This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3057766, IEEE Access

IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Date of publication xxxx 00, 0000, date of current version xxxx 00, 0000.

Digital Object Identifier 10.1109/ACCESS.2017.DOI

A Taxonomy of Security Issues in Industrial Internet-of-Things: Scoping Review for Existing Solutions, Future Implications, and Research Challenges

PLS JAYALAXMI[1], , RAHUL SAHA [1] (MEMBER, IEEE), GULSHAN KUMAR [1] (MEMBER, IEEE), NEERAJ KUMAR[2] (SENIOR MEMBER, IEEE), TAI-HOON KIM[3] (MEMBER, IEEE)

[1]School of Computer Science and Engineering, Lovely Professional University, Punjab, India
[2]Department of Computer Science and Engineering, Thapar University, Punjab, India
[3]Glocal Campus, Konkuk University, 268 Chungwon-daero Chungju-si Chungcheongbuk-do, 27478, South Korea

Corresponding author: Rahul Saha (e-mail: rsahaaot@gmail.com), Tai-Hoon Kim (e-mail: taihoonn@daum.net).

ABSTRACT Industrial Internet of Things (IIoTs) are the extensions of the Internet of Things (IoTs) and have paved the way towards the industry revolution 4.0. IIoT accelerates the industry automation of internal and external working process including transport, manufacturing, and marketing units with a number of connected devices. Being the extension of IoT, it inherits the insecurities of the technology; however, this sensor-configured infrastructure of IIoT needs some extra effort to customize the existing security solutions. In spite of the reconstructions of security models, the scope of improved developments is open to detect unknown attacks. The present study helps the researchers to understand the cause for intrusion by classifying and comparing various attacks of each IIoT layers. The main focus of this survey is to analyze various security issues faced by IIoT and provide a comparative analysis on the available solutions to enhance the industrial IoTs' protection systems. This study also notifies some open research problems for academia, technologists, and researchers to flourish the IIoT domain and its security aspects.

INDEX TERMS Security, Industrial, IoT, Internet, Intrusion, Detection

I. INTRODUCTION

Internet-of-Thing (IoT) has created the changeover from the digital world to a smart connected world by establishing an end-to-end communication with automated services and minimizing human intervention. The growth of artificial intelligence and communication technologies has enabled a real-time optimization in industry processes [1]. Initially, digitization has been focused on operational optimization and efficiency in automated maintenance for water and steam-powered mechanical manufacturing. It is then followed by the deployment of electronic and Information Technology (IT) based production systems [2]. Industry 4.0 has generated a severe positive impact by incorporating IoT in every domain of industrial developments. Thus, Industrial Internet-of-Thing (IIoT) has smoothen up the smart startups for transportation, resource management, manufacturing, energy renewable resources, and the development of smart cities, etc. The various advancements in smart manufacturing units have grabbed unpredictable attention for the last decade. Most of the popular IIoT applications include digital/connected factory, automatic production flow management, industrial security systems, industrial configuration alerts and maintenance safety, and health (conditions) monitoring of workers and many more [1] [2].

The entire IIoT process is implemented with the key element of Cyber-Physical System (CPS). CPS is used to control and coordinate physical activities, enable conditional monitoring, structural health checking, remote diagnosis, and dynamic control of production systems in real-time. Still, there is a possibility of insecure environment for digital communication as the number of devices connecting with IIoT is increasing everyday. Smart factories consist of multiple Cyber-Physical Production Systems (CPPS), an integrated component of hardware, software, and communication devices; each layer is vulnerable to cyber-attacks. For example, electronic and hardware devices are prone to face

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3057766, IEEE Access

side-channel and reverse-engineering attacks. The software components can be vulnerable with malicious codes such as trojans, viruses, and runtime attacks. The communication channels are vulnerable subject to network protocol attacks, man-in-the-middle, and denial-of-service attacks [3]. Finally, manual CPPS is affected by social attacks such as phishing, spamming, and social engineering. Existing security solutions are becoming insufficient as heterogeneous devices and networks are increasing with the popularity of IIoTs [4].

To establish a secured automatic operation and avoid intermediate intrusions, a strong security system is required in IIoT. The aim of the industrial production system is availability (to prevent unnecessary delay in production and protect from Denial of Service (DoS) based attacks against CPS). Moreover, the integrity of IIoT to avoid physical damage by raising protection against sabotage attacks (which cause low quality and high usage of resources) is also a goal of security provisioning in IIoTs. Avoidance of unauthorized access or unintentional use of industrial components, maintaining authenticity and integrity for third parties' operations come along with the security requirements of IIoTs. Sustaining confidentiality for customer and employee information by protecting industrial intelligence code, data, and configuration of production systems (blueprint of the products) is also important and crucial factor to be maintained by IIoT. Therefore, the research in IIoT security is in boom and various security developments are in current trends. The main contribution of this survey are as follows.

1) We provide an extensive survey of the existing insecurity techniques against IIoTs and also their related solutions.
2) We show a taxonomy of solutions against security issues in IIoTs including the approaches of machine learning, deep learning and other techniques. It summarizes the advantages and disadvantages of the solutions.
3) The present study also provides a comparison of the existing surveys to clearly notify the effectiveness of our study.
4) This study explores some open research problems for the readers, researchers, academicians and technologists.

A. ARCHITECTURE OF IIOT

There is no single technology or reserved standards to establish the IoT infrastructure; indeed it is changed based on the perception of the researcher and the application used. IIoT is an integrated system with intelligence and interconnection of heterogeneous devices, sensors, actuators, processors, network devices, and transceivers in the framework of IoT. The primary three-layer architecture with physical, network, and application layers is used to establish a basic connection and interaction among devices. The addition of the support/middleware layer is used for information exchange and implements data control measures. A five-level architecture includes a business layer which is applied to manage the complete IoT system, business applications, profit models, and users' private data [5]. Figure 1 represents the layered IIoT architecture. This includes the physical components in the first layer, communication devices in the second layer, the data storage unit in the support layer, and interactive layer in the fourth level. A detailed description of each layer is given below.

Perception layer: This layer is a combination of physical and sensor devices. It identifies the environment and gathers the relevant data and forwards to the server. It is very sensitive and more likely to be attacked. Node capture, eavesdropping, replay attacks, fake node inclusion, and timing attacks are some of the common threats in this layer [6].

Network layer: This layer is responsible for data transmission among smart things, network devices, and servers using wired or wireless medium. This acts as a bridge between the presentation and application layers. It is highly sensitive but, most prominent to dangerous threats such as DoS and Man-in-the-Middle (MiTM) [6]. Moreover, other network related attacks also seem negotiable.

Application layer: It defines various applications used to control and monitor the connected devices. It is an intermediate layer between connected device and user. This acts as a mediator between the end nodes and the network, and establishes communication with the authorized software components.

Support layer: Three-level architecture is not much secured as the information is directly passed to the network layer; thus, it creates breaches for multiple threats. To overcome these flaws and protect against threats, the new support layer has been proposed; thus, it forms a four-level architecture. The data collected from the perception layer is authenticated with pre-shared secret keys and passwords, and then the data is transmitted to the network layer. Some of the attacks which affect the support layer are DoS attack, malicious insider, unauthorized access [6].

The *Industrial Internet Consortium* has presented a working framework for IIoT in 2017; it is considered as *Industrial Internet Reference Architecture (IIRA)*. The architecture is built on five major domains as control, information, operation, application, and business as shown in Figure 2. The architecture is divided into three tiers as: i) edge tier is responsible for physical and control devices, ii) platform tier is used to manage information and operations, and iii) enterprise tier is involved to control the application interface. Control domain is responsible to coordinate between the physical system and input devices (sensor, actuators) to collect the data and pass on to the information domain. Information domain provides a data service platform for the transformation and distribution of data. Operational domain manages the metadata and monitors and diagnoses the applications and portals used for interaction. Application domain provides logic and rule for accessing the information and control the flow of data from the business domain [6].

An integrated component is used to establish the IIoTs for accessing smart factories with multiple controls, i.e. CPPS. A. Sadeghi et.al presents a three-tier CPPS architecture with

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3057766, IEEE Access

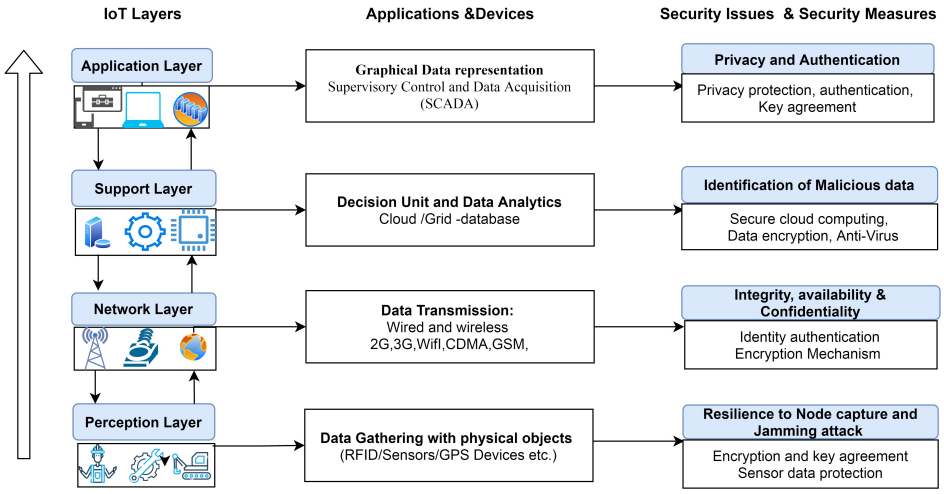

FIGURE 1: IIoT layered architecture, technology, security issues and basic security mechanisms

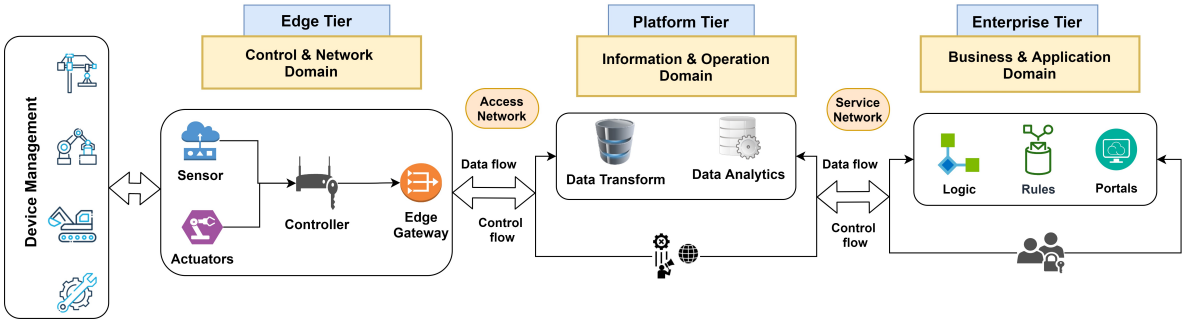

FIGURE 2: Three Tier IIoT System architecture

three stacks [2]. The framework is organized with the application, cyber, and physical stack. Each stack consists of integrated components to perform selected operations. The application stack combines the workers and the devices used for interaction and storage. The cyber stack is a middle layer with a combination of network devices as Ethernet, WiFi, and software applications used to establish communication between the application and physical stack. Finally, the physical stack with the combination of electronic and physical devices is used to collect the inputs and forward to the production process [2]. The structure of CPPS is shown in Figure 3.

B. SECURITY IN IIOT

When we talk about security, the major things come into our vision are strong passwords and cryptographic keys. However, password authentication and smart key generation are not the only source for security. To ensure secured access, advanced security techniques like cryptography algorithms, face, voice, and biometric recognition systems should be implemented. Tracking the device details and monitoring the communication processes are important in IIoTs; detecting, mitigating and preventing the intrusions are also the objectives of a security system. IIoT is already established with integrated component Supervisory Control and Data Acquisition (SCADA) from the past two decades. SCADA works on physical machinery, and intelligent network devices; machinery is used to monitor and network is used to control the process. The connected nature of these devices is very much prone to be vulnerable for attacks. Besides, other target systems under the industrial controls such as Programmable Logic Controller (PLC) and Distributed Control System (DCS) are also concerns of security in IIoTs. Major reasons for insecurity issues in industries include the age of the device, old and incompatible systems, inefficient connectivity and communication, heterogeneous devices resulting in inconsistent interaction, failure of traditional algorithms to detect the zero-day attacks, etc. [7]. Various attacks and the effects caused in IIoT layers are given in Figure 4.

Industry Control System (ICS) is a centralized management system used to coordinate and automate industrial activities. Security in traditional ICS is providing safety but, in a connected industrial system security becomes more crucial. It includes confidentiality and protection for data, and avoids the impact of hardware and software failures. Security requirements to be considered for ICS are real-time monitoring of physical devices; small deviation may cause physical loss (for example, temperature variation in nuclear power plant). Limited computing and storage of the sensor devices in IIoTs

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3057766, IEEE Access

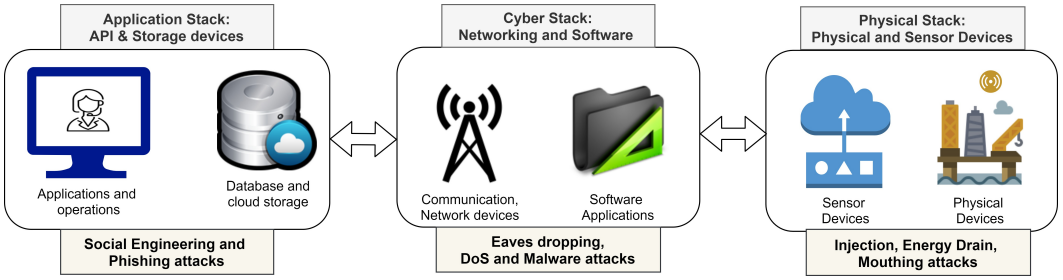

FIGURE 3: Cyber physical production system architecture

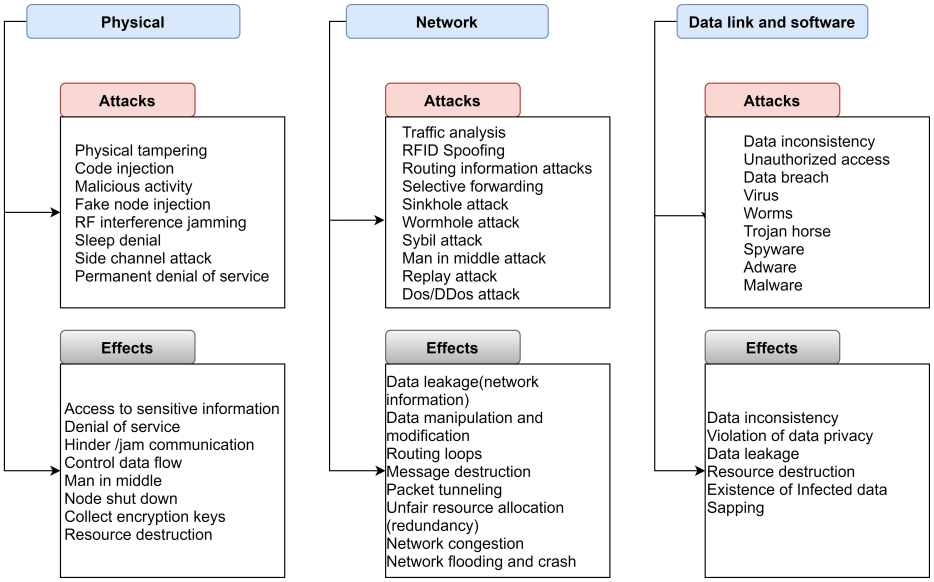

FIGURE 4: Various IIoT attacks and the Effects Caused for IIoT Layers.

also lead to security problem related to resource exhaustion. Continuous updating and restarting the industrial device are not always feasible and practical; it's hard to stop running the industrial functions to debug and fix the issues. Some of the outdated industry-oriented security protocols can be seen [8].

SANS survey report with the respondents from multiple domains focuses on the security loopholes of IIoT [9]. It has been proved that the majority of IIoT devices are used to collect data for monitoring the devices using a wired network (IEEE802.3) with internet protocol for configuration. Some other reasons for collecting data are to raise alert and alarm notifications, and to have predictive maintenance. Operational data is mostly collected via network log collectors and existing corporate IT systems. Security Information Event Management (SIEM) systems are also used to retrieve data, with periodic network scanning and traffic analysis with device-specific configuration and monitoring software. Most of the IIoT sectors are following Cyber Security Framework (CSF) developed by National Institute of Standards and Technology (NIST). Even then too, endpoint vulnerability, data accessibility, reliability, availability and integrity, networking infrastructure, and appliances issues are identified. The reasons behind the security issues in the IIoT environment are lack of security considerations in product and system installation, configuration, service, support, and maintenance. Lack of relevant, sensible, and enforceable industry standards on IIoT devices and systems also add on these issues. Lack of updates for vulnerabilities for operating systems, firmware, or other software for IIoT devices, vulnerabilities with oversight, misconfiguration, and user-errors contribute to the security disadvantages. IIoT devices are also connected directly to the internet bypassing traditional IT security layers [9]. The report has also analyzed various issues and suggested some of the mitigating techniques to reduce the impact of the attacks such as network monitoring emphasizing unusual communication behaviors with network segmentation. Implementation of firewalls, data diodes, IT/OT gateways, and applying encryption techniques by maintaining device level updates with endpoint protection are some of the regular security solutions in IIoT domain. Out of all these methods, 60% of the IIoT sectors are using device-level patching to protect IIoT device and maintain system security.

The organization of the remaining part of this study is structured as follows. In Section II we discuss about security frameworks with various services and recent solutions. Introduced intrusions in IIoT and explored various Intrusion

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3057766, IEEE Access

detection techniques implemented for IIoT devices. Various solutions proposed for detection, prevention and mitigation of intrusions in IIoT are discussed in Section III. Section IV compares various existing surveys and expresses the unique quality of current study. Section V notifies some open research problems and conclusion is drawn in Section VI.

II. SECURITY FRAMEWORKS FOR IIOT

Industrial Control System (ICS) is a centralized control scheme to operate, manage, monitor and control the complete industrial process. It is an integrated component comprised of sensors, physical devices, controllers and complex networks for communication. This system ensures a smooth execution of operation by collecting input from remote sensors, sends instructions to control valves and coordinates the task by taking relevant decisions. Combination of IoT with ICS automates the task with global data sharing and communication methods. Present ICS is a merging unit of several other technologies such as distributed control systems, remote terminal units, programmable logic controllers, SCADA and other technologies that are used to run industrial concerns. Traditional industry security mechanism was implemented with two modules: Trusted Execution Environment (TEE) and Software Guard Extensions (SGX). These are regularly used to maintain security in the IIoT environment. TEE allocates space with in the process for loading the files and provide confidentiality and integrity with high-level security. SGX is an in-built security code available with Intel CPUs. It helps to define specific memory areas to store and protect the data [9] [10]. Internal encryption and decryption are performed by CPU providing a protection against modification threats. The collaboration of IoT with multiple domains has given extreme popularity but, has discovered many security vulnerabilities especially with the rise of applications of IIoT communication methods [10]. Available measures are not significant enough for the applications due to heterogeneous architecture, huge network area, and resource constraints. Some of the security services to be considered for IIoT are shown in Figure 5.

The major security requirements of IIoTs are discussed here. *Access Control:* Secured intercommunication among nodes can be established only with a proper access control mechanism. This is implemented using authentication and authorization and also depends upon data policies. *Authentication:* The first phase of control in security systems is to authenticate user identity and establish a trust-based communication in the sharing environment. Exchange of data among IoT devices is implemented using M2M communication mode. Authentication of the node is necessary to identify the legitimate user and block the fake node attack. Password protection, secret PIN, and pattern code are the regular methods of authentication; they are extended with random number generator, fingerprint for dynamic authentication based on the requirements [10]. *Authorization:* It is used to allow the user to access the content which is permitted and block the other accesses based on conditions. Each layer of IoT is assigned with specific functions, granting access and rights to the resources as read, write, and execute will mitigate the problem of external entry [11]. *Confidentiality:* Maintaining confidentiality is generally done by converting data into a non-readable format using mathematical functions with symmetric and asymmetric algorithms. Some popular crypto methods used in IoT technology are Advance Encryption Standard (AES) to maintain confidentiality, Secure Hash Algorithms (SHA) and Diffie Hellman (DH) for key agreement [12] etc. *Integrity:* Data transferred in the network can be misused or sometimes deleted by the hacker. To exchange the same format of the data and maintain accuracy, constrained data values are imposed to disable unauthorized access, and limiting the access control to maintain integrity. *Non-Repudiation:* It is a process to provide protection against denial of sending or receiving the communication. Security service is an action to protect the network and data, identify various malicious activity and threats; these services are processed by selected security mechanism [13].

The purpose of the information system and security techniques is to assure the protection of the system and network from malicious attacks and provide the basic security services. The industrial security system should safeguard ICS and other related hardware and software applications used to control the machinery and other devices in the industries. The security system should create a transparent control room which reflects the production floor activities, to avoid the intrusions. As discussed in the beginning, connected components are more vulnerable for cyber attacks; the effect of this on ICS could result in massive outages, physical damage, and other disasters. The requirement of a strong security framework to protect the industrial structure from accidental or intentional risks has always been felt [13].

A. SERVICE BASED FRAMEWORKS

Very slow growth is observed for the research in industrial security structure. Some of the research works explore the security issues [15]- [24] in IIoT are reviewed below with the perception of authentication, authorization, defending, and preventing attacks [14]. An M2M authentication technique proposed by A. Esfahani et.al is implemented in two phases; registration phase accepts the sensor value and validation to check the authenticity [15]. Another authentication technique by J. Srinivas A et.al for biometric validation is based on three factors such as personal biometric validation, password protection, and smartcard verification [16]. X. Li et.al presents a biometric privacy-preserving protocol with the Elliptic Curve Cryptography (ECC) technique to validate the gateway authenticity [17]. F. Al-Turjman et. al shows a verification protocol named as Context-sensitive Seamless Identity Provisioning (CSIP). It is validated with cloud data and analyzes further information using deep analysis with hash methods [18]. The certificateless signature method proposed by A. Karati, S et. al provides authentication with bilinear pairing methods [19]. Y. Zhang et.al has proposed an improvement over [19] with a Robust CertificateLess Signature

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3057766, IEEE Access

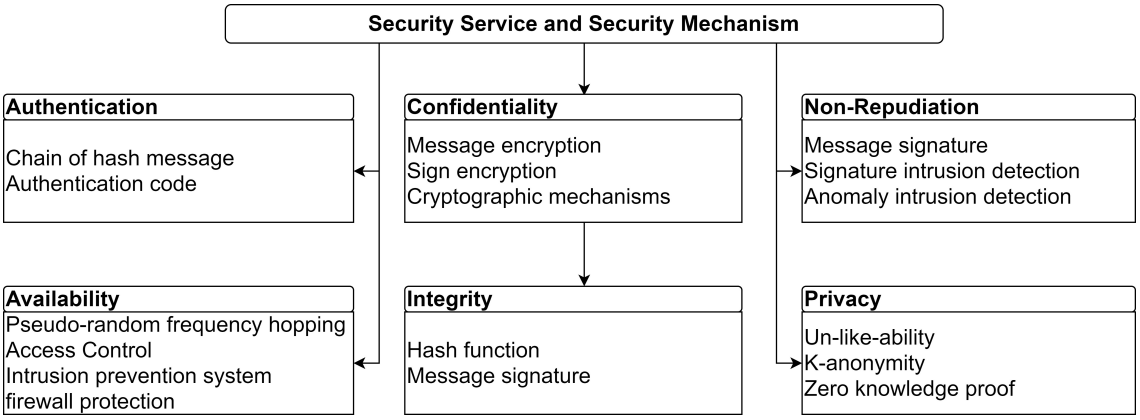

FIGURE 5: Various Security Services and the Suitable security mechanism

(RCLS) scheme. It reduces the risk of signatures' forgery and ensures protection with short signature private key method [20]. W. Yang has pointed out the issues and insecurities raised in RCLS and suggests for public key replacement and duplication of signature [21]. G. Chen et.al has proposed Sec IIoT- Authorization indexed framework for large scale placement based on metadata to define the location and time constraints [22]. R. Zhou et. al has researched a File Centric Multikey Aggregate Keyword Searchable Encryption (FC-MKA-KSE) for centralized data sharing in IIoT sectors. It provides two methods such as IND-SF-KGA (guessing), IND-SF-CKA (Choosing). Table 1 presents various authorization and authentication techniques proposed in recent research articles [23].

B. DEFENSIVE AND PREVENTIVE FRAMEWORKS

Authentication and authorization techniques restrict unauthorized entries. Sophisticated hackers bypass these techniques easily and launch the attacks for the host and network. To prevent the attacks and reduce the consequences generated by them various works have been shown in recent years [15] [16] [17] [24]. They are used to defend and prevent MiTM, DDoS and other attacks. Technique proposed by [15] is used for authentication and prevent resilient and MiTM attacks with alias sensors. A biometric protocol has been extended to prevent attacks by regenerating identification and establish communication with random number and avoids the use of secret (IDs); it controls MiTM attacks [16] [17]. Multi-level DDoS Mitigation framework (MLDMF) is used to defend fog, cloud and edge level attacks with Software-Defined Networking (SDN) gateway analysis [24]. Some of the important solutions in this direction are summarized in Table 2.

C. SMART FACTORY FRAMEWORKS

Building smart factories is a significant exertion for organizations. The IIoT framework is a combination of information technology (IT) and operational technology (OT). Smart factories allow real-time monitoring, interoperability, and virtualization. This realistic view involves surface attacks, risks, and threats for physical devices, databases, and communication channels. Smart factory uses various internal units such as PLC systems, Remote Terminal Unit (RTU) systems, SCADA servers, Human Machine Interface (HMI) servers, DCS sensors and Intelligent Electronic Devices (IEDs) to monitor and control the industrial systems. Smart manufacturing is the key component of a smart factory and acts as a bridge between digital and physical environments through IoT. The combination of upcoming technologies as cloud, machine learning, and data analytics with the industrial system leads to extreme productivity and fabricates new challenges. A secured framework incorporates the effective maintenance of the devices and ensures security for smart factories. Cheng et.al has proposed a framework for 5G technology using a digital twin mechanism to overcome the challenges faced in 4G and enhance the security controls for the Cyber-Physical Manufacturing Systems (CPMS). The model is incorporated with three modes: Enhance Mobile BroadBand (EMBB), Massive Machine-Type Communication (MMTC), Ultra-Reliable and Low Latency Communication (URLLC) [4]. J. Wan et.al has proposed a partially distributed expandable architecture, based on Bell-la Padula (BLP) along with the Biba model. This is used to address the triad of Confidentiality, Integrity, and Availability (CIA) [25]. A fog layer architecture is researched by X. Yao et.al based on Credential based Public Key Cryptography (AC-PKC) schema. Two-level verification is enforced with signature generation and access controls using fuzzy techniques [26]. To overcome the hurdles faced by traditional TCP/IP based network infrastructure and protect the IIoT environment R. Chaudhary et.al has shown a SDN-enabled multi-attribute secure communication model. The model is executed in three phases: first, communication using cuckoo with filter based fast forwarding scheme; second, attribute-based encryption for secured communication, and third, authentication using Kerberos [27]. Vakaloudis et.al has shown a five-layer architecture for Small Medium Enterprises (SME), and is successful for a limited area [28]. Considering the com-

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3057766, IEEE Access

TABLE 1: Authentication and authorization techniques for IIoT

Source	Model	Technique based on	Results
A. Esfahani et.al [15]	Machine to Machine (M2M)	Hash and XOR operations	Register and validate
J. Srinivas, A et.al [16]	Three factor protection	Chaotic map, fuzzy extractor	Blocking anonymous entry
X. Li et.al [17]	Biometric privacy-preserving	ECC	Gateway authenticity
F. Al-Turjman et.al [18]	Context Sensitive seamless identity Provisioning (CSIP)	Hash and mutual values	Deep validation with cloud data
A. Karati, S et.al [19]	Certificateless signature	Based on bilinear pairing	Pair and Compare
Y. Zhang et.al [20]	Robust certificateless signature	ECC	Reduce the risk of signature forgery
G. Chen et.al [22]	SecIIoT-Authorization	Annotated metadata	Location and time-based constraints
R. Zhou et.al [23]	Searchable encryption scheme	Centralized data sharing in IIoT	Guess and chooses the suitable solutions

TABLE 2: Defending and prevention Techniques

Source	Model	Attack	Results
A. Esfahani et.al [15]	Mutual authentication scheme & Resilient replay	MiTM attacks	Implementation of alias of sensors
J. Srinivas, A et.al [16]	User authentication scheme	Man in-the Middle attacks	Evading multiple secret (IDs) parameters is difficult
X. Li et.al [17]	Biometric protocol	Prevent replay Attacks	Regenerate ID and use random numbers.
Q. Yan et.al [24]	Mitigation framework	Defend DDoS attacks	Monitor the gateway.

patibility issues Hansch, G et.al has proposed an OLE for Process Control – Unified Architecture (OPC UA). It is based on an object-oriented model. This has been successfully implemented with XML applications [29]. To mitigate the challenges and reduce the problems faced with key-escrow and secret key distribution Verma et.al has shown the first Certificate-Based Proxy Signature (PFCBPS) scheme without pairing. This authentication mechanism is proved to be the most suitable method to secure the Random Oracle Model (ROM) with minimum computational cost [30]. Chen et.al proposes a Searchable Public-key Encryption scheme that achieves Forward Privacy (SPE-FP). This is used to overcome the problems faced by ineffective encryption schemes and has been proved effective in generating trapdoor and searching keywords; however, it results in higher computational cost [31]. Various security frameworks proposed to maintain device level, data level, and network-level protection are summarized in Table 3.

D. BLOCKCHAIN BASED FRAMEWORKS

Blockchain is considered as one of the best techniques to provide security and control for real-time conditions by creating events as blocks and maintain transparency in a decentralized environment. Mitigating the risk factor from internal and external intruders are very much required for IIoT devices. Y. Xu et. al proposes a non-repudiation network service scheme based on blockchain applications. This is used as a service publication proxy and evidence recorder. It is processed using on-chain and off-chain channels [32]. Another security framework based on blockchain is proposed by C. Lin et. al [33]. It avoids end-user anomalies. This has been implemented using Message Authentication Code (MAC) and integrated with attribute signatures for protecting network and host systems. An extension for this framework is proposed by S. H. Islam et.al [34]. It uses a multi-receiver encryption technique to provide confidentiality. Deep learning tools are apt for detection and prediction analysis. To ensure physical and device-level security, C. H. Liu et. al has proposed an Ethereum blockchain framework with Deep Reinforcement Learning (DRL) [35]. J. Huang et. al shows a credit-based Proof-of-Work (PoW) mechanism using Directed Acyclic Graph (DAG) structure to regulate sensor data and ensure data privacy [36]. A hybrid IIoT framework for Communicating Things Networks (CTNs) is used to maintain transparency among devices; it reduces product loss and has been proved effective than conventional approaches [37]. A summarization of these models is shown in Table 4.

III. SOLUTIONS AGAINST INTRUSIONS IN IIOT

According to a report, there is a possibility of wide increase for enterprise attacks by the end of 2022; more than 25 percent of attacks are targeting IIoTs. An increase in cybersecurity threats interrupts the protection of data and devices. The reflection of these threats has a severe impact on the industry domain compared to consumer IoT segments. Traditional security techniques are not efficient in an industrial environment. Larger attack surface, specialized devices with embedded system operations, and exceeding the scope of devices from the IT security perimeter are some of the major reason behind it. In general, a hacked system has a lot of data

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3057766, IEEE Access

TABLE 3: Security Framework proposed for Smart Factory

Source	Proposal	Technique	Results
Cheng et.al [4]	5G technology	Broadband, and ultra reliable a low latency communication	Digital twin operational model
J. Wan et.al [25]	Partial distributed architecture	Based on state machine model -BLP	Ensure basic security service- CIA
X. Yao et.al [26]	Fog layer architecture	Cryptographic techniques	Signature authentication and encryption.
R. Chaudhary et.al [27]	Multi-attribute communication model	Executed in three phases for communication, encryption and authentication	Effective for SND-IIoT environment
Vakaloudis et.al [28]	Five layer Architecture	Small Medium Enterprises (SME)	Successful for small scale test-bed.
Hansch, G et.al [29]	Unified architecture	Object oriented model –XML	Provided automatic security and communication
Verma et.al [30]	PFCBPS with out pairing	Key generation , certification delegation and verification	Most suitable method to secure random oracle model
Chen et.al [31]	SPE-FP	public key encryption scheme	Effective in generating trapdoor and searching keywords

TABLE 4: Security framework built on blockchain models

Source	Proposal	Technique	Results
Y. Xu et.al [32]	Non-repudiation network service scheme	Off-chain and on-chain models	Used as evidence recorder
C. Lin et.al [33]	BSEIN for industry 4.0	Message Authentication Code (MAC) and signatures	Authentication and network level protection
S. H. Islam et.al [34]	Extension for [33]	Multi receiver encryption technique	Assure confidentiality.
C. H. Liu et.al [35]	Ethereum blockchain framework	Deep Reinforcement Learning (DRL)	Ensure security and reliability
J. Huang et.al [36]	Proof-of-Work (PoW) mechanism	Directed a Cyclic Graph (DAG)	Provide data privacy.
Rathee, G et.al [37]	Hybrid IIoT framework	Blockchain analysis	89% success compared to conventional approach.

loss consequences, and if an industry is hacked it is more dangerous and even leas to a serious life-threatening issue. Intrusion in the industry can cause abrupt shut down of the power grid, breakdown in the production line, out of control of a machine, and other dangerous physical and financial loss [38].

IIoT intrusions can be caused at the device level (physical layer), application level (inserting malware for industrial applications), database level (breaking the consistency of the data, and hacking confidential information), and network-level (unauthorized access) [38]. A firewall is used as an initial security measure to block the suspicious attempt; this is not much suitable for a large scale security system like IIoT. An Intrusion Detection System (IDS) is a special service for protecting the data from unauthorized access. IDS is an extended solution mitigating and detecting malicious activity by sensing the attacks based on inbuilt patterns and raise alerts to security officers or preventing the attack by blocking the processes [39]. Various frameworks and models are proposed for device level, network level, and database-level detection for IIoTs. In the following subsections we have discussed these solutions based on used machine learning, deep learning and other techniques.

A. MACHINE LEARNING-BASED SOLUTIONS

The complex nature of cyber-attack needs an efficient and adaptive method for intrusion detection. Many of the research proposals are developed on anomaly detection with the combination of statistical and Machine Learning (ML) techniques to monitor network and identify the threats. These techniques are more successful in fault tolerance, high computational speed, error resilience, proved valuable and produced effective IDS. ML classification techniques are learnt from labelled input and use the same for evaluating new observations into binary or multi-class format. Some of the techniques used for classification include Support Vector Machine (SVM), Discriminate Analysis (DA), Naïve Bayes (NB), and K-Nearest Neighbor (KNN). Regression techniques are used as predictive models and to identify the relationship between the dependent and independent variables preferably for forecasting and time series models of IIoTs. Some of the techniques under this category are linear regression, Logistic Regression (LR), Decision Trees (DT), and Random Forest (RF). Unsupervised learning is used to detect unknown patterns with clustering, k-means, Gaussian Mixture, and Hidden Markov algorithms [40].

Complementary support for existing IDS is proposed by Patric Nader et.al [41]. It is used with ML algorithm to integrate one class classification algorithm with Kernel Principle Component Analysis K-(PCA). The study is tested on water distribution system in France and has been proved effective comparatively. Comparing the traditional detection techniques, anomaly detection has a high demand in industrial sectors. ML for anomaly detection ends up with many

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3057766, IEEE Access

challenges in real-time for large-scale deployment. Meshram et.al proposes a multi-module solution to overcome the challenge by Anomaly Detection Industrial Network (ADIN) suit with ML techniques [42]. Keliris et.al shows a process-aware defense strategy for the industrial control system to recognize, discover, analyze and mitigate the attacks using the SVM model; it is tested for Hardware-In-The-Loop (HITL) testbed with payload delivery method [43]. Lee.s et. al implements ML techniques for various IIoT components and proves the stability of the solutions by deploying three detection models as a packet diversity based anomaly detection system, protocol specific whitelist model, and One-Class Support Vector Machine (OCSVM) [44]. To improve detection capability Wu, M et. al has researched the KNN algorithm for identifying threats in Cyber Manufacturing System (CMS) resulted in 52.62% accurate for host and network intrusion detection [45]. To find the most suitable technique for detection M.Zolanvari et.al has compared seven ML techniques (SVM, KNN, NB, RF, DT, LR, and Artificial Neural Network (ANN)) and has stated that RF and NB are effective in anomaly detection for SCADA system [46]. Considering the importance of data set in IDS Zolanvari et. al proposes an ML algorithm for an imbalanced dataset. The study explores some of the classification algorithms as applying power spectral density, Fourier analysis, the linear feature extracting, and Principal Component Analysis (PCA). The use of public datasets and the consistency of features are some of the reasons for the low detection rate. The algorithm is executed using Matthews Correlation Coefficient (MCC) technique and has resulted in 0% False Rate Ratio (FRR). It is proved as the best suitable method for detection in IIoT. At the same time, this model is suitable only for binary classification too [47]. A. A. Kurniawan et. al proposes an ensemble learning-based intrusion detection method called as Synthetic Minority Over-Sampling Technique (SMOTE). K-NN classification is used to determine the parameter value and deviation between training and testing data. The results comparatively proves high in case of accuracy with 97.02% with detection rate of 97% and 0.16% false alarm rate [48]. Considering the alert identification as a unique parameter, to improve the significance of detection for hidden attacks, Capture The Invisible (CTI) is used as a pattern recognition algorithm as proposed by Bhardwaj A et.al [49]. The authors suggest that repeated testing with dynamic datasets helps to discover invisible attacks compared to the Inductive Miner algorithm [49]. A summary of the solutions based on machine learning is shown in Table 5.

B. DEEP LEARNING-BASED SOLUTIONS

Outlier detection, increased error rates, semantic gap, network traffic diversion, evaluation difficulties are the major challenges of machine learning techniques for IDS in the industrial environment. Deep Learning (DL), a division of machine learning based on concerning algorithms, is used to create high-level abstraction in data with the hierarchical layered architecture of learning. DL techniques are inspired by human brain structure and function which mimics the network of neurons in a brain to extract hidden features from original data. The main purpose of DL is to deal with a huge amount of unsupervised data and implement layer-wise learning techniques. The learning is implemented in two phases. First, to accept nonlinear transformation and create a statistical model as output and the second, to improve the model with derivatives (mathematical methods). In between a huge combination of hidden layers establish network connection [50]. The most popular DL techniques implemented for IDS are discussed here. *Generative Adversarial Network (GAN)s:* it is used to build a security architecture to IIoT and to train more than one model. *Deep Belief Network (DBN):* It is a multi-layer structure with fine-tuned pre-training models and effective in identifying malicious attacks. At the same time, it results with high computational cost, extensive initialization. *Recurrent Neural Network (RNN):* Is the mostly used for internal features extraction and characteristics identification, accurate in network traffic classification, effective in identifying time series-based threats. Vanishing or exploding gradients is the major issues of this technique. *Convolutional Neural Network (CNN):* It is another most suitable for network intrusion detection to analyse traffic and classify good and bad node; it provides end-to-end security. High computational cost and limited to resource-constrained devices are the major falloffs of this technique [50]. Considering these many qualities of DL techniques, research community have provided various detection and prevention models to mitigate the effects of vulnerabilities in IIoTs and a summarization is shown in Table 6.

To solve the problems raised due to the lack of interconnection among nodes in traditional Neural Network (NN) Yanmiao Li et.al has proposed Multi-Convolutional Neural Network (Multi-CNN) detection model. By creating a connected dropout layer as regularization layer, between the convolutional and pooling layer at the top, the model allows a two-dimensional structure of input data. It results in binary classification with 76.67% accuracy and multiclass classification with 86.95% accuracy [51]. To ensure security and identify the faults for real-time IIoT structure in Industrial Gas Turbines (IGTs) Zhang, Y., Et.al has shown Gaussian Mixture Model (GMM) with an Outlier Component (GMMOC). It detects the emerging faults and provides early warnings to mitigate the risk. The study has been extended with Variational Bayesian Gaussian Mixture Model (VBGMM) [52]. It is an automatic clustering method to remove transient measurements and accept only steady-state operations. Collecting information to develop an intelligent detection agent to handle new attacks is a difficult task in Network-IDS. AL Hawawreh et.al has proposed an anomaly detection technique using Deep Auto Encoder (DAE) and Deep Feed Forward Neural Networks (DAE-DFFNN) for the Internet Industrial Control (IIC) systems. The model is based on a self-learning method and validates information collected from TCP/IP packets. Evaluation of the model is done by NSL-KDD and INSW-NB15 datasets; the model shows 99%

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3057766, IEEE Access

TABLE 5: Summary of IDS models and methods proposed using machine learning for IIoT

Source	Solution type	Technique used	Results claimed	Scope/ research gap
Patric Nader et.al [41]	Detection	One class classification algorithm	Complementary support for IDS	Integration required
Meshram, A et.al [42]	Detection	ADIN-Suit An Multi module technique	Anomaly detection and secured protection	Compatibility
Keliris, A. et.al [43]	Mitigation	SVMs	Reducing false rates	Processing speed enhancement
Lee.s et.al [44]	Detection	Packet, protocol and classification based models	Applicable for next generation power control system	Improvement in classification techniques
Mingtao Wu et.al [45]	Detection	K-Nearest Neighbors algorithm (KNN)	Combination of cyber and physical data	Recovery to be concerned.
Maede Zolanvari et.al [46]	Detection	Comparative analysis	Random Forest and Naïve Bayes(NB) were effective	Integrated model can be developed
M.Zolanvari, et.al [47]	Detection	Matthews Correlation Coefficient (MCC)	Very low False Rate Ratio (FRR)	Appropriate for binary classification only.
A. A. Kurniawan et.al [48]	Detection	Synthetic Minority Over-sampling Technique (SMOTE)	Superior comparatively for accuracy, detection rate and False alarm rates	Enhancement needed for processing time
Bhardwaj, A. et.al [49]	Detection	Capturing-the-Invisible (CTI)	Best than inductive miner algorithm	Enhancement for behaviour detection.

detection rate and 1.8% false positive rates [53].

In order to train high-dimensional modbus data packets, Hijazi et.al. has proposed a detection model based on multi-layer processing with binary classification. The test results in 99% accuracy compared with Self Taught Learning (STL) and SoftMax Regression (SMR) [54]. Considering the popularity of deep learning techniques, and with the idea of integration, Lbitoye et. al has investigated a model to mitigate the intrusion attacks. Feed-forward Neural Networks (FNN) and Self-normalizing Neural Network (SNN) are observed and the differences have been compared with real-time data set samples. The performance is measured on accuracy, precision, and recall, and classification score. SNN- IDS is having higher accuracy than FNN IDS but fails in handling adversarial attacks with below 50% detection value and concludes to be not much suitable for real-life applications [55]. Autoencoder (AE) deep learning-based anomaly detection algorithm for the smart factory environment is shown in [56]. The test has been conducted with three scenarios for real-time data from Korea steel companies for the experiment. The model has been compared with the Density-Based Spatial Clustering of Applications with Noise (DBSCAN) and results in an average of 95% accuracy. Jafar A et. al has proposed a Hashed Needham Schroeder Cost Optimized Deep Machine Learning (HNS-CODML) method to ensure secured cloud transfer of data with minimum computational cost. Public Key Generation (PKG) mechanism is used to measure the computational cost and overhead. Data transfers are implemented using the cloud by any user with authenticated privileges and join the receivers with asymmetric cryptography techniques [57].

Extending the scope of IDS to the automobile industry Jiayan Zhang et.al has shown a security model for vehicle IDS using Gradient Descent with Momentum (GDM) and GDM-Adaptive Gain (GDM-AG) techniques. GDM/AG algorithm is effective with approximately 98% accuracy than GDM to detect the anomaly in milliseconds [58]. Ankang Chu et. al has proposed a detection model using GoogLeNet which combines the qualities of CNN for feature extraction and LSTM for time-series level detection. The detection is classified into multiple categories and implemented for the gas pipeline dataset of Modbus protocol and resulted in 97.56% accuracy and 2.42% false positive rate [59]. A Bidirectional Long and Short-Term Memory (B-MLSTM) network with a multi-feature layer model is proposed by Li, X et al [60]. It is trained from historical data and updated to a double-layer reverse unit for comparative detection with time intervals. Integrated model with Recurrent neural network (RNN) and Long short-term memory (LSTM) has been tested for three classic IIoT datasets and results in 46.79% false positive rate and 79.85% false-negative rate [60].

A combination of ML and DL model for detection is proposed by Park et.al [61]. It uses a five-step analysis for anomaly detection using classification linear regression, Random Forest, K-means, Auto Encoder, and DB scan for supervised, unsupervised, and hybrid Classifications. A drill-down analysis has been conducted to integrate the data set with time standard. It performs correlation analysis on data with result relationship model. Jun Gao et.al has developed a detection model for SCADA. Feed Forward Neural Network (FNN) is much compatible with temporally uncorrelated attacks and long-short term memory (LSTM) for detecting correlated attacks. The comparison demonstrates that FNN outperforms LSTM and NDAE RF [62]. Yan X et. al has designed a Hinge Classification Algorithm on mini-batch Gradient Descent with an Adaptive Learning Rate and Momentum "(HCA-MBGDALRM) detection model [63]. It uses a parallel framework to improve the safety for IIoT. Data and workload are distributed and maintained using globally shared parameters. Time intervals are monitored with pull

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3057766, IEEE Access

and push thread to mitigate the burden on the server. J.Choi has proposed an information sharing security system. It uses a filter module for the feature section. Self organizing Maps (SOMs) neural model is used for filtering normal activities utilizes PCA and Fisher Dimension Reduction is used to filter noises [64].

C. OTHER SOLUTIONS

The current status of IIoT security is with multiple flaws such as low detection accuracy, high false-positive rate, and very less real-time performance. Apart from various machine learning based approaches and deep learning methods for IIoTs, some others significant solutions exist that turn on the effectiveness of IIoT security.

To mitigate the effect of threats on SCADA, den, P. et.al has presented a seven stem forensic model for IIoT structure. This model understands, detects, isolates, avoids, analyzes, responds and reports the finding and then updates the system architecture and requirements for future prevention [65]. Another detection model to collect and communicate attack data to the forensic department is shown by T.Guo et.al [66]. This framework shows a mitigation technique for edge devices and the detection model is used to identify the attacks using clustering techniques. The model is executed with four nodes as Raspberry Cluster, IoT Edge gateway, Matrix Creator Node, and an attacker node. Results classify the status of edge gateway (prone to attack or not by continuous monitoring) and provide information for the forensic department. Kirupakar j et.al has proposed a framework with an intelligent agent for the IIoT gateway platform for IIoT using Hybrid IDS. This is an update module of IDS which was earlier designed for wormhole attack detection with low powered IIoT gateway and sub-devices. The model is compatible with the IIoT structure and successful in identifying the threats [67].

N.E. Petroulakis et.al has investigated a SEMIoTICS pattern derived and multi-layered embedded intelligence framework for detection. The architecture is implemented with three layers: field layer, orchestration layer, and application layer. The model is tested for the wind energy industry and e-Health supporting system for detecting local and global anomalies and reduced unnecessary traffic with quick and effective detection of abnormalities [68]. Arshad J et.al has proposed a framework for energy-constrained IoT devices with Signature-based Intrusion Detection (SID) techniques on the Contiki operating system. The model is structured using two basic components as a Global Detection Enactor (GDE) with three agents as detection agent, correlation agent, alert collector used to identify intrusion connected to the edge router. The monitoring unit is comprised of network monitor, system monitor, and detection engine connected to the host in the network. The framework minimizes the overall overhead in terms of energy consumption and memory and is effective within constrained devices [69]. E. Aydogan et.al has shown a detection model based on genetic programming against Routing Protocol for Low-Power and Lossy Networks (RPL) and has suggested this as the best suitable architecture for the IIoT environment. Genetic programming is suitable for detecting threats and implemented successfully with low false-positive rates by testing on 26 IIoT nodes with Telos -B mode on Cooja stimulation. The central intrusion detection system is proved as a suitable architecture for the IIoT network with effective detection [70].

Rui-Hong Dong et.al. has proposed an IDS model traffic characteristics map perceptual hash algorithm (TCM-PH) to monitor and analyze the traffic data with attribute set. Initially, the model collects required values using the information entropy method, then transforms the vector into a triangle area mapping matrix using Multiple Co-relation Analysis (MCA) approach. Finally, Discrete Cosine Transform (DCT) and Singular Value Decomposition (SVD) methods are implemented for discriminating the normal and abnormal traffic [71]. Liang, W et.al has shown an optimization model on multifeatured data clustering with network intrusion detection. The special feature of this model is a two-fold rapid selection node for repeated selection and detection process resulted with 97.8% detection accuracy and 8.8% false-positive rates [72]. A comparative analysis by Zeeshan Ali Khan et.al on various techniques used for detection in IIoT is significant in this direction [73]. Six features were considered for effective detection systems as decision, quality, technique, attack responses, type of attacker and attack implementation strategy. Suitability of the approach is completely depended on the type of IoT network. Nine different implementation methods are compared with energy, a processor with and without powerful nodes, detection accuracy, and resource-constrained nodes. Cross-layer, game theory, machine learning, and reputation detection methods are consuming high energy comparatively. The summarization of these solutions is provided in Table 7.

IV. COMPARISON WITH EXISTING SURVEYS

Industrial 4.0 has explored various new technologies to create a self-organized automated structure. More the ease created by this revolution; more vulnerabilities are existing. The evolution of smart industry techniques raised many security threats and issues. These cause data loss, physical damage, and unintentional hazards. Creating a secured environment for IIoT is a thriving research area. Considering this as a scope for development, various research articles are reviewed which disclosed various methods, models, techniques, and technologies. Considering security violation as the main issue of the study, we have focused on existing surveys related to security and intrusion detection to reach the current advancement of the research area in Industry IoT. Table 8 projects a comparative analysis of the existing surveys with the present study.

V. OPEN RESEARCH PROBLEMS

The main aim of the paper is to provide an overview of IIoT security issues and challenges and the comparative analysis of existing solutions. After the detailed comparative discussion on threats, methods, and techniques, we provide

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3057766, IEEE Access

TABLE 6: Summary of IDS Models and Methods proposed using Deep learning for IIoT

Source	Solution type	Technique used	Results claimed	Scope/ research gap
Yanmiao Li et.al [51]	Detection	Multi-CNN	Effective for multiclass than binary	Performance enhancement is required
Zhang.y et.al [52]	Detection and Mitigation	Gaussian mixture and its variations	Trace operational status	Low performance in high dimensions
AL Hawawreh et.al [53]	Detection	Auto encoder and Feed forward Neural Network	Comparatively efficient	Not suitable for nonnumeric content
Hijazi et.al. et.al [54]	Detection	Multi-layer binary classification on Neural Network	Accurate compared to Learning and regression techniques	Limited to attack type.
Lbitoye et.al [55]	Mitigation	SNN and FNN - IDS	SNN-IDS s more accurate than FNN-IDS	Enhancement for real time applications.
Bae, G et.al [56]	Detection	AE based Anomaly detection	Physical and network level protection	Noise levels are not mentioned.
Jafar A et.al [57]	Secured Transfer	Deep learning and Asymmetric cryptography techniques	Computational cost calculation	Detection methods can be emphasised.
Jiayan Zhang et.al [58]	Detection	Gradient Descent with Momentum (GDM)	Accurate in-vehicle security	Limited to device level security.
Ankang Chu et.al [59]	Detection	GoogLeNet-LSTM Model	Secured network communication using Modbus Protocol	Application centric
Li, X et al. [60]	Detection and Mitigation	RNN and LSTM	Bidirectional multistage detection	High computational cost
Park, S [61]	Detection	ML and DL techniques	Industry specific- detection and accuracy.	Can be expanded with other DL techniques.
Jun Gao et.al [62]	Detection	FNN and LSTM	Suitable for SCADA protection	Further development with CNN technique.
Yan X et.al [63]	Detection	Parallel detection with time intervals	Combatively effective based on scale and speed	Missing gradient problem may raise.
J.Choi et.al [64]	Detection	SOMs and Principal Component Analysis and Fisher	Effective for feature selection and filtering	Accuracy to be improved.

some emerging security issues and IDS challenges that can be used as future perspectives. It is observed from the above discussion that the major challenges faced by the IIoT sector arise due to huge traffic, heterogeneous network structure, variations in data sets, lack of common format, lack of regular updates for the data set, lack of unique real-time IoT dataset availability etc. These have serious impact on the IIoT system and performance. Most of the IIoT models are integrated with sensors, cloud, network, and communication devices, etc,; therefore, the intrinsic vulnerabilities and the application specific loopholes make the IIoT sector facing multiple hiccups. Lack of patching in IIoT devices, accidental exposures, huge financial, technical, and human loss can result in out of these reasons. Difficulties in controlling, tracking and managing heterogeneous architectures are some of the challenges faced by IIoT in upcoming years. Open research problems to develop an efficient security solutions are discussed below.

1) *System integration:* Is there any suitable integrated model for IIoT devices with edge and data-level security? All the above-discussed models have an application-based impact, no single model is compatible with multiple automatic services. The compatibility and verifiability of system integration can be explored further.
2) *Communication:* How to create a secured communication between IIoT devices and apt security model to protect the data? Data exchange with a public network creates vulnerable security issues. High power secured protocol or model can restrict the data access for intruders.
3) Energy factor: High quality, power, and energy-constrained device with quality data collection need to be developed. Industry sector power consumption is a major challenge; lightweight and effective detection systems to be developed which maintain the balance between power, energy, and efficiency of the industrial processing.
4) Preventive and detective measures: Lack of preventive measures for malware and injection attacks are observed the literature study. Attack detection is considered mostly and prevention is avoided. Therefore, some efficient techniques are required which are able to detect attacks and prevent the attacks from future execution. Malware detection solutions need to be devised to protect the IoT devices from malware.
5) *Authorization:* Enhanced authorization methods with double layer validation are in the future scope and will be beneficial for IIoT security. User-level customization should be allowed in such method for being com-

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3057766, IEEE Access

TABLE 7: Summary of IDS models and methods proposed using various technologies

Source	Solution type	Technique used	Results claimed	Scope/ research gap
Eden et.al [65]	Mitigation	Forensic model with seven steps	Used for attack prediction	Limited checking
T.Guo et.al [66]	Detection and Mitigation	Clustering techniques	Edge-level security	Enhancement required for detection methods
Kirupakar j et.al [67]	Detection	Hybrid Intrusion Detection system	Updated model of Worm-hole attack	Protocol security can be improved.
N. E. Petroulakis et al. [68]	Detection	Three layer detection and mapping.	Overall security for IIoT network.	Processing Delay.
Arshad J et.al [69]	Detection	Global detection and monitor system	Executed with minimum energy	Enhancement required for detection techniques
Aydogan, E. [70]	Detection	Genetic Programming	Counter method for RPL's DODAG mechanism.	High computational cost.
Dong et.al [71]	Mitigation	TCM-PH	Innovative solutions for NIDS	Misassumption to be monitored.
Liang, W et.al [72]	Detection	NIDS Clustering model	Two fold repeated detection process	Behaviour patterns can be considered.
Zeeshan Ali Khan et.al [73]	Detection	Comparative analysis	Energy consuming techniques were highlighted	Less exposure on detection methods.

TABLE 8: Comparison with existing surveys

Source	Attributes	Results
H. Boyes et.al [74]	Analytical framework on IIoT with detailed taxonomies for various categories and the limitations	The study help's the researcher to explore more in the area and find out the research gap in technology, network, detection and security
L. D. Xu, et.al [75]	Service-Oriented Architecture (SOA) model, infrastructure limitation, technical glitches and security issues were highlighted	Integrating social networking with IoT, development of Green IoT technologies, combination of cloud and AI with IoT were the suggested for future research
E. Oztemel, et.al [76]	Explored on recent trends effecting the Industry, components and framework. Industry development life cycle, projects like ENTOC, Metamo FAB, Parsi FAI 4.0, ESIMA, INESA.	Smart factory is discussed and concluded with challenges and scope of study. Real time security issues can be focused for further research.
V. Alcacer [77]	Key technologies and the impact of cloud computing, bigdata. augmented reality, cyber security and autonomous robots	Represented the research gab between major manufacturing system and I4.0
Rubio et.al [78]	Comparative analysis of IS and ICS, detection techniques	Issues of each model was explored, security services and the impact on IIoT is clearly mentioned
Current survey	IIoT security issues, layer-based attacks, detection methods, security services and solutions, machine learning, deep learning and other techniques for IIoT security solutions	Understanding attacks and impacts, security frameworks, security solutions based on machine learning and deep learning and other techniques; open opportunities

patible for all the application framework. Development of application based protection system for sensitive data using deep learning algorithms and game theoretic approach can be explored further.

6) *Architecture:* Sophisticated IoT architecture needs to be developed for multiple platforms with reduced feedback latency. At present, very less security architectures in IIoTs can support multiple platforms; therefore, the compatibility can be a point of research concern.

VI. CONCLUSION

Uninterrupted connectivity and unrestricted data transfer, irrespective of distance, and providing intelligent service are the major qualities of IIoT technologies. The integrated components with sensors, processing, and visualization capabilities are more vulnerable to cyber-attacks. The large-scale connectivity, irregular device, and interrupted network connectivity patterns create some of the issues for physical systems. Considering these as major challenges, our present study focuses on security issues, challenges, and mitigation techniques implemented by IIoT. This survey also explores various other surveys related to IIoT and distinguishes its properties. The study also identifies some open research problems for future researchers.

REFERENCES

[1] G. George and S. M. Thampi, "A Graph-Based Security Framework for Securing Industrial IoT Networks From Vulnerability Exploitations," in IEEE Access, vol. 6, pp. 43586-43601, 2018, doi: 10.1109/ACCESS.2018.2863244.

[2] A. Sadeghi, C. Wachsmann and M. Waidner, "Security and privacy challenges in industrial Internet of Things," 2015 52nd ACM/EDAC/IEEE Design Automation Conference (DAC), San Francisco, CA, 2015, pp. 1-6, doi: 10.1145/2744769.2747942.

[3] F. Koushanfar, A.-R. Sadeghi, and H. Seudie. Eda for secure and dependable cybercars: Challenges and opportunities. In Proceedings of the 49th Annual Design Automation Conference. ACM, 2012.

[4] Cheng, Jiangfeng, Weihai Chen, Fei Tao, and Chun-Liang Lin. "Industrial IoT in 5G environment towards smart manufacturing." Journal of Industrial Information Integration 10 (2018): 10-19.

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3057766, IEEE Access

[5] Sethi, P., & Sarangi, S. R. (2017). Internet of Things: Architectures, Protocols, and Applications. Journal of Electrical and Computer Engineering, 2017, 1–25. doi:10.1155/2017/9324035

[6] Muhammad Burhan 1,Rana Asif Rehman 1,Bilal Khan 1 andByung-Seo Kim . IoT Elements, Layered Architectures and Security Issues: A Comprehensive Survey Sensors 2018, 18(9), 2796; https://doi.org/10.3390/s18092796

[7] Sengupta, J., Ruj, S., Bit, S.D., A comprehensive survey on attacks, security issues and blockchain solutions for IoT and IIoT, Journal of Network and Computer Applications (2019), doi: https://doi.org/10.1016/j.jnca.2019.102481

[8] Hu, Y., Yang, A., Li, H., Sun, Y., & Sun, L. (2018). A survey of intrusion detection on industrial control systems. International Journal of Distributed Sensor Networks. https://doi.org/10.1177/1550147718794615

[9] The 2018 SANS Industrial IoT Security Survey: Shaping IIoT Security Concerns Written by Barbara Filkins Advisor: Doug Wylie, July 2018 Sponsored by: ForeScout Technologies, Inc.

[10] Challa, Sravani, Ashok Kumar Das, ProsantaGope, Neeraj Kumar, Fan Wu, and Athanasios V. Vasilakos. "Design and analysis of authenticated key agreement scheme in cloud-assisted cyber–physical systems." Future Generation Computer Systems 108 (2020): 1267-1286.

[11] Kumari, S., Karuppiah, M., Das, A.K. et al. A secure authentication scheme based on elliptic curve cryptography for IoT and cloud servers. J Supercomput 74, 6428–6453 (2018). https://doi.org/10.1007/s11227-017-2048-0

[12] Jurcut, Anca Ranaweera, Pasika & Xu, Lina. (2019). Introduction to IoT Security. 10.1002/9781119527978.ch2.

[13] Inayat Ali, Sonia Sabir , Zahid Ullah, "Internet of Things Security, Device Authentication and Access Control: A Review", International Journal of Computer Science and Information Security (IJCSIS), Vol. 14, No. 8, August 2016.

[14] H. Noura. Adaptation of Cryptographic Algorithms According to the Applications Requirements and Limitations : Design, Analyze and Lessons Learned. HDR dissertation, UNIVERSITY of PIERRE MARIE CURIE -Paris VI, 2016.

[15] A. Esfahani, G. Mantas, R. Matischek, F. B. Saghezchi, J. Rodriguez, A. Bicaku, S. Maksuti, M. G. Tauber, C. Schmittner, J. Bastos, A lightweight authentication mechanism for m2m communications in industrial IoT environment, IEEE, Internet of Things Journal 6 (1) (2019) 288-296.

[16] J. Srinivas, A. K. Das, M. Wazid, N. Kumar, Anonymous lightweight chaotic map-based authenticated key agreement protocol for industrial internet of things, IEEE Transactions on Dependable and Secure Computing.

[17] X. Li, J. Niu, M. Z. A. Bhuiyan, F. Wu, M. Karuppiah, S. Kumari, A robust ecc-based provable secure authentication protocol with privacy preserving for industrial internet of things, IEEE Transactions on Industrial Informatics 14 (8) (2018) 3599-3609.

[18] F. Al-Turjman, S. Alturjman, Context-sensitive access in industrial internet of things (IIoT) healthcare applications, IEEE Transactions on Industrial Informatics 14 (6) (2018) 2736-2744.

[19] A. Karati, S. H. Islam, M. Karuppiah, Provably secure and lightweight certificate less signature scheme for IIoT environments, IEEE Transactions on Industrial Informatics 14 (8) (2018) 3701-3711.

[20] Y. Zhang, R. Deng, D. Zheng, J. Li, P. Wu, J. Cao, E client and robust certificateless signature for data crowdsensing in cloud-assisted industrial IoT, IEEE Transactions on Industrial Informatics.

[21] W. Yang, S. Wang, X. Huang, Y. Mu, On the security of an efficient and robust certificateless signature scheme for IIoT environments, IEEE Access 7 (2019) 91074-91079.

[22] G. Chen, W. S. Ng, Anefficient authorization framework for securing industrial internet of things, in: TENCON 2017 –1320 2017 IEEE Region 10 Conference, 2017, pp. 1219-1224.

[23] R. Zhou, X. Zhang, X. Du, X.Wang, G. Yang, M. Guizani, File-centric multi-key aggregate keyword searchable encryptionfor industrial internet of things, IEEE Transactions on Industrial Informatics 14 (8) (2018) 3648-3658.

[24] Q. Yan, W. Huang, X. Luo, Q. Gong, F. R. Yu, A multi-level ddos mitigation framework for the industrial internet of things, IEEE Communications Magazine 56 (2) (2018) 30-36.

[25] J. Wan, J. Li, M. Imran, D. Li, F. 1330 e-Amin, A blockchain-based solution for enhancing security and privacy in smartfactory, IEEE Transactions on Industrial Informatics.

[26] X. Yao, H. Kong, H. Liu, T. Qiu, H. Ning, An attribute credential based public key scheme for fog computing in digital manufacturing, IEEE Transactions on Industrial Informatics.

[27] R. Chaudhary, G. S. Aujla, S. Garg, N. Kumar and J. J. P. C. Rodrigues, "SDN-Enabled Multi-Attribute-Based Secure Communication for Smart Grid in IIoT Environment," in IEEE Transactions on Industrial Informatics, vol. 14, no. 6, pp. 2629-2640, June 2018, doi: 10.1109/TII.2018.2789442.

[28] Vakaloudis and C. O'Leary, "A framework for rapid integration of IoT Systems with industrial environments," 2019 IEEE 5th World Forum on Internet of Things (WF-IoT), Limerick, Ireland, 2019, pp. 601-605, doi: 10.1109/WF-IoT.2019.8767224.

[29] Hansch, G., Schneider, P., Fischer, K., & Bottinger, K. (2019). A Unified Architecture for Industrial IoT Security Requirements in Open Platform Communications. 2019 24th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA). doi:10.1109/etfa.2019.8869524

[30] Verma, Girraj Kumar, B. B. Singh, Neeraj Kumar, Mohammad S. Obaidat, Debiao He, and Harendra Singh. "An efficient and provable certificate-based proxy signature scheme for IIoT environment." Information Sciences 518 (2020): 142-156.

[31] Chen, Biwen, Libing Wu, Neeraj Kumar, Kim-Kwang Raymond Choo, and Debiao He. "Lightweight searchable public-key encryption with forward privacy over IIoT outsourced data." IEEE Transactions on Emerging Topics in Computing (2019).

[32] Y. Xu, J. Ren, G. Wang, C. Zhang, J. Yang, Y. Zhang, A blockchain-based non-repudiation network computing service scheme for industrial iot, IEEE Transactions on Industrial Informatics.

[33] C. Lin, D. He, X. Huang, K.-K. R. Choo, A. V. Vasilakos, Bsein: A blockchain-based secure mutual authentication withne-grained access control system for industry 4.0, Journal of Network and Computer Applications 116 (2018) 42 - 52.URL http://www.sciencedirect.com/science/article/pii/S1084804518301619

[34] S. H. Islam, M. K. Khan, A. M. Al-Khouri, Anonymous and provably secure certificate less multireceiver encryption without bilinear pairing, Security and Communication Networks 8 (13) (2015) 2214-2231. URL https://onlinelibrary.wiley.com/doi/abs/10.1002/sec.1165

[35] C. H. Liu, Q. Lin, S. Wen, Blockchain-enabled data collection and sharing for industrial iot with deep reinforcement learning, IEEE Transactions on Industrial Informatics.

[36] J. Huang, L. Kong, G. Chen, M. Wu, X. Liu, P. Zeng, Towards secure industrial iot: Blockchain system with credit-basedconsensus mechanism, IEEE Transactions on Industrial Informatics.

[37] Rathee, G., Sharma, A., Kumar, R., & Iqbal, R. (2019). A Secure Communicating Things Network Framework for Industrial IoT using Blockchain Technology. Ad Hoc Networks, 101933. doi:10.1016/j.adhoc.2019.101933

[38] https://new.siemens.com.

[39] E. Denning, "An Intrusion-Detection Model," 1986 IEEE Symposium on Security and Privacy, Oakland, CA, USA, 1986, pp. 118-118

[40] Zamani, Mahdi, and Mahnush Movahedi. "Machine learning techniques for intrusion detection." arXiv preprint arXiv:1312.2177 (2013).

[41] Nader, P., Honeine, P., & Beauseroy, P. (2016). Detection of cyberattacks in a water distribution system using machine learning techniques. 2016 Sixth International Conference on Digital Information Processing and Communications (ICDIPC). doi:10.1109/icdipc.2016.7470786

[42] Meshram, A., & Haas, C. (2016). Anomaly Detection in Industrial Networks using Machine Learning: A Roadmap. Machine Learning for Cyber Physical Systems, 65-72.

[43] Keliris, A., Salehghaffari, H., Cairl, B., Krishnamurthy, P., Maniatakos, M., & Khorrami, F. (2016). Machine learning-based defense against process-aware attacks on Industrial Control Systems. 2016 IEEE International Test Conference (ITC). doi:10.1109/test.2016.7805855

[44] Lee, S., Lee, S., Yoo, H., Kwon, S., & Shon, T. (2017). Design and implementation of cybersecurity testbed for industrial IoT systems. The Journal of Supercomputing. doi:10.1007/s11227-017-2219-z

[45] Wu, M., and Moon, Y. B. (January 22, 2019). "Intrusion Detection System for Cyber-Manufacturing System." ASME. J. Manuf. Sci. Eng. March 2019; 141(3): 031007. https://doi.org/10.1115/1.4042053

[46] M. Zolanvari, M. A. Teixeira, L. Gupta, K. M. Khan and R. Jain, "Machine Learning-Based Network Vulnerability Analysis of Industrial Internet of Things," in IEEE Internet of Things Journal, vol. 6, no. 4, pp. 6822-6834, Aug. 2019, doi: 10.1109/JIOT.2019.2912022.

[47] M. Zolanvari, M. A. Teixeira and R. Jain, "Effect of Imbalanced Datasets on Security of Industrial IoT Using Machine Learning," 2018 IEEE International Conference on Intelligence and Security Informatics (ISI), Miami, FL, 2018, pp. 112-117, doi: 10.1109/ISI.2018.8587389.

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3057766, IEEE Access

[48] Kurniawan, H. A. Santoso, M. A. Soeleman and A. Z. Fanani, "Intrusion Detection System as Audit in IoT Infrastructure using Ensemble Learning and SMOTE Method," 2019 5th International Conference on Science in Information Technology (ICSITech), Yogyakarta, Indonesia, 2019, pp. 205-210, doi: 10.1109/ICSITech46713.2019.8987524.

[49] Bhardwaj, A., Al-Turjman, F., Kumar, M., Stephan, T., & Mostarda, L. (2020). Capturing-the-Invisible (CTI): Behavior-based Attacks Recognition in IoT-oriented Industrial Control Systems. IEEE Access, 1–1. doi:10.1109/access.2020.2998983

[50] Ferrag, Mohamed Amine, Leandros Maglaras, Helge Janicke, and Richard Smith. "Deep learning techniques for cyber security intrusion detection: a detailed analysis." In 6th International Symposium for ICS & SCADA Cyber Security Research 2019 6, pp. 126-136. 2019.

[51] Li, Y., Xu, Y., Liu, Z., Hou, H., Zheng, Y., Xin, Y., Cui, L. (2019). Robust Detection for Network Intrusion of Industrial IoT Based on Multi-CNN Fusion. Measurement, 107450. doi:10.1016/j.measurement.2019.107450.

[52] Zhang, Y., Bingham, C., Martínez-García, M., & Cox, D. (2017). Detection of Emerging Faults on Industrial Gas Turbines Using Extended Gaussian Mixture Models. International Journal of Rotating Machinery, 2017, 1–9. doi:10.1155/2017/5435794

[53] AL-Hawawreh, M., Moustafa, N., & Sitnikova, E. (2018). Identification of malicious activities in industrial internet of things based on deep learning models. Journal of Information Security and Applications, 41, 1–11. doi:10.1016/j.jisa.2018.05.002

[54] Hijazi, Ahmad, Abed El Safadi, and Jean-Marie Flaus. "A Deep Learning Approach for Intrusion Detection System in Industry Network." In BDCSIntell, pp. 55-62. 2018.

[55] O. Ibitoye, O. Shafiq and A. Matrawy, "Analyzing Adversarial Attacks against Deep Learning for Intrusion Detection in IoT Networks," 2019 IEEE Global Communications Conference (GLOBECOM), Waikoloa, HI, USA, 2019, pp. 1-6, doi: 10.1109/GLOBECOM38437.2019.9014337.

[56] Bae, G., Jang, S., Kim, M., & Joe, I. (2019). Autoencoder-Based on Anomaly Detection with Intrusion Scoring for Smart Factory Environments. Springer Series on Fluorescence, 414-423.

[57] Jafar A. Alzubi, Ramachandran Manikandan, Omar A. Alzubi, Issa Qiqieh, Robbi Rahim, Deepak Gupta, Ashish Khanna, Hashed Needham Schroeder Industrial IoT based Cost Optimized Deep Secured data transmission in cloud, Measurement, Volume 150,2020,107077,ISSN 0263-2241,https://doi.org/10.1016/j.measurement.2019.107077.

[58] Jiayan, Z., Fei, L., Haoxi, Z., Ruxiang, L., & Yalin, L. (2019). Intrusion Detection System using Deep Learning for In-vehicle Security. Ad Hoc Networks, 101974. doi:10.1016/j.adhoc.2019.101974

[59] Ankang Chu, Yingxu Lai, Jing Liu, "Industrial Control Intrusion Detection Approach Based on Multiclassification GoogLeNet-LSTM Model", Security and Communication Networks, vol. 2019, Article ID 6757685, 11 pages, 2019. https://doi.org/10.1155/2019/6757685

[60] Li, X., Xu, M., Vijayakumar, P., Kumar, N., & Liu, X. (2020). Detection of Low-frequency and Multi-stage Attacks in Industrial Internet of Things. IEEE Transactions on Vehicular Technology, 1–1. doi:10.1109/tvt.2020.2995133

[61] Park, S., Li, G. & Hong, J. A study on smart factory-based ambient intelligence context-aware intrusion detection system using machine learning. J Ambient Intell Human Computer 11, 1405–1412 (2020). https://doi.org/10.1007/s12652-018-0998-6

[62] J. Gao et al., "Omni SCADA Intrusion Detection Using Deep Learning Algorithms," in IEEE Internet of Things Journal, doi: 10.1109/JIOT.2020.3009180.

[63] Yan, X., Xu, Y., Xing, X., Cui, B., Guo, Z., & Guo, T. (2020). Trustworthy Network Anomaly Detection Based on an Adaptive Learning Rate and Momentum in IIoT. IEEE Transactions on Industrial Informatics, 1–1. doi:10.1109/tii.2020.2975227

[64] J. Choi, Y. Shin and S. Cho, "Study on information security sharing system among the industrial IoT service and product provider," 2018 International Conference on Information Networking (ICOIN), Chiang Mai, 2018, pp. 551-555.

[65] Eden, P., Blyth, A., Jones, K., Soulsby, H., Burnap, P., Cherdantseva, Y., & Stoddart, K. (2017). SCADA System Forensic Analysis Within IIoT. Cybersecurity for Industry 4.0, 73–101.

[66] T. Guo, D. Khoo, M. Coultis, M. Pazos-Revilla and A. Siraj, "Poster Abstract: IoT Platform for Engineering Education and Research (IoT PEER)–Applications in Secure and Smart Manufacturing," 2018 IEEE/ACM Third International Conference on Internet-of-Things Design and Implementation (IoTDI), Orlando, FL, 2018, pp. 277-278, doi: 10.1109/IoTDI.2018.00038.

[67] Kirupakar, J., Shalinie, S. M. (2019). Situation Aware Intrusion Detection System Design for Industrial IoT Gateways. 2019 International Conference on Computational Intelligence in Data Science (ICCIDS). doi:10.1109/iccids.2019.8862038

[68] N. E. Petroulakis et al., "SEMIoTICS Architectural Framework: End-to-end Security, Connectivity and Interoperability for Industrial IoT," 2019 Global IoT Summit (GIoTS), Aarhus, Denmark, 2019, pp. 1-6, doi: 10.1109/GIOTS.2019.8766399.

[69] Arshad, J., Azad, M. A., Abdeltaif, M. M., & Salah, K. (2019). An intrusion detection framework for energy constrained IoT devices. Mechanical Systems and Signal Processing, 106436. doi:10.1016/j.ymssp.2019.106436

[70] Aydogan, E., Yilmaz, S., Sen, S., Butun, I., Forsstrom, S., & Gidlund, M. (2019). A Central Intrusion Detection System for RPL-Based Industrial Internet of Things. 2019 15th IEEE International Workshop on Factory Communication Systems (WFCS). doi:10.1109/wfcs.2019.8758024

[71] Dong, RH, Wu, DF, Zhang, QY. Traffic characteristic map-based intrusion detection model for industrial internet. Int J NetwSecur 2018; 20(2): 359–370.

[72] Liang, W., Li, K.-C., Long, J., Kui, X., & Zomaya, A. Y. (2019). An Industrial Network Intrusion Detection Algorithm based on Multi-Feature Data Clustering Optimization Model. IEEE Transactions on Industrial Informatics, 1–1. doi:10.1109/tii.2019.2946791

[73] Zeeshan Ali Khan, Peter Herrmann, "Recent Advancements in Intrusion Detection Systems for the Internet of Things", Security and Communication Networks, vol. 2019, Article ID 4301409, 19 pages, 2019. https://doi.org/10.1155/2019/4301409

[74] H. Boyes, B. Hallaq, J. Cunningham, T. Watson, The industrial internet of things (iiot): An analysis framework,Computers in Industry 101 (2018) 1 - 12.

[75] L. D. Xu, W. He, S. Li, Internet of things in industries: A survey, IEEE Transactions on Industrial Informatics 10 (4)1180 (2014) 2233-2243.

[76] E. Oztemel, S. Gursev, Literature review of industry 4.0 and related technologies, Journal of Intelligent Manufacturing.URL https://doi.org/10.1007/s10845-018-1433-8

[77] V. Alcacer, V. Cruz-Machado, Scanning the industry 4.0: A literature review on technologies for manufacturing systems, Engineering Science and Technology, an International Journal, 22(3) (2019) 899 - 919.

[78] Rubio, Juan Enrique, Cristina Alcaraz, Rodrigo Roman, and Javier Lopez. "Analysis of Intrusion Detection Systems in Industrial Ecosystems." In SECRYPT, pp. 116-128. 2017.

PLS JAYALAXMI is a PhD scholar in Lovely Professional University -Punjab and also working as an assistant professor in Bhavans Vivekananda College. She has completed her master's from IGNOU in 2018. Her research interest includes Cybersecurity, Intrusion detection, Banking fraud identification, Authentication in IoT networks etc. She has many research articles in these areas to her credit.

RAHULSAHA is working as an Associate Professor in Lovely Professional University, Punjab India and did his B.Tech from Academy of Technology, West Bengal in Computer Science Engineering, M.Tech and PhD from Lovely Professional University, Punjab India with area of specialization in Cryptography, Position and Location computation in Wireless Sensor Networks. He has many publications in well renowned International journals and Conferences.

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3057766, IEEE Access

GULSHAN KUMAR received his Ph.D. in Computer Science from Lovely Professional University (L.P.U.), Punjab, India. Currently, he is working as Assistant Dean and Associate Prof. with the Division of Research and Development, L.P.U. His current research interests include cyber physical systems, blockchain, edge and cloud computing. Kumar has authored and co-authored more than 35 research papers including international journals (IEEE IoT, IEEE Access, Sensors, IJDSN etc.) and conferences. He is a member of various technical organizations such as IEEE, ISCA etc.

TAI-HOON KIM received the B.E. and M.E. degrees from Sungkyunkwan University, South Korea, and the Ph.D. degrees from the University of Bristol, U.K., and the University of Tasmania, Australia. He is currently with Beijing Jiotong University, Beijing, China. His main research areas are security engineering for IT products, IT systems, development processes, and operational environments

NEERAJ KUMAR (SENIOR MEMBER, IEEE) received the Ph.D. degree in CSE from Shri Mata Vaishno Devi University, Katra, India. He was a Postdoctoral Research Fellow with Coventry University, Coventry, U.K. He is a Visiting Professor at Coventry University, Coventry, U.K. He is currently a Full Professor with the Department of Computer Science and Engineering, Thapar University, Patiala, India. He has published more than 300 technical research papers in leading journals and conferences from IEEE, Elsevier, Springer, John Wiley, and so on. Some of his research findings are published in top-cited journals such as the IEEE TIE, IEEE TDSC, IEEE TITS, IEEE TCC, IEEE TKDE, IEEE TVT, IEEE TCE, IEEE Netw., IEEE Comm., IEEE WC, IEEE IoTJ, IEEE SJ, FGCS, JNCA, and ComCom. He has guided many Ph.D. and M.E./M.Tech. students. His research is supported by fundings from Tata Consultancy Service, Council of Scientific and Industrial Research (CSIR), and the Department of Science and Technology. He has awarded the best research paper awards from IEEE ICC 2018 and IEEE Systems Journal 2018. He is leading the research group Sustainable Practices for the Internet of Energy and Security (SPINES), where group members are working on the latest cutting edge technologies. He is a TPC member and reviewer of many international conferences across the globe.

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/