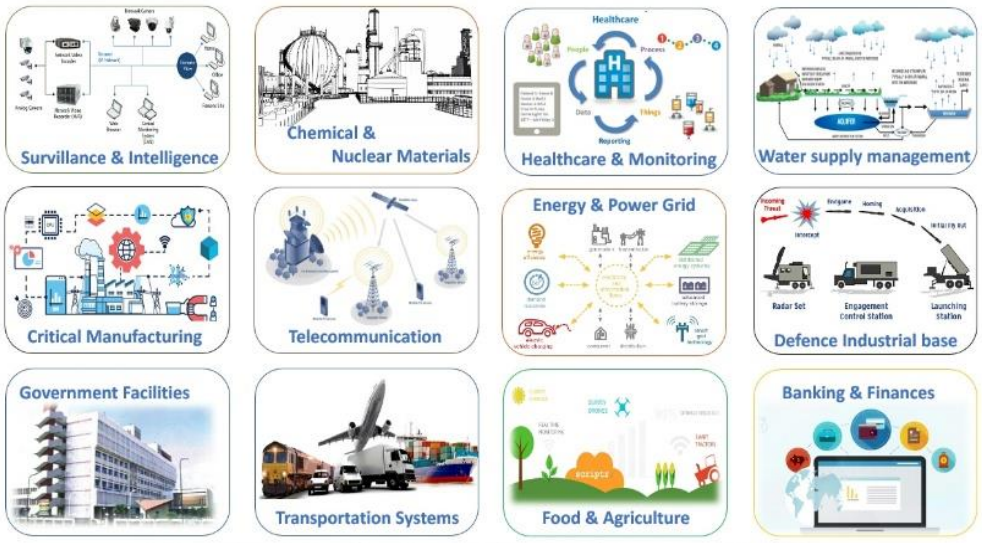


**Fig. 1 Critical infrastructure sectors with potential for IIoT application [8]**

## II. CYBERSECURITY ASPECTS FOR CRITICAL INFRASTRUCTURE PROTECTION

In this section, we briefly discuss some available literature related to the area of this study. The scheme of the literature review is divided into three perspectives, first, the different cybersecurity challenges in critical infrastructures; second, the emerging technologies for the security of IoT systems; and third, the IIoT security solutions for the critical infrastructure sector.

### *A. Cybersecurity Challenges*

Assessment of vulnerabilities and related threats is a primary challenge for cybersecurity of critical infrastructures. Q. Qassim *et al*. [13] describe the potential vulnerabilities and threats to the electrical power grid Supervisory Control and Data Acquisition (SCADA) system. Past incidents of attack reveal that Stuxnet is one of the major cyberattacks on industrial control systems and can be incidental to cyberwarfare [10].

Another key challenge in critical infrastructure complexes is managing access to systems and information in the presence of many people internal and external to the organization. Security policy requirements for access control to offices, resources, local area network devices, etc., in critical infrastructure premises need to be analyzed. A building information model is an integral part of security operations by N. Skandhakumar *et al*. [17].

One of the challenges to cybersecurity is the detection of cyber incidents. To detect attacks on the power system grid, N. Wallace and T. Atkinson [18] have proposed a technique to retrieve information using Principal Component Analysis (PCA) and predict malicious activity. P. Haller *et al*. [19] present a useful monitoring mechanism for intrusion detection in industrial control systems based on deviation in rates of task scheduling from normal rates due to disturbance in network traffic. This approach transforms industrial controllers into integrated security modules for the early detection of cyberattacks.

Security challenges related to detecting anomalies in huge process data of Industrial Control Systems (ICS) have been discussed by X. Clotet *et al*. [20]. Their work proposes an algorithm for an Intrusion Detection System (IDS) based on learning the attributes of normal process data and using this as a base for separating anomalies. X. Jie *et al*. [21] have proposed a model for detecting abnormal behavior of a control system using data mining and association rules. The detection of attacks calculates reliability based on the time taken.

Another challenge is to secure communication in ICS. A survey by Y. Yang *et al*. [22] has suggested privacy issues and security for IoT networks. In an asymmetric cryptosystem, the key is transmitted along with the message. Eavesdropping can compromise key information and sensitive data. Pramod T. C. *et al*. [23] have proposed a model for the pre-distribution of secret keys to secure communication in a SCADA-based system. Each device's secret key is locally computed in the proposed scheme whenever it receives an instruction for the key update, join or leave operation. This approach provides high resilience to key exposure.

### *B. Emerging Technologies for IoT Security*

This section discusses the literature on potential technologies to secure the IoT environment. We review work related to security mechanisms having conventional and emerging approaches. We also analyze literature focused on improving detection and security countermeasures to fulfill security objectives.

I. Farris *et al*. [24] present an analysis of the scope of Software Defined Networks (SDN) and Network Function Virtualization (NFV) technologies as complementary to conventional IoT security solutions. SDN works to provide end-to-end protection in CPS. It is not feasible for system users to make security configurations of every device on the network separately. NFV enables decoupling software from hardware by configuring security requirements to devices through firewalls and Deep Packet Inspectors (DPI). The role of the SDN controller is to manage traffic flow. SDN's security mechanisms are virtual platforms like vIDS, vDPI, and firewalls. This enables the scalability of network and processing resources corresponding to how much data traffic and connected IoT devices are present. This improves their energy efficiency, on-demand network programmability, mobility support, and flexibility.

S. Yu *et al*. [25] have proposed a Blockchain platform that can allow the transfer of data from intelligent devices efficiently in IoT. This paper has compared the performance of IoT based on blockchain with that of cryptocurrency and shown that in their design, efficiency and throughput have increased while latency is lowered. The results favor the integration of Blockchain with IoT applications.

M. Singh *et al*. [26] have discussed how blockchain works and its architecture in IoT networks. They elaborate on how IoT security can be strengthened by blockchain. This paper suggests that the Blockchain security model can provide secure communication using asymmetric cryptography and public keys storing ledger. Another security feature is the authentication of users and digital signatures. It also provides integrity and data confidentiality. D. Fakhri and K. Mutijarsa [27] have demonstrated experimentally that IoT communication using Blockchain is more secure than in the absence of blockchain. Simulated attacks were used in this study to observe the resilience of encryption algorithms in resolving security issues like integrity.

K. Elbehiery and H. Elbehiery [28] have proposed using 5G as a service for IoT applications, especially in large-scale enterprises. They have compared various cloud-based 5G edge architectures, which provide low costs and business agility. 5GIoT architecture enables the speedy transformation of critical IT systems for banking, manufacturing, and other industries. It gives the advantage of cost optimization, consistent security, compliance with standards, and simplified automation and monitoring of IoT applications.

D. Wang *et al*. [29] have suggested using 5G in IoT to expand the coverage of many sensors. This work has classified 5G in IoT into three components and discussed the interrelation using big data processing techniques. It has shown experimental results that the performance of 5G communication will benefit the capacity of IoT applications. P. Kiss *et al*. [30] have discussed possible solutions to use edge computing to gain maximum benefits of 5G technologies in IoT. Edge computing will reduce overheads in communication and build trusted IoT services with reliability. It deploys cloud servers closely located to the edge devices to reduce the computation burden and manage security. Regarding IoT security, edge computing and network slicing have security concerns like design and authentication.

S. Paliwal and S. O. Hasan [31] have derived those factors which make 5G technology beneficial to the IoT environment. The identified factors can quantitatively and qualitatively drive the growth and success of IoT. Other determinants less influence some factors. Such factors are called independent and can be harnessed to deploy the benefits of 5G to IoT. Results show that high bandwidth is a driving factor. Virtual latency is zero, and entire network coverage is also achieved.

Significantly, various challenges and limitations related to the implementation of IoT are taken into consideration by researchers, such as latency, power management, scalability, performance and throughput, interoperability, standardization, reliability, and cybersecurity.

### *C. Industrial IoT Security Solutions*

The cybersecurity challenges in critical infrastructures have increased in the IoT environment since online devices. For implementing IoT, researchers have to focus on addressing multiple challenges related to architecture, technology, hardware, standards, business, and security and privacy [32].

Research has highlighted that assessing attacks and vulnerabilities in system architecture is key to efficient cybersecurity management.

- N. R. Rodofile *et al*. [33] have presented a complete framework of cyberattacks in entire SCADA-based architecture for critical infrastructures. The work describes the range of attacks into four categories related to IT system, protocol, configuration, and control process.
- G. Falco *et al*. [34] have analyzed the risk to SCADA system in IIoT application using statistical methods. SCADA systems run on the Windows operating system, and a challenge exists to connect SCADA online in IIoT securely. They developed prioritization of SCADA-related vulnerability exploitation risk to identify risk metrics of the heterogeneous IIoT system.

To demonstrate IIoT security solutions in critical infrastructures, most of the research is based on specific domain area use cases, for example, smart grids.

- K. Kimani *et a*l. [35] have identified security as a critical factor of consideration before deciding on large-scale deployment of IoT devices in smart grids. The vulnerability of smart grids based on IoT increases manifolds compared to the ordinary grid network.
- To ascertain the sustainability of smart grids, B. Mohandes *et al*. [36] have analyzed the security and reliability challenges in smart grids. It proposes a comprehensive approach based on disseminating issues at the level of the physical device layer, network control layer, and Information and Communication Technology (ICT) layer.
- U. B. Baloglu and Y. Demir [37] have proposed a scheme for data aggregation using encryption and perturbation techniques to secure the privacy of communication in smart grid metering infrastructure, suggesting it is better than previously developed aggregation solutions.
- K. Demir *et al*. [38] have proposed Hierarchical Hybrid Cloud-Extension Concept (HHCEC) for a smart grid. In case one or more servers are attacked, replica servers can become active without interrupting the rest of the traffic since it utilizes the quick elasticity feature of the cloud. This approach improves availability against Denial-of-Service (DDoS) attacks with a negligible tradeoff on latency requirements.

Security objectives and criticalities of industrial processes are important concerns in IIoT security research.

- M. S. Varalakshmi [39] has discussed various security factors for the cyber-physical system to design a multilevel security solution for CPS. The proposed multilevel security provides availability, confidentiality, authentication, and data integrity. It protects the critical infrastructure corresponding to each function of CPS, such as data sensing, actuation, monitoring, and storage. The concept of multilevel security uses essential restrictions at each level and hierarchy to control access. It provides authentication for data sensing, security protocols for the communication channel, authorization for device actuation, and information security of stored data, all

depending on the security hierarchy levels.

- L. Russell *et al*. [40] have developed an agile IoT sensing solution for adding situational awareness in sensors deployed for critical infrastructure. This work implements an algorithm for a given sensor to measure another variable that was not originally designed without requiring any new hardware. This approach improves resilience and makes the system more robust to failures by examining alternative communications.

Some research works have proposed compliance models to deal with the challenges of business and security standards.

- R. Leszczyna [41] has discussed various industry standards for cybersecurity management of industrial applications. Guidelines on standards compliance of cybersecurity controls for smart grids application are discussed in [42]. The author has proposed a framework for selecting appropriate standards and evaluation criteria.
- D. Makupi and N. Masese [43] have designed a model to assess organizations' information security maturity levels that follow the standard ISO/IEC 27001 to fulfill their security objectives. Based on this model, an organization can be distinguished into either full or acceptable or basic or initial compliance or no compliance with IT security standards.

Another focus area of research is to deal with technology and security challenges in deploying Industrial IoT applications.

- Al-Rubaye *et al*. [44] have proposed an SDN platform for the IIoT model in smart grids to respond quickly to failures in real-time. It uses an SDN switch segment for data processing at the local network level while traffic flow is monitored by an SDN controller in the IIoT infrastructure. The experimental simulation results show that the reliability and resiliency of smart grid networks can increase.
- K. Hajri *et al.* [45] have highlighted IoT use cases with 5G services in the oil and gas industry. 5G brings advantages of high bandwidth, speed, and low latency, which are highly desirable in critical IoT processes and their security needs, such as smart surveillance. It has protocols and standards to eliminate cybersecurity threats through preventative controls in the service design phase.
- Lakshwanth Prasad K *et al*. [46] have proposed using redactable blockchain technology for the IIoT environment. This security solution provides restoration to the blockchain if there has been an attack. This architecture has reduced security challenges unless an attacker possesses huge resources to breach the complex blockchain. However, high-level mining is required at each transaction execution to validate the blocks leading to a tradeoff between blockchain security and usability features in an IoT environment.

## III. IIOT CHALLENGES FOR INDUSTRIAL AUTOMATION AND CONTROL

In the present era of Industry 4.0, one of the most sought system goals is automation and control. IACS is used commonly in critical infrastructures for remote and distributed operations in a complex System-of-Systems architecture. The collective objective is to achieve: Efficiency and Ease of operations. However, with the adoption of IoT, the issue of sustainability has gained concern with security as one of the factors.

Firstly, realizing IoT-based Cyber-Physical Systems poses three technological challenges: Computation, Communication, and Compatibility [47].

- Extensive computation is at local end devices, for automation and control and remote computation of process data, often big data, for business analytics.
- The flow of related process information on the internet increases extensive communication requirements.
- For heterogeneous devices and systems to connect, protocol compatibility is required.

Secondly, IACS implementation has two limiting factors in critical infrastructure sectors: Reliability and resilience [48].

- Reliability in terms of uninterrupted and safe operations to fulfill important needs of public socio-economic utilities.
- Resiliency in terms of protection of critical information against cyberattacks.

With this background, there is a need to analyze how much effort is required to operate critical information infrastructures in an IoT environment corresponding to the attributes described above: Computation; Communication; Compatibility; Reliability; and Resiliency. For transformation of IACS in an IoT environment, it may need cybersecurity considerations such as:

- Whether IoT technology again offers these attributes or exposes vulnerabilities for exploitation by cyber attackers or both [49]?
- What measures and practices can control the consequences of IoT implementation on the cybersecurity of critical infrastructures [50]?

## IV. CYBERSECURITY CONSIDERATIONS FOR IACS

This section perceives the range of attack landscapes in IACS and focuses on three cybersecurity considerations for businesses to implement their IoT plan. The aim is to systematically motivate the industry to use IoT applications in critical infrastructures securely.

### *A. Prioritization of Security Objectives*

The information involved in the processes is critical and needs to be protected on the "CIA" scale: Confidentiality, Integrity, Availability, authentication, and authorization [51]. Based on the literature review on cybersecurity challenges

for IIoT in critical infrastructures (Section II.A) and their security solutions (Section II.C), the prioritization of security objectives for IACS could be done as below:

***a) Availability***

From [19]–[21], [36], [38], [40], it is suggestive that amongst the security objectives, system availability has the most priority to ensure the reliability of IACS. Availability of ICS is crucial for the continued operation of a critical infrastructure industry [52]. Availability may be threatened by attacks like DoS, DDoS, hacking, ransomware, etc.

***b) Authentication and Authorization***

From [10], [17], [26], [34], [36], [39] it is observable that authentication of source and authorization based on policy rules is vital to stop intrusions like DoS, IP spoofing, hacking, etc. In [22], authentication is a crucial step for information security and privacy from illegitimate users in IoT-based infrastructure.

***c) Confidentiality***

It is observed from [23], [32], [37], [41] that for secure communication, confidentiality is an important security objective. Break-in confidentiality can have adverse implications in processes related to some sectors like defense, nuclear, telecommunication, and government facilities where process data requires secrecy. In processes like automation of health infrastructure, information-carrying patients' data will require privacy. Confidentiality may be threatened by Man-in-the-Middle attacks, sniffing, eavesdropping, cyber espionage, etc., leading to data or identity theft.

***d) Integrity***

Literature for addressing integrity goals in cybersecurity of critical infrastructure are few like [24], [27]. Integrity is needed not to manipulate data by intruders, causing probable malfunctioning or loss of legitimate information. Information integrity and confidentiality are complementary objectives in processes like banking, healthcare, and government facilities. Even when confidentiality is assured, a breach of data integrity can have an indirect adverse bearing on the availability of critical information [46]. More research focus is needed on integrity as a security objective of IIoT.

***B. Selection of Security Standards***

Security standards are considered for designing IIoT security solutions to fulfill the security objectives [41]–[43]. The regulatory standards for IoT systems differ depending on the industrial segment they guide and their design objectives [53]. To protect the information in critical infrastructures, the existing cyber security practices should follow standards that address the IoT cyber risks [54]. Table 2 depicts the cybersecurity countermeasures and cybersecurity management system practices addressed by the security standards [42].

**Table 2. Cybersecurity standards applicable to IACS [42]**

| **Standards** | **'ISA/IEC 62443'** | **'ISO/IEC 27019'** | **'NIST SP 800-82'** | **ISO 27001, 27002 (General standards)** |
|---|---|---|---|---|
| **Cybersecurity countermeasures** | Filtering, blocking, & Access control. | Access control. | Access control. | Access control. |
| | Authentication Authorisation | | Identification & Authentication | |
| | Encryption & data validation | | System and communications protection | |
| | | | System Information Integrity | |
| | Physical Security control | Physical and Environmental security | Physical and environmental protection | Physical and environmental security |
| | Monitoring & Detection tools | | | |
| **Cyber Security Management System (CSMS)** | Management | Information security incident management. | Incident response | Information security incident management. |
| | | Security Policy | Security assessment | Security Policy |
| | | The organization of Information Security. | Security planning | The organization of Information Security. |
| | | Asset management | Risk assessment | Risk assessment |
| | Auditing | Compliance | Audit and accountability | Compliance |

A comparison of standards relevant to IACS has been represented here to identify those security requirements where the standards overlap each other; where the standards are complementary; where the standard addresses any unique security requirement not present in other standards; where application-specific standards are available, and where generic standards can be adopted.

***a) ISA/IEC 62443 series***

It addresses the cybersecurity of IACS. IEC-62443-2-1 standard describes the process of developing an IACS-security management system. Other versions define security mechanisms and techniques for protecting IACS.

***b) ISO/IEC 27019***

It contains Cyber Security Management System (CSMS) guidelines derived from ISO/IEC 27002 for IACS process control. It may direct to general standards ISO/IEC27001 & 27002 to be cross-referred for further guidance. It provides additional IACS-specific indications, and some new controls are also defined, particularly for IACS

***c) NIST SP 800-82***

It is the regional standard dealing with IACS cybersecurity. It gives guidelines for network systems like DCS, SCADA, and PLCs.

***d) ISO/IEC 27001 & 27002***

These are general standards on information security. Here the system information may not necessarily be exposed to the internet. ISO/IEC27001 specifies best practices for implementing Information Security Management System (ISMS) during its complete life cycle. ISO/IEC 27002 describes measures for ISMS implementation.

***C. Selection of Emerging Technologies for IIoT Security***

The use of emerging IT technologies can address IoT security challenges. an early plan and design of IoT products, besides other preventive mechanisms, is considered useful by researchers for effective cybersecurity solutions [55]. From our literature review, the following technologies have been identified as potential considerations for IIoT security by design:

***a) Software Defined Networks (SDN)***

SDN, along with Network Functions Virtualization (NFV), is an enabling technology with many advantages for decentralized yet connected heterogeneous IoT ecosystems [44]. It primarily manages the data traffic flow. To reconfigure the network, it offers robustness and reliability through virtual features like firewalls, vIDS, vProxy, etc. SDN can define the network by SDN controller whose high computational power increases scalability and flexibility [24].

***b) 5G Technology***

The demand for real-time wireless communication with high speed and capacity offered by the internet is ever increasing in IIoT. Many connectivity technology enablers for IoT, such as Ethernet-based or wireless or cellular communication [56]. In this direction, 5G Cellular, or the 5th generation mobile technology, will boost the technological improvement of IoT as per predictions. 5G internet network may have speed capabilities as high as 10Gbps with lowered latency. It can encompass enormous network traffic in an IoT environment [29].

***c) Blockchain Technology***

Blockchain emerged from the regime of cryptocurrency a few years back. It records transactions on a network, public or private, in the form of a chain using the cryptographic technique hashing. The main elements in each block are the message hash tree, the previous block's hash, and the timestamp of the recorded transaction. Each block is unique and unalterable unless the whole network agrees to modification [46]. This process consumes extra energy. Any block of this chain is available for open access in-network for verification [26].

These emerging technologies are considered to compare their advantages and tradeoffs to derive their potential for integration in the IoT environment: SDN with NFV, 5G technology, and Blockchain technology. Their implications on cybersecurity requirements are mapped in Table 3.

**Table 3. Mapping of enabling technologies with cybersecurity features**

| Enabling Technology | Feature Attributes | Security Implications | Security Features |
|---|---|---|---|
| SDN | +Scalability, +Flexibility<br>+Energy efficiency<br>+Interoperability | +End-to-End protection<br>+Reliability, +Resilience | vIDS, firewall<br>vProxy |
| NFV | +Flexibility | +Efficiency | Virtual Security configuration |
| 5G Technology | +High bandwidth +efficiency<br>+energy performance<br>+low latency, +Scalability | + availability<br>- Authentication<br>- Privacy | Edge computing |
| Blockchain | + Scalability, + Efficiency<br>+Low latency | +privacy, +Integrity<br>+Authentication | Hash functions |

## V. RESULTS AND DISCUSSION

Based on our literature review, three cybersecurity considerations were identified related to security objectives, standards, and enabling technologies for IIoT security. Alternative solutions for each of these considerations are analyzed from the perspective of an IACS.

The first cybersecurity consideration is to prioritize those security objectives that need to be fulfilled by using suitable hardware or software.

- To ensure the availability of IACS, we require efficient monitoring and detection tools that can monitor and manage network and end devices.
- For authentication, we need improvised IDS techniques. For authorization, role-based access control can be assigned. In CPS, security measures focus on anomalies or intrusion detection and early detection and isolation through various algorithms or additional hardware.
- To assure confidentiality, the latest encryption techniques should be incorporated. Key management is a vital requirement in an IoT environment where millions of nodes are set to communicate over the internet. Architecture for key generation, storage, and distribution over the network has scope for improving security.
- System information integrity can be ensured using secure communication protocols and data validation techniques.

The second cybersecurity consideration is to identify the suitable cybersecurity standards for IIoT. It comprises adaptation to generic as well as dedicated standards. When dedicated standards are not yet available for any IIoT area, the existing standards, which are not domain-specific, can be directly adapted for information security, especially CSMS practices. For the seamless transition to IoT in IACS, the following combination of standards are suggested:

- ISO/IEC 27019 is a dedicated IACS cybersecurity standard accepted worldwide which defines controls for CSMS practices and should be directly referred by the cybersecurity team for adherence; however, some reference to general information security standards IEC 27001 & 27002 is made for controls when directed by IEC 270019.
- Another IACS-specific standard is the ISA/IEC 62443 series, which guides the IACS security program for CSMS and defines security mechanisms (access control, authentication, encryption, data validation, monitoring, and detection tools), their technical implementation, and auditing.

The third cybersecurity consideration is identifying enabling IT technologies that can also overcome IIoT security challenges. From Table 3, we can observe that most of the enabling technologies come with the added advantage of cybersecurity. However, in a few areas, there are negatives.

- There is a positive security implication of SDN technology. It offers End-to-End protection with improved reliability and resilience to failures or attacks by implementing security features like virtual IDS and Firewall. It suffers from the rise in latency due to additional payload. NFV enables the security configuration of devices on the network using the software.
- The recent development of 5G technology will enable the huge data traffic on the internet with high speeds; however, it will make it more difficult to separate threats in the crowd. High speed will imply quicker attacks with less time to rectify.
- Blockchain technology is more focused on positive security implementations. It enables a trusted IIoT environment in critical infrastructures like banking and government facilities where transactions must be immutable.

The proposed cybersecurity considerations are based on prioritizing security objectives, studying relevant standards, and mapping enabling technologies to cybersecurity implications. This approach addresses cybersecurity before deploying Industrial automation and control systems in IoT environments. The proposed work will help organize relevant information for security assessment in the critical infrastructure business planning process and gain concerned stakeholders' confidence.

## VI. CONCLUSION

IoT-led technological changes are driving digital transformation in critical infrastructures. It involves important decision-making for the design and deployment of Industrial IoT. However, recent research trends highlight the need for cybersecurity considerations in decision-making. The proposed cybersecurity considerations for IACS can be useful in multidisciplinary critical infrastructure sectors such as critical manufacturing, power generation, and water processing plants. IoT transformation to strategic sectors such as defense, telecommunication, banking, and Government facilities that are critical infrastructures and have critical information need extended security considerations.

This paper provides an integrated approach to developing critical information infrastructure in an Industrial IoT environment. In IACS-based infrastructures, depending on the business or social interest, the stakeholders need to identify appropriate security standards and controls and make selective tradeoffs in security considerations for IIoT. For transforming the otherwise isolated industrial processes into a secured IoT environment, the cybersecurity features need to be balanced with computation, communication, interoperability, efficiency, and reliability by leveraging emerging IT technologies.

## ACKNOWLEDGMENT

The author is thankful for the research guidance and support received from the Department of Computer Science & Engineering, Jamia Hamdard University, New Delhi, as part of their postgraduate degree program, which was helpful in taking up this study. The author has received insight and expertise in the related areas of this study from a previous work association with Aravali Power Company Private Limited, Jhajjar, India, which greatly assisted the research.

## REFERENCES

[1] Sreedevi T. R., Internet of Things: A Survey of Iot Applications Based on Their Desirable Device Characteristics, Int. J. of Recent Engineering Research and Development. 02(10) (2017) 10-20.

[2] S.O. Muhanji, A.E. Flint and A.M. Farid, The Development of Iot Within Energy Infrastructure, In Iot, 1st Ed., Cham, Germany: Springer. (2019) 27-90.

[3] T. Lynn, P. T. Endo, AMNC Ribeiro, G.B.N. Barbosa, and P. Rosati, The Internet of Things: Definitions, Key Concepts, and Reference Architectures, In The Cloud-To-Thing Continuum, 1st Ed., T. Lynn, J. Mooney, B. Lee, P. Endo, Eds., Ser. Palgrave Studies In Digital Business & Enabling Technologies. Cham, Germany: Palgrave Macmillan. (2020) 1-22.

[4] (2017) Internet of Things Outlook, The Ericsson Mobility Report. [Online]. Available: Https://Www.Ericsson.Com/En/Mobility-Report/Internet-of-Things-Outlook.

[5] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications, IEEE Communication Survey & Tutorials, 17(4) (2015) 2347–2376.

[6] S. Mittal, M. A. Khan, and T. Wuest, Smart Manufacturing: Characteristics and Technologies, In Product Lifecycle Management For Digital Transformation of Industries, 1st Ed., R. Harik, L. Rivest, A. Bernard, B. Eynard, A. Bouras, Eds., Ser. IFIP Advances In Information and Communication Technology. Cham, Germany: Springer. 492 (2016) 539-548.

[7] R. Nicolescu, M. Huth, P. Radanliev and D. De Roure, Mapping The Values of Iot, J. of Information Technology, 33(4) (2018) 345-360.

[8] V. Moulos, G. Chatzikyriakos, V. Kassouras, A. Doulamis, N. Doulamis, G. Leventakis, T. Florakis, T. Varvarigou, E. Mitsokapas, G. Kioumourtzis, P. Klirodetis, A. Psychas, A. Marinakis, T. Sfetsos, A. Koniaris, D. Liapis and A. Gatzioura, A Robust Information Life Cycle Management Framework For Securing and Governing Critical Infrastructure Systems, Inventions, 3(4) (2018) 71-109.

[9] A. B. Pawar and S. Ghumbre, A Survey on Iot Applications, Security Challenges, and Countermeasures, In Proc. Int. Conf. on Computing, Analytics, and Security Trends, Pune, India, Paper (2016) 294-299.

[10] G. Stergiopoulos, V. Kouktzoglou, M. Theocharidou and D. Gritzali, A Process-Based Dependency Risk Analysis Methodology For Critical Infrastructure, Int.J. of Critical Infrastructures, 13(2/3) (2017)184-205

[11] M. Ghita, B. Siham, M. Hicham, *Et Al*., Digital Twins: Development and Implementation Challenges Within Moroccan Context, SN Applied Sciences, 2(5) (2020) 885.

[12] S. Walker-Roberts, M. Hammoudeh, O. Aldabbas, *Et Al*., Threats on The Horizon: Understanding Security Threats In The Era of Cyber-Physical Systems, The J. of Supercomputing, 76 (2020) 2643–2664.

[13] Q. Qassim, N. Jamil, M. Daud, and H. Hasan, Towards Implementing Scalable and Reconfigurable SCADA Security Testbed In The Power System Environment, Int. J. of Critical Infrastructures, 15(2) (2019) 91-120.

[14] V. S. Kumar, J. Prasad, and R. Samikannu, A Critical Review of Cyber Security and Cyber Terrorism - Threats To Critical Infrastructure In The Energy Sector, Int. J. of Critical Infrastructures, 14(2) (2018) 101-119.

[15] I. Kozine, B. Petrenj, and P. Trucco, Resilience Capacities Assessment For Critical Infrastructures Disruption: The READ Framework (Part 1), Int. J. of Critical Infrastructures, 14(3) (2018) 199-220.

[16] J. Jansen and A. Van Der Merwe, A Framework For Industrial Internet of Things, In Responsible Design, Implementation and Use of Information and Communication Technology, 1st Ed., M. Hattingh, M. Matthee, H. Smuts, I. Pappas, Y. Dwivedi, M. Mäntymäki, Eds., Ser. Lecture Notes In Computer Science. Cham, Germany: Springer. 12066 (2020) 138-150.

[17] N. Skandhakumar, J. Reid, F. Salim and Ed Dawson, A Policy Model For Access Control Using Building Information Models, Int. J. of Critical Infrastructure Protection, 23 (2018) 1-10.

[18] N. Wallace, T. Atkison, on The Detection of Cyber-Events In The Grid Using PCA, Int. J. of Critical Infrastructures, 13(2/3) (2017) 96-112.

[19] P. Haller, B. Genge, and Adrian-Vasile Duka, on The Practical Integration of Anomaly Detection Techniques In Industrial Control Applications, Int. J. of Critical Infrastructure Protection, 24 (2019) 48–68.

[20] X. Clotet, J. Moyano, and G. Leon, A Real-Time Anomaly-Based IDS For Cyber-Attack Detection At The Industrial Process Level of Critical Infrastructures, Int. J. of Critical Infrastructure Protection, 23 (2018) 11-20.

[21] X. Jie, H. Wang, M. Fei, D. Du, Q. Sun and T.C. Yang, Anomaly Behavior Detection and Reliability Assessment of Control Systems Based on Association Rule, Int. J. of Critical Infrastructure Protection, 22 (2018) 90-99.

[22] Y. Yang, L. Wu, G. Yin, L. Li, and H. Zhao, A Survey on Security and Privacy Issues In Internet-of-Things, IEEE Internet of Things Journal, 4(5) (2017) 1250-1258.

[23] Pramod T. C., Kianoosh G. Boroojeni, M. Hadi Amini, N.R. Sunitha and S.S. Iyengar, Key Pre-Distribution Scheme With Join Leave Support For A SCADA System, Int. J. of Critical Infrastructure Protection, 24 (2019) 111-125.

[24] I. Farris, T. Taleb, Y. Khettab, and J. Song, A Survey on Emerging SDN and NFV Security Mechanisms For Iot Systems, IEEE Communication Survey & Tutorials, 21(1) (2019) 812–837.

[25] S. Yu, K. Lv, Z. Shao, Y. Guo, J. Zou and B. Zhang, A High-Performance Blockchain Platform For Intelligent Devices, In Proc. 2018 1st IEEE Int. Conf. on Hot Information-Centric Networking (Hoticn), Shenzhen, Paper (2018) 260-261.

[26] M. Singh, A. Singh, and S. Kim, Blockchain: A Game-Changer For Securing Iot Data, In Proc. 2018 IEEE 4th World Forum on Internet of Things (WF-Iot), Singapore, Paper (2018) 51-55.

[27] D. Fakhri and K. Mutijarsa, Secure Iot Communication Using Blockchain Technology, In Proc. 2018 International Symposium on Electronics and Smart Devices (ISESD), Bandung, Paper (2018) 1-6.

[28] K. Elbehiery and H. Elbehiery, 5G as A Service (5gaas), SSRG Int. J. of Electronics and Communication Engineering, 6(8) (2019) 22-30.

[29] D. Wang, D. Chen, B. Song, N. Guizani, X. Yu and X. Du, From Iot To 5G I-Iot: The Next Generation Iot-Based Intelligent Algorithms and 5G Technologies, IEEE Communications Magazine, 56(10) (2018) 114-120.

[30] P. Kiss, A. Reale, C. J. Ferrari, and Z. Hestenes, Deployment of Iot Applications on 5G Edge, In Proc. 2018 IEEE Int. Conf. on Future Iot Technologies (Future Iot), Eger Hungary, Paper (2018) 1-9.

[31] S. Paliwal and S. O. Hasan, 5G as The Principal Enabler Towards The Establishment of 'Iot' Society, In Proc. Int. Conf. on I-SMAC (Iot In Social, Mobile, Analytics, and Cloud), Palladam, Paper (2017) 16-21.

[32] G. Begum, M. Ramabai and M. C. Mohan, Challenges and Concerns of Privacy In Internet of Things, SSRG Int. J. of Computer Science and Engineering, 3(2) (2016) 28-33.

[33] N. R. Rodofile, K. Radke and E. Foo Extending The Cyber-Attack Landscape For SCADA-Based Critical Infrastructure, Int. J. of Critical Infrastructure Protection, 25 (2019) 14-35.

[34] G. Falco, C. Caldera, and H. Shrobe, Iiot Cybersecurity Risk Modelling For SCADA Systems, IEEE Internet of Things Journal, 5(6) (2018) 4486-4495.

[35] K. Kimani, V. Oduol and K. Langat, Cyber Security Challenges For Iot-Based Smart Grid Networks, Int. J. of Critical Infrastructure Protection, 25 (2019) 36-49.
[36] B. Mohandes, R. Al Hammadi, W. Sanusi, T. Mezher and S. El-Khatib, Advancing Cyber-Physical Sustainability Through Integrated Analysis of Smart Power Systems: A Case Study on an Electric Vehicle, Int. J. of Critical Infrastructure Protection, 23 (2018) 33-48.
[37] U. B. Baloglu and Y. Demir, Lightweight Privacy-Preserving Data Aggregation Scheme For Smart Grid Metering Infrastructure Protection, Int. J. of Critical Infrastructure Protection, 22 (2018) 16-24.
[38] K. Demir, H. Ismail, T. Vateva-Gurova and N. Suri, Securing The Cloud-Assisted Smart Grid, Int. J. of Critical Infrastructure Protection, 23 (2018) 100-111.
[39] M. S. Varalakshmi, an Introduction To Multilevel Security In Cyber-Physical Systems, SSRG Int. J. of Computer Science and Engineering, 4(7) (2017) 26-29.
[40] L. Russell, R. Goubran, F. Kwamena, and F. Knoefel, Agile Iot For Critical Infrastructure Resilience: Cross-Modal Sensing as Part of A Situational Awareness Approach, IEEE Internet of Things Journal, 5(6) (2018) 4454- 4465.
[41] R. Leszczyna, Cybersecurity and Privacy In Standards For Smart Grids – A Comprehensive Survey, Computer Standards & Interfaces, 56 (2018) 62-73.
[42] R. Leszczyna, Standards with cybersecurity controls for smart grid – A systematic analysis, Int. J. of Communication Systems, 32(6) (2019) e3910.
[43] D. Makupi and N. Masese, Determining Information Security Maturity Level of an organization based on ISO 27001, SSRG Int. J. of Computer Science and Engineering, 6(7) (2019) 5-11.
[44] Al-Rubaye, E. Kadhum, Q. Ni and A. Anpalagan, Industrial Internet of Things Driven by SDN Platform for Smart Grid Resiliency, IEEE Internet of Things Journal, 6(1) (2019) 267-277.
[45] K. Hajri, A. Sowailem, S. Shahrani, and M. Yami, 5G Deployment in the Oil and Gas Industry, SSRG Int. J. of Industrial Engineering, 8(2) (2021) 13-15.
[46] Lakshwanth Prasad K, Bhuvanesh H, Vasanth S and Subramaniam M, Consortium Blockchain for Certificateless Signatureless Scheme in Industrial IOT Environments, SSRG - SCA-2020, (2020) 60-64.
[47] S. Alam, M.M.R. Chowdhury, and J. Noll, Interoperability of security-enabled Internet of Things, Wireless Personal Communications, 61 (2011) 567–586.
[48] S. J. Moore, C.D. Nugent, S. Zhang, *et al*., IoT reliability: a review leads to 5 key research directions, CCF Transactions on Pervasive Computing and Interaction, 2(3) (2020) 147–163.
[49] S. Cheruvu, A. Kumar, N. Smith and D. M. Wheeler, IoT Frameworks and Complexity, in Demystifying Internet of Things Security, 1st ed., Berkeley, CA: Apress. (2020) 23-148.
[50] A. Jurcut, T. Niculcea, P. Ranaweera, *et al*., Security Considerations for Internet of Things: A Survey, SN Computer Science, 1(4) (2020) 193.
[51] S. Cheruvu, A. Kumar, N. Smith and D. M. Wheeler, IoT Software Security Building Blocks, in Demystifying Internet of Things Security, 1st ed., Berkeley, CA: Apress. (2020) 213-346.
[52] (2013) Mitigating attacks on Industrial Control Systems (ICS); the new Guide from EU Agency ENISA. [Online]. Available: https://www.enisa.europa.eu/ news/enisa-news/mitigating-attacks-on-industrial-control-systems-the-new-guide-from-enisa
[53] S. Cheruvu, A. Kumar, N. Smith and D. M. Wheeler, IoT Vertical Applications and Associated Security Requirements, in Demystifying Internet of Things Security, 1st ed., Berkeley, CA: Apress. (2020) 413-462.
[54] P. Radanliev, D. C. De Roure, J. R. C. Nurse, *et al*., Future developments in standardization of cyber risk in the Internet of Things (IoT), SN Applied Sciences, 2(2) (2020) 169.
[55] K. Kandasamy, S. Srinivas, K. Achuthan, *et al*., IoT cyber risk: a holistic analysis of cyber risk assessment frameworks, risk vectors, and risk ranking process, EURASIP J. on Information Security (2020)8.
[56] S. Cheruvu, A. Kumar, N. Smith and D. M. Wheeler, Connectivity Technologies for IoT, in Demystifying Internet of Things Security, 1st ed., Berkeley, CA: Apress. (2020) 347-411.