Journal of Electronics, Computer Networking and Applied Mathematics
ISSN: 2799-1156
Vol: 02, No. 05, Aug-Sept 2022
http://journal.hmjournals.com/index.php/JECNAM
DOI: https://doi.org/10.55529/jecnam25.1.22

Overview of Innovative Trends for Industrial Internet of Things Adoption for Achieving High-Quality Deployment

Aminu Adamu Ahmed[1*], Jibril Hussein Kawure[2], Ibrahim Maimunatu Ya'u[3], Bashir Adamu[4], Zakiya Yahaya Shehu[5]

[1, 4]Department of Information and Communication Technology, Federal Polytechnic Kaltungo, Nigeria*
[2] Centre Director, Professor Iya Community Resource Centre, Bauchi, Nigeria
[3, 5]Department of Management and Information Technology, Abubakar Tafawa Balewa University, Bauchi, Nigeria

Email: [2]kawurejibreel@live.com, [3]yimaimunatu.pg@atbu.edu.ng, [4]elnafaty4@gmail.com, [5]zaksan.bello@gmail.com
Corresponding Email: [1]aminuaa.inkil@gmail.com*

Received: 20 April 2022 **Accepted:** 10 July 2022 **Published:** 17 August 2022

Abstract: Purpose – The aim of this study is to bring about a comprehensive overview of innovative tends (technologies) employ for IIoTs adoptions for achieving high-quality deployment.
Methodology/Approach – This study initially identified 702 different articles from reputable research databases namely Science Direct, Emerald Insight, Wiley Online Library, Google Scholar, IEEE Access and Z Online Library from the years 2018 to June, 2022. A total of 32 articles were selected after undergoing a screening of its titles, keywords, abstracts and contents inclusion and exclusion for rigorous analysis. The data extracted were analysed and presented in form of descriptive statistics (tables, frequency, figures and charts) using Microsoft Excel software.
Findings –The results carefully analyse how these trends influence the adoption of IIoTs in the industries.
Novelty/value – Being the most growing innovation for industrial internet of things using industry 4.0 technologies have gradually changed the way traditional industries operate.

Keywords: Innovative Trends;Internet of Things (IoTs); Industrial IIoTs Adoption; Application; and Benefits;

Journal of Electronics, Computer Networking and Applied Mathematics
ISSN: 2799-1156
Vol: 02, No. 05, Aug-Sept 2022
http://journal.hmjournals.com/index.php/JECNAM
DOI: https://doi.org/10.55529/jecnam25.1.22

1. INTRODUCTION

Industrial Internet of Things (IIoTs) is a new technological innovation that is derived from the emergence of Internet of Things (IoTs) using Industry 4.0 technologies. Both IoTs and IIoTs have used smart objects for collecting, sensing, monitoring, processing and communicating and share information about assigned tasks for achieving operations and processes automation in industrial settings (Prakash, Savaglio, Garg, Bawa & Spezzano, 2022). The concepts of IIoTs have been defined as application of IoTs in industries to automate various existing industrial operations and processes (Khan, Rehman, Zangoti, Afzal, Armi & Salah, 2020), it also be defined as interconnection of smart industrial machineries with wireless sensor network devices to sense, monitor, and execute an assigned tasks on the production life cycles (Khayyat, Khayyat, Abdel-Khalek & Mansour, 2022).

Nowadays, IIoTs have graduated to new innovations (trends) such as IIoTs for forensics services (Kebande, 2022), Supply-sided Energy modelling for improve energy utilization (Peng Peng, Liu, Geissdoerfer & Evans, 2021), modernize system for smart energy (Zhang, Chan & Zhou, 2018) and many more that could be seen in Table 2. IIoTs is a very important aspect of economic development in this era of digital age. The application of internet of things in industrial sectors forms internet of things today. The Internet is a short form of international network. With respect to this study the term internet refers to the use of computers and computer-related devices for communications and sharing of IT and non-IT resources. While we also referred industry as any organized setting where production and construction is taking place. Adoption of IIoTs is one of the fastest trends in production and construction industries using industry 4.0 technologies (Javaid, Haleem, Singh, Rab, & Suman, 2021). While the adoption of IIoTs have taken new dimensions because there is a reason behind the application of any IIoTs' innovative trends in every industry that wish to adopt for its operation and service automation. The reasons for IIoTs applications include: operations and processes transformations in the industries (Buetas et al., 2020; Chen, 2020; Prakash et al., 2022) Moreover, these operations and processes transformation have to do with IIoTs innovative trends which include: Deep/machine learning related trends (Khan & Al-badi, 2020; Liu et al., 2021; Nayak et al., 2021; Zhao, Li, Liu, Fan, & Lin, 2020; Ren, Sun, & Peng, 2020); Blockchain related trends (Chi et al., 2020; Hu & Li, 2021; Javaid et al., 2020; Khayyat et al., 2022); Security related trends (Ferretti et al., 2021; Javaid et al., 2021; Kebande, 2022; Kolisnyk et al., 2020; Shimei, 2020; Shuai et al., 2020); Energy related trends (Peng et al., 2021; Zhang et al., 2018; Oruganti, Khosla, & Thundat, 2020); and Smart factory related trends (Buetas et al., 2020; Chen, 2020; Prakash et al., 2022; Ning, Wang, Chen, & Liu, 2020; Duhaime, 2020; Kolla, et al. 2022) for more details about this trends, as well as its application purposes and benefits (see Table 2).

The IIoTs as new technological innovation that is derived from the emergence of IoTs. Both IoTs and IIoTs have required the use of some components namely: big data analytics; machine learning (machine-to-machine communication); automation; actuations; wireless sensor technology; cloud platforms; and Internet services (Javaid, & Sikdar, 2020; Serror, Hack, Henze, Schuba, & Wehrle, 2020). Consequently, the revolution of IIoTs have come from the persistent increase in demand for: *security and privacy* (degree of safety coupling devices); *reduction of energy consumption*; *improve latency* (time required for transmitting the data on

Journal of Electronics, Computer Networking and Applied Mathematics
ISSN: 2799-1156
Vol: 02, No. 05, Aug-Sept 2022
http://journal.hmjournals.com/index.php/JECNAM
DOI: https://doi.org/10.55529/jecnam25.1.22

a network); *improve throughput* (maximizing volume of data transmission across network); *scalability* (number of accommodated devices), *ensure automation of operations and processes* and *reliable topology* (interconnection of devices). Therefore, industrial practices have been revolutionized by Industry 4.0 technology, it has changes the way industries are conducting its daily operations. In addition, this study underpinned some perceived benefits of IIoTs application. These benefits include: ensuring end-to-end security (protection), managing energy (power) usage, system integration and upgrade, latency and throughput, performance and optimization, reliability, efficiency and availability of smart objects for IIoTs adoption.

In a nutshell, the sole aim of this study is to answer the research questions: what constitutes IIoTs and what made its various innovative trends different from one another. Even though there are few researchers focused on IIoTs innovative trends which result in limited number of studies concerning its adoption and trends. Therefore, this study intends to bring about a comprehensive overview of innovative technologies (trends) of IIoTs for achieving high-quality development.

2. Literature Review and Related Studies

The concept of IoTs and IIoTs are dynamic worldwide information network made up of devices that can connect to the Internet, including radio frequency identification (RFID), sensors, actuators, and other instruments and smart appliances that are rapidly becoming a vital part of the Internet. Numerous IoT solutions have recently entered the industrial sector, according to the analysts. These solutions are based on well-known notions of context-aware computing. This study aims to provide a conceptual framework and guidelines for the creation of context-aware products in the IoT paradigm. Additionally, it thoroughly analyses the market's offerings of IoT goods and identifies any trends and research areas that could be important. We examined a sizable number of IoT solutions available on the market for industry in our survey. The five market groups we've divided up the IoT solutions into are smart wearables, smart homes, smart cities, smart environments, and smart enterprises. Finally, we outlined and discussed seven key takeaways as well as potential directions for further research and development in the field of context-aware computing. Our ultimate objective is to provide a foundation that aids in comprehending previous IoT market events so that researchers may more effectively and efficiently plan for the future (Perera & Liu, 2015).

In prior research, Ren et al., (2020), a deep reinforcement learning (DRL) based on fog access point (F-AP) selection technique for compute offloading situations in the IIoT. A multi-agent configuration is used to alleviate the limitation that standard DRL systems have. The most critical failures in an IIoT system are server failure and power cable failure. Measures must be taken to ensure the high reliability of the server and power cables. One of the recommended methods to increase their reliability is the backup method for the server, by duplication (Kolisnyk et al., 2020).

It was highlighted that the Industry 4.0 technologies can have an influence on regular active monitoring measures. Identifying a possible issue to an attacker might be important for future issue identification and prevention. Information security and incidents assessment concepts and methods have defined standards to speed up digital investigations. This can

Journal of Electronics, Computer Networking and Applied Mathematics
ISSN: 2799-1156
Vol: 02, No. 05, Aug-Sept 2022
http://journal.hmjournals.com/index.php/JECNAM
DOI: https://doi.org/10.55529/jecnam25.1.22

indeed not be transformed and incorporated into modern IIoT contexts (Kebande, 2022). However, IIoT issues cannot be solved using blockchain in its original form with traditional system requirements. There was a new proposed architecture that suggests deployment of traditional and modern system of checkpoint mechanism. It was also suggested a design that is capable to offers adequate security integrity while being scalable and able to handle the continuously growing transaction load associated with industrial networks (Javaid et al., 2020). IIoTs to provide security of information using blockchain technology for cryptographic pixel value in the image, which ensures the security and privacy of the images. Future extensions could include light-weight cryptographic techniques with biometric authentication schemes (Khayyat et al., 2022). By examining IIoTs technologies and its use in manufacturing workshops, the prior study suggests a reference design and development roadmap for smart factories. The shop floor's real-time status can be automatically gathered, giving the higher-level planning management department a solid decision-making basis (Chen, 2020).

The historical development of computer systems and the rising popularity of distributed energy are comparable. The same trend in energy technology is enabling enterprises and people to buy and operate their own energy systems, much as smaller size and cheaper cost of computers have allowed individuals to own and run their own computing power. IITs offer the benefit of combining information in real-time, enabling significantly quicker decision-making than a conventional network. It may also manage the substantial control signal flow of dispersed energy assets using the most recent IT methods, such as big data or cloud computing (Zhang et al., 2018).

Requirement of IIoTs Adoption

In this study we underlined some of the IIoTs adoption's requirements as a general rules of adoption of every technology, there must be resources available. These resources are usually technology products that are made for use to create other products or services, among which include: big data analytics; machine to machine interaction; hardware & software connectivity; cloud computing platform; machine learning (see Figure 2).

Industrial Revolutions

Machado et al. (2022) highlights industrial revolutions in four different phases with corresponding periods (see, figure 1):

- 1st Industrial Revolution *for mechanized productions,*
- 2nd Industrial Revolution *for mass productions,*
- 3rd Industrial Revolution *for Internet evolution and automations,*
- 4th Industrial Revolution *for IIoTs (Industry 4.0*).

Journal of Electronics, Computer Networking and Applied Mathematics
ISSN: 2799-1156
Vol: 02, No. 05, Aug-Sept 2022
http://journal.hmjournals.com/index.php/JECNAM
DOI: https://doi.org/10.55529/jecnam25.1.22

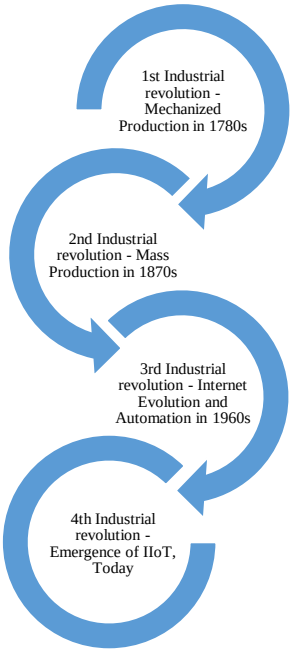

Figure 1. Industrial Revolutions
Source: Authors

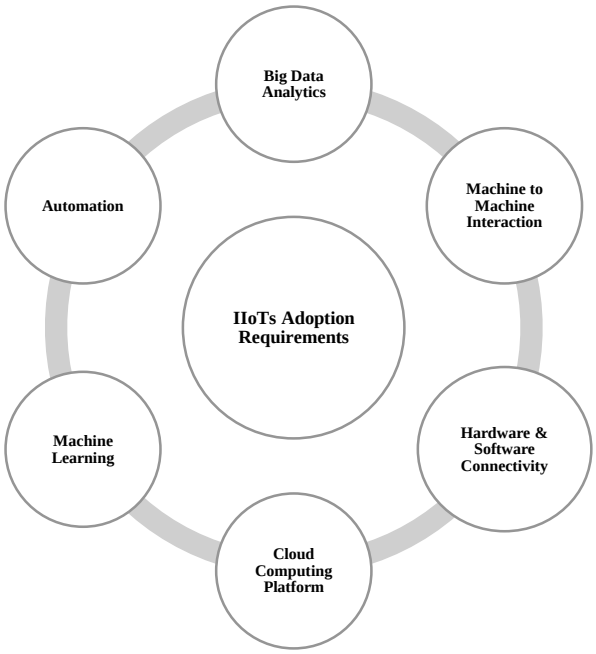

Figure 2. IIoTs Requirements
Source: Authors

Differences between IoTs and IIoTs

It is well-known fact that the evolution of IoTs is one of the predominant factors that helps in the IIoTs into being. Despite being, parent-child relation, the IoTs has its reasons for adoption and usage and so for IIoTs. Some of the reasons of IoTs adoption include design, implementation and usage of: smart city, smart home, smart transport, etc., on the other hand, the IIoTs have been used for design, implementation and usage to transform industrial operations and processes industries with the help of industry 4.0 technologies as a modern way of production of goods and services. For more details on comparisons between IoTs and IIoTs are well explained as illustrates in Table 1.

Table 1. Comparison and Contrast between IoTs and IIoTs

Comparison	**IoTs**	**IIoTs**
Target	Satisfying individuals	Satisfying operations and processes life cycles
Level of Application	Consumers level	Industrial level
Machine to Machine Communication	Narrow	Wide
Acceptance & Usage	Only for individual needs	For industrial needs
Service model	Human oriented	Machine oriented
Communication	Mostly wireless	Both wired and wireless

Journal of Electronics, Computer Networking and Applied Mathematics
ISSN: 2799-1156
Vol: 02, No. 05, Aug-Sept 2022
http://journal.hmjournals.com/index.php/JECNAM
DOI: https://doi.org/10.55529/jecnam25.1.22

Business model	Mostly commercial sectors	Mostly industrial sectors
Data management	Medium data	Huge amount of data
	Mostly machine-to-human communication	Machine-to-machine communication

3. METHODOLOGY

The sole of aim of this study is to bring a comprehensive overview of innovative trends (energy, latency, throughput, scalability and many others) for IIoTs adoption. The study pinpoints five IIoTs related trends which include: deep/machine learning related trends; blockchain related trends; security related trends; energy related trends and smart factory related trends (see Table 3). Various articles have been traced from trustworthy research databases namely: Science Direct; Emerald Insight; Wiley Online Library; Google Scholar; IEEE Access and Z Online Library latest from the years 2018 to June, 2022 (see Figure 3). At first, this study identified 702 different articles at the end 27 articles were selected after meeting titles, keywords, abstracts and contents inclusion and exclusion criteria for rigorous analysis.

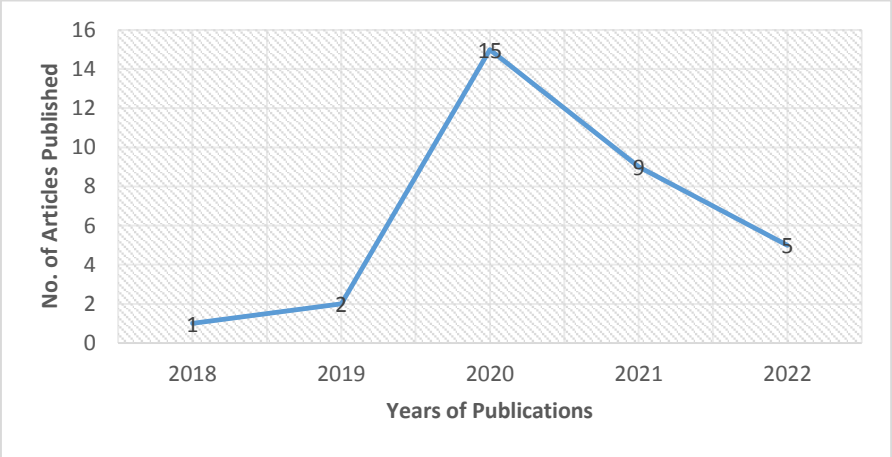

Figure 3. Distribution of articles over time

Search & Screening Strategy

The study employed Boolean operators (AND, OR, and/or combinations of the two) as searching procedure and screening using literature search, identification filtration, reliability and validity, inclusion, and analysis (SIFRIA). Initially, (Adoption OR Application of Industrial Internet of Things) and (Smart Industry OR (Industry 4.0)), hence, SIFRIA flowchart was applied using titles, abstracts, keywords, and entire content of the articles for inclusion and exclusion in the lists of appropriate articles that would be undergone rigorous analysis (see Figure 4 and Table 2).

Journal of Electronics, Computer Networking and Applied Mathematics
ISSN: 2799-1156
Vol: 02, No. 05, Aug-Sept 2022
http://journal.hmjournals.com/index.php/JECNAM
DOI: https://doi.org/10.55529/jecnam25.1.22

Method of Data Analysis

The data extracted were analysed and presented in form of descriptive statistics (tables, frequency, figures and charts) using Microsoft Excel software. The results carefully analyse how these trends influence the adoption of IIoTs in the industries.

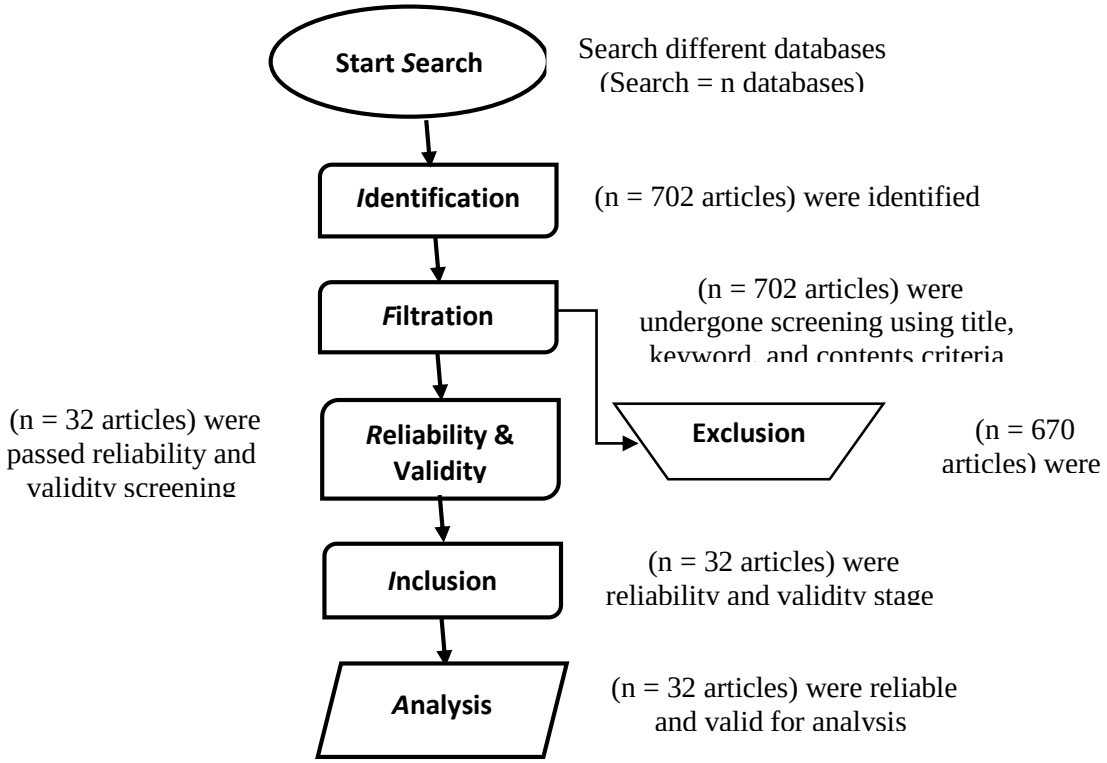

Figure 4. SIFRIA Flowchart adapted from (Ahmed, Saidu & Kawure, 2022)

4. RESULTS AND DISCUSSIONS

As stated earlier this study aims to bring a comprehensive overview of IIoTs innovative trends. In our study we classified IIoTs innovative trends into five namely: Deep/Machine Learning related; Blockchain related; Security related; Energy related and Smart Factory related trends as stated in table 3 and figure 4.

Table 2. Articles inclusion and exclusion criteria of study

Inclusion	Exclusion
▪ Related to IIoTs	▪ Not related to IIoTs
▪ Journal or conference published 2018 to June 2022	▪ Not journal or conference published 2018-June 202
▪ Full-text not only abstract	▪ Not full-text or only abstract
▪ Written in English	▪ Not written in English
▪ Passed the screening (reliability & validity)	▪ Not passed the screening
▪ Undergone a peer-review	▪ Not undergone peer-review

Journal of Electronics, Computer Networking and Applied Mathematics
ISSN: 2799-1156
Vol: 02, No. 05, Aug-Sept 2022
http://journal.hmjournals.com/index.php/JECNAM
DOI: https://doi.org/10.55529/jecnam25.1.22

▪ Published in one of the recognized journal or conference	▪ Not published in one of the recognized journal or conference

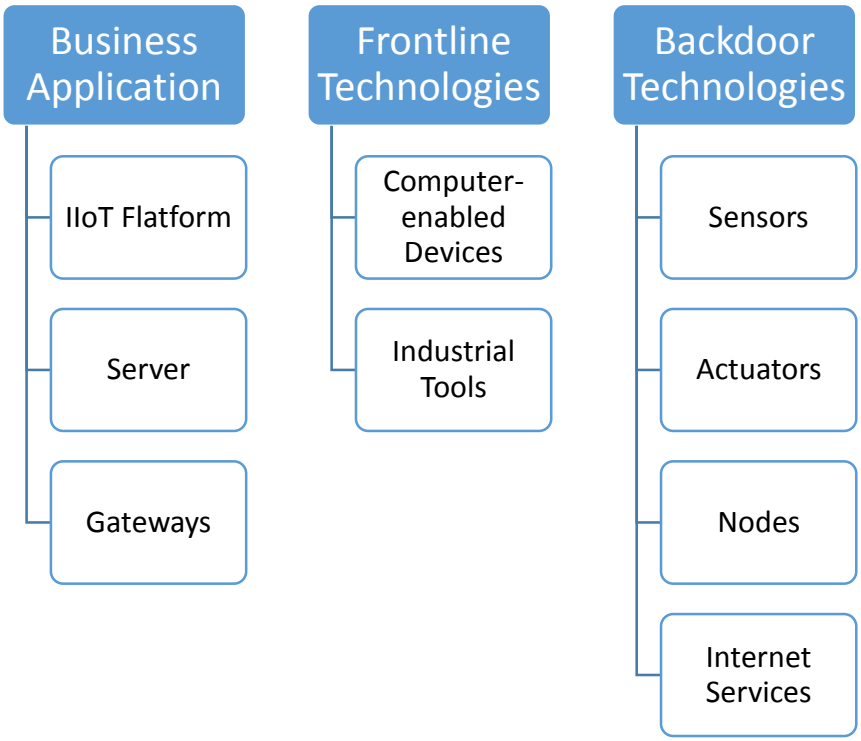

Figure 5: IIoTs Infrastructural Design

Deep/Machine Learning Related Trends

The deep and machine learning trends appeared 6 times out of the total of 32 number of articles selected for analysis. It was revealed in the prior studies that IIoTs innovative trends diffused in most of the industries around the globe. However, adoption and usage of these trends depend on the specific industrial application purpose. As some industries adopt one or more of the trend to transform its operations whereas some for processes. Various trends are discussed under this section. With regards to deep/machine learning, the direct transaction among machines is improved in terms of intelligence, real-time responsiveness, and security. Different situations might involve peer-to-peer (P2P) distributed energy transfers. On the basis of blockchain, a P2P learning transaction mechanism for the IIoT was suggested. To guarantee the transparency, openness, and non-tampering of credit ratings, smart contracts and credit value appraisal are used. To encourage the reliability of transaction nodes, an energy currency incentive system is implemented. To increase transaction security and efficiency, P2P direct transactions based on credit value were developed (Hu & Li, 2021). Machine learning frameworks that are open source and focused on the industrial sector. Industries may greatly benefit from IIoTs data, which can be used to forecast customer demand and alter supply chains. Newcomers have trouble understanding and utilising the machine learning framework for data processing and machine learning models that is currently available. Five open source frameworks for building machine learning models have been described in a research. The study

Journal of Electronics, Computer Networking and Applied Mathematics
ISSN: 2799-1156
Vol: 02, No. 05, Aug-Sept 2022
http://journal.hmjournals.com/index.php/JECNAM
DOI: https://doi.org/10.55529/jecnam25.1.22

provides more evidence of data production in an IoT setting. To create a predictive maintenance model, future work will use Tensorflow on industrial IoT data from the oil and gas sector (Khan & Al-badi, 2020).

Table 3: Comparison of Open Source Machine Learning Model Development Environment

Machine Leaning Frameworks	Programming Language	Platforms	Maitainer	Applicability
Tensorflow	Python, C++	Windows, MacOS, Linux	Google	Deep speech, Smart reply, Computer recognition
Microsoft Cognitive Toolkit	Python, C++, C#	Windows, Linux	Microsoft Research	Handwriting image, voice recognition
Caffe	C, C++, Python, MATLAB	Ubuntu, MacOS, Windows	BVLC	Training models for classification
HO2	Java, Python	Windows, Linux	HO2	Creates productionize machine learning models
Torch	Lua	Linux, Android, MacOS, iOS, Windows	Ronan Clement, Koray, Soumith	Detecting and solving hardware problems for data flows
PyTorch	Python	Linux, Android, MacOS, iOS, Windows	Ronan Clement, Koray, Soumith	Reinforcement learning and scaled production of models.

Source: (Khan & Al-badi, 2020)

By utilising automation and IoT, the IIoTs enhances manufacturing and production operations. Machine learning algorithms can help with automated control of sophisticated IIoT systems. Despite substantial performance gains, the security risks posed by the IoT's extensive interconnectedness must be addressed. In this article, we look into IIoT system-related DQN-based controller security concerns. We create two generic assaults that an adversary might use to hinder the performance of these controllers during either the training phase or the post-training phase. To approximate the reward function of a trained DRL-based controller, we employed the maximum entropy in Inverse RL. Then, we launched the function-based and performance-based assaults on the target using the approximation of the reward function (X. Liu et al., 2021).

Journal of Electronics, Computer Networking and Applied Mathematics
ISSN: 2799-1156
Vol: 02, No. 05, Aug-Sept 2022
http://journal.hmjournals.com/index.php/JECNAM
DOI: https://doi.org/10.55529/jecnam25.1.22

Blockchain Related Trends

Blockchain related trends appeared only 5 times out of 32 selected samples. Prior studies on the blockchain-based IIoT is extremely resistant to phishing and other potential attacks. Because the same data is saved on any and all nodes in the blockchain, there is no possibility of data loss. The system will be implemented and shown in the future for effective approaches including self-service as well as on manufacturing (Kumar et al., 2021) and many more innovative trends (see Table 2).

Security Related Trends

Security-related trends was among the top two innovative trends which appeared 9 times out of 32 total number of sample articles. In order to account for the effects of assaults on the IIoT system's subsystems in the event of a firewall failure, a Markov model of the system was proposed. According to research, when a firewall malfunctions, the availability function rapidly drops to a critical value (Kolisnyk et al., 2020). A network of connected sensors, instruments, and other equipment makes up the IIoTs. The use of image encryption algorithms has grown in recent years. This paper introduces a novel Hopfield Chaotic Neural Network-Enabled Shark Smell Optimization. A composite Chaotic Map (CM), which is incorporated into staged logistic and tent maps, is used by the proposed SSO-HCNN model. To assess if the model outperformed cutting-edge techniques, a series of simulations using benchmark test photos were run (Khayyat et al., 2022). Ferretti et al. (2021), revealed that cyber-physical devices and linkages to business processes that provide flexible manufacturing, remote monitoring, control, and maintenance are added benefits of modern industrial systems. These authors provide a novel architecture that use authorization delegation processes to control access to resources in industrial systems. It ensures the ability to audit permissions granted by other parties, uncover wrongdoing, and stop potential threats. It was also highlighted that a method that enables auditing of authorisation processes used in industrial IoT settings, which are characterised by highly secure air-gapped systems and confined device placement (see Table 3).

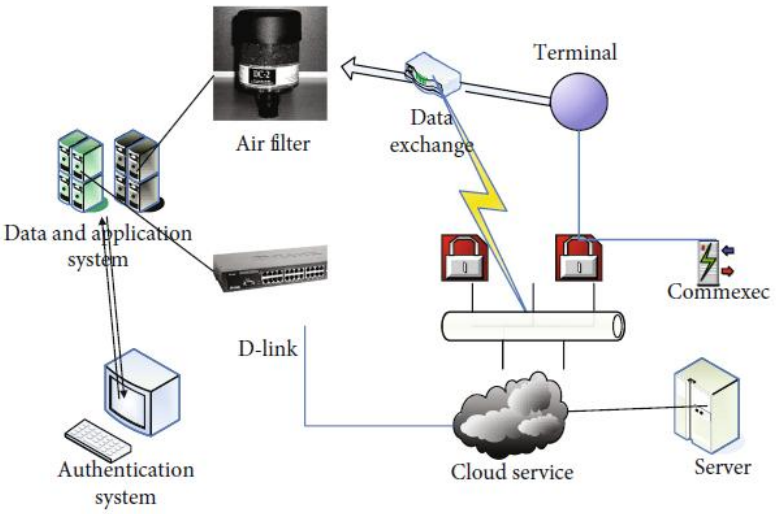

Figure 6: Security Architecture (Lu, 2022)

Journal of Electronics, Computer Networking and Applied Mathematics
ISSN: 2799-1156
Vol: 02, No. 05, Aug-Sept 2022
http://journal.hmjournals.com/index.php/JECNAM
DOI: https://doi.org/10.55529/jecnam25.1.22

Data Encryption Standard encryption algorithm is a symmetric password encryption method.

Energy Related Trends

Energy is the least trend with least appearance of 3 out of 32 total number of sample articles. The prior studies highlights some countermeasures such as NICE EOS is being developed as an open architectural framework for nano-grid for energy control and management under the NicerNet idea. The largest energy firm in China, Shenhua Group, has submitted a legitimate application in favour of it. a Mist-COMPUTING layer built on fractals and an associated DDS communication layer for efficient linked analysis amongst devices in real time. For big industry customers like Shenhua, the Industrial Smart Energy Consortium (ISEC) Initiative is suggested as one efficient method for developing industrial IoT laws and standards (Zhang et al., 2018).

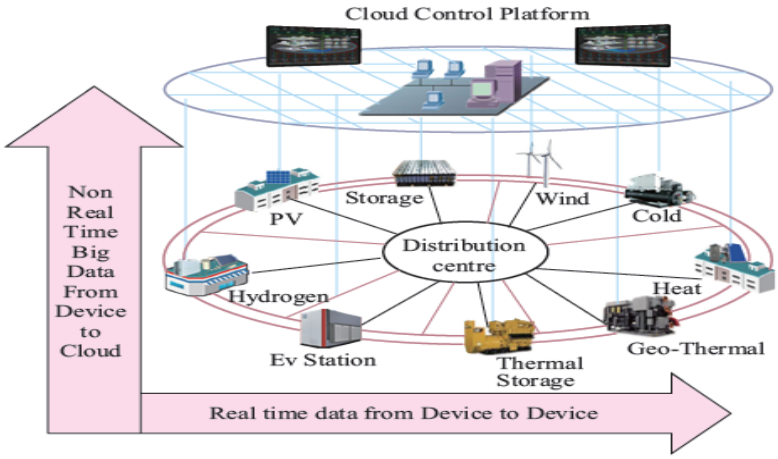

Figure 7: Smart Energy System (Zhang et al., 2018).

Smart Factory Related Trends

The smart factory-related trends is another top trend which appeared 9 times out of the total number of sample selected. There are some highlights on smart factories trends in prior studies such as the one by (Chen, 2020; Duhaime, 2020; W. Z. Khan et al., 2020; J. Liu et al., 2021). By utilising automation and IoT, the IIoTs enhances manufacturing and production operations. Machine learning algorithms can help with automated control of sophisticated IIoT systems. Despite substantial performance gains, the security risks posed by the IoT's extensive interconnectedness must be addressed. In this article, we look into IIoT system-related DQN-based controller security concerns. We create two generic assaults that an adversary might use to hinder the performance of these controllers during either the training phase or the post-training phase. To approximate the reward function of a trained DRL-based controller, we employed the maximum entropy in Inverse RL. Then, we launched the function-based and performance-based assaults on the target using the approximation of the reward function (X. Liu et al., 2021). The industrial IoT solution for manufacturing workshops is provided in light of the variety of on-site production data, high amounts of data, changing status, and strong correlation between data. Real-time and quality perspectives are used to analyse the system's performance. The basic elements of smart factories are the intelligent production workshops, which are built on the industrial IoT system. This article analyses the associated ideas of the

Journal of Electronics, Computer Networking and Applied Mathematics
ISSN: 2799-1156
Vol: 02, No. 05, Aug-Sept 2022
http://journal.hmjournals.com/index.php/JECNAM
DOI: https://doi.org/10.55529/jecnam25.1.22

current smart factory and suggests a reference design and development strategy for the latter. The outcomes demonstrate how well the system monitors data from the production line (Chen, 2020).

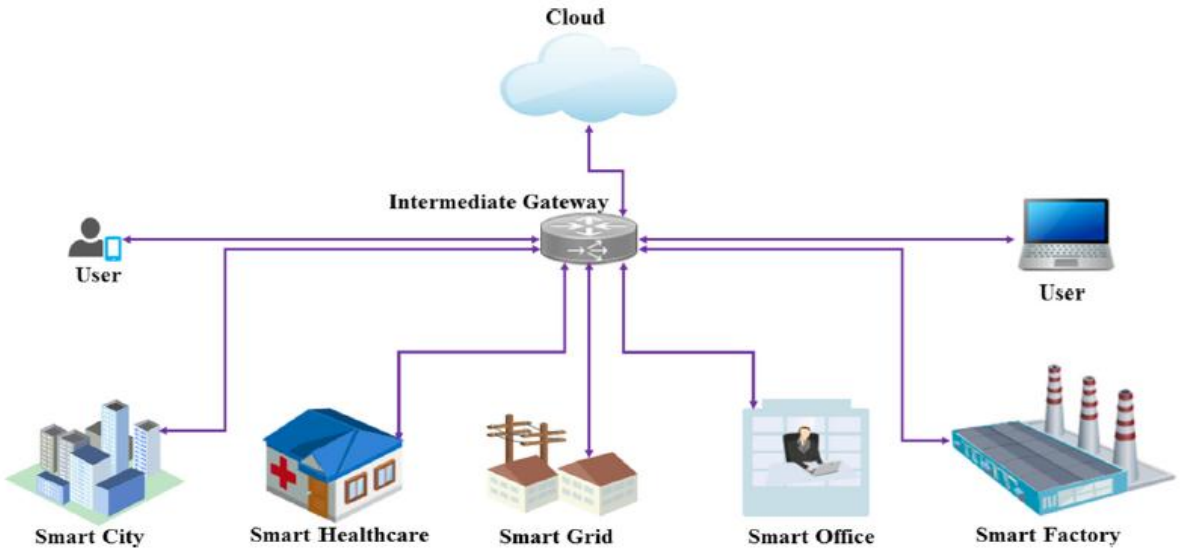

Figure 8: Smart System (Hussain et al., 2022)

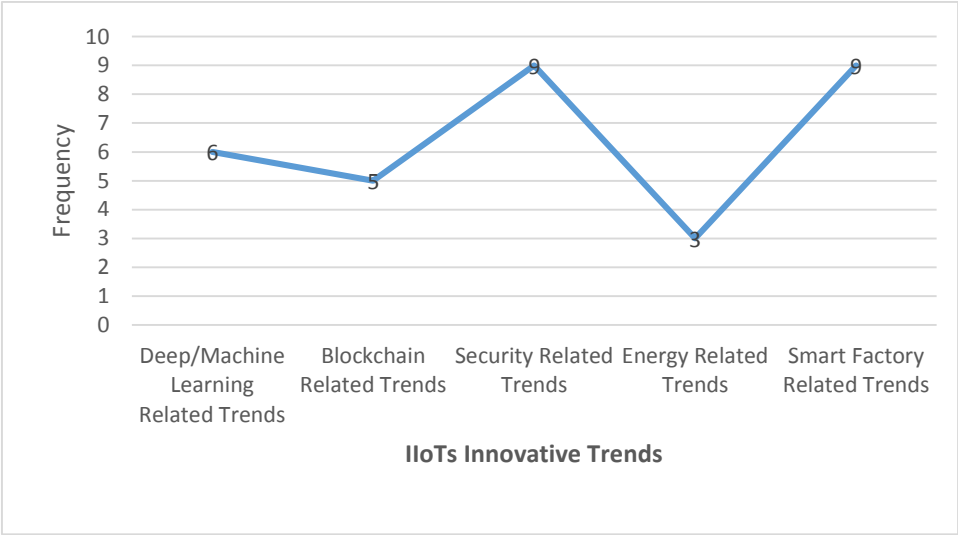

Figure 9. IIoTs Innovative Trends

Emerging IIoTs systems face dozens of new issues, including poor interoperability, uniqueness, security and reliability flaws, and resource constraints. Present form of blockchain approaches, which give solutions through better secrecy, can be used to tackle IIoT problems. The essay assesses the benefits of using the technology and explains the structure of such a system (Kumar et al., 2021). Based on the prior studies it was suggested solution that is in line with industrial architectural security and performance standards as well as the characterization

Journal of Electronics, Computer Networking and Applied Mathematics
ISSN: 2799-1156
Vol: 02, No. 05, Aug-Sept 2022
http://journal.hmjournals.com/index.php/JECNAM
DOI: https://doi.org/10.55529/jecnam25.1.22

of the industrial environment. The suggested solution may utilise current software services for a dependable deployment and complies with industry-standard authorisation and network communication standards. Its security is built on well-known cryptographic protocols, including common digital signature techniques and hash functions, and it enables all system participants to openly demonstrate wrongdoing (Ferretti et al., 2021). It will be necessary to engage specialised incident response teams from outside sources. Forensic investigation of complex occurrences may call for collaboration amongst many groups. It will be very difficult to achieve the strict criteria established by industrial environments if standards are not clearly defined or are not strictly adhered to (Tange et al., 2020). In order to satisfy the requirement of balancing generation and demand, two-way power flow control, data, and communications are being used as a result of the rise of renewable energy. In order to create a distributed energy network using Energy Operating System (EOS)-based assets and devices, we are using the same technique for the Internet of Everything (IoE) idea. This article covers a software and control platform powered by IIoT created in a lab for Shenhua Group as a part of the NICE Smart System Initiative. This campaign aims to draw together business partners, academic institutions, suppliers of modules and equipment, and other relevant parties (Zhang et al., 2018).

5. CONCLUSION

For the IIoTs throughout this study, we carried out an extensive literature investigation on deep learning, blockchain, security, energy, and smart factories-related trends. Our first search searches produced 702 potentially relevant publications; we finally chose 32 items out of the entire collection. These papers were thoroughly evaluated and analyzed in order to meet the goals of this study, resulting in the creation of this overview of these chosen publications. According to the review's findings, deep and machine learning trends, followed by security- and smart factories-related innovativeness, play a key role in the adoption and usage of IIoTs to replace conventional industrial operations and processes. However, among other trends, blockchain-related trends are the least well-liked, followed by energy-related trends.

Acknowledgement
We are really grateful to Allah (SWT) for allowing us the chance to conduct this research and for providing us with the necessary resources and environment. Second, we sincerely thank the distinguished authors for their significant contributions to the creation of this work. And thank God the authors have no competing interests. Finally, we would like to express our gratitude to the conference and/or journal reviewers, editors, and other board members for their excellent service.

6. REFERENCES

1. Ahmed, A. A., Saidu, A. A., & Kawure, J. H. (2022). The Role of Central Bank Digital Currency on Features , Perceived Benefits and Challenges Compared to Physical Currency. Traditional Journal of Law and Social Sciences (TJLSS), 1(1), 51–67. http://traditionaljournaloflaw.com/
2. Buetas, E., Abad, I., Cerrada, J. A., & Cerrada, C. (2020). A propagation breakdown

Journal of Electronics, Computer Networking and Applied Mathematics
ISSN: 2799-1156
Vol: 02, No. 05, Aug-Sept 2022
http://journal.hmjournals.com/index.php/JECNAM
DOI: https://doi.org/10.55529/jecnam25.1.22

management model for the industrial internet of things. Computers in Industry, 123, 103305. https://doi.org/10.1016/j.compind.2020.103305

3. Chen, W. (2020). Intelligent manufacturing production line data monitoring system for industrial internet of things. Computer Communications, 151(December 2019), 31–41. https://doi.org/10.1016/j.comcom.2019.12.035
4. Chi, J., Li, Y., Huang, J., Liu, J., Jin, Y., Chen, C., & Qiu, T. (2020). A secure and efficient data sharing scheme based on blockchain in industrial Internet of Things ☆. Journal of Network and Computer Applications, 167(June). https://doi.org/10.1016/j.jnca.2020.102710
5. Dhungana, D., Haselböck, A., Meixner, S., Schall, D., Schmid, J., Trabesinger, S., & Wallner, S. (2021). Multi-factory production planning using edge computing and IIoT platforms. The Journal of Systems & Software, 182, 111083. https://doi.org/10.1016/j.jss.2021.111083
6. Duhaime, S. (2020). Industrial Internet of Things Puts New Pressure on Traditional Control Systems. February, 14–15. https://doi.org/10.1002/opfl.1322
7. Ferretti, L., Longo, F., Merlino, G., Colajanni, M., & Puliafito, A. (2021). Verifiable and auditable authorizations for smart industries and industrial Internet-of-Things. Journal of Information Security and Applications, 59(April).
8. Hu, W., & Li, H. (2021). A blockchain-based secure transaction model for distributed energy in Industrial Internet of Things. Alexandria Engineering Journal, 60(1), 491–500. https://doi.org/10.1016/j.aej.2020.09.021
9. Huang, H., Ye, P., Hu, M., & Wu, J. (2022). A multi-point collaborative DDoS defense mechanism for IIoT environment. Digital Communications and Networks. https://doi.org/10.1016/j.dcan.2022.04.008
10. Hussain, S., Sajid, S., Ali, I., Xie, J., & Inukollu, V. N. (2022). Certificateless signature schemes in Industrial Internet of Things : A comparative survey. Computer Communications, 181(August 2021), 116–131. https://doi.org/10.1016/j.comcom.2021.10.010
11. Javaid, M., Haleem, A., Pratap, R., Rab, S., & Suman, R. (2021). Upgrading the manufacturing sector via applications of Industrial Internet of Things (IIoT). Sensors International, 2(September), 100129. https://doi.org/10.1016/j.sintl.2021.100129
12. Javaid, U., Sikdar, B., & Member, S. (2020). A Checkpoint Enabled Scalable Blockchain Architecture for Industrial Internet of Things. Transactions on Industrial Informatics, 3203(c), 1–9. https://doi.org/10.1109/TII.2020.3032607
13. Kan, C., Yang, H., & Kumara, S. (2018). Parallel computing and network analytics for fast Industrial Internet-of-Things (IIoT) machine information processing and condition monitoring. Journal of Manufacturing Systems, 46, 282–293. https://doi.org/10.1016/j.jmsy.2018.01.010
14. Kebande, V. R. (2022). Industrial internet of things (IIoT) forensics : The forgotten concept in the race towards industry 4 . 0. Forensic Science International: Reports, 5, 100257. https://doi.org/10.1016/j.fsir.2022.100257
15. Khalil, R. A., & Saeed, N. (2020). Network Optimization for Industrial Internet of Things (IIoT). 1472(c), 9–12. https://doi.org/10.1109/LSENS.2020.3002232
16. Khan, A. I., & Al-badi, A. (2020). Open Source Machine Learning Frameworks for

Journal of Electronics, Computer Networking and Applied Mathematics
ISSN: 2799-1156
Vol: 02, No. 05, Aug-Sept 2022
http://journal.hmjournals.com/index.php/JECNAM
DOI: https://doi.org/10.55529/jecnam25.1.22

Industrial Internet of Things. Procedia Computer Science, 170, 571–577. https://doi.org/10.1016/j.procs.2020.03.127

17. Khan, W. Z., Rehman, M. H., Zangoti, H. M., Afzal, M. K., Armi, N., & Salah, K. (2020). Industrial internet of things : Recent advances , enabling technologies and open challenges R. Computers and Electrical Engineering, 81, 106522. https://doi.org/10.1016/j.compeleceng.2019.106522
18. Khayyat, M. M., Khayyat, M. M., Abdel-khalek, S., & Mansour, R. F. (2022). Blockchain enabled optimal Hopfield Chaotic Neural network based secure encryption technique for industrial internet of things environment. Alexandria Engineering Journal, 61(12), 11377–11389. https://doi.org/10.1016/j.aej.2022.05.002
19. Kolisnyk, M., Kharchenko, V., & Piskachova, I. (2020). Availability Models of Industrial Internet of Things Wired System Considering Cyberattacks. 138–144.
20. Kumar, R. L., Khan, F., Kadry, S., & Rho, S. (2021). A Survey on blockchain for industrial Internet of Things. Alexandria Engineering Journal. https://doi.org/10.1016/j.aej.2021.11.023
21. Liu, J., Duan, Y., Wu, Y., Chen, R., Chen, L., & Chen, G. (2021). Information flow perception modeling and optimization of Internet of Things for cloud services. Future Generation Computer Systems, 115, 671–679. https://doi.org/10.1016/j.future.2020.10.012
22. Liu, X., Yu, W., Liang, F., Griffith, D., & Golmie, N. (2021). On deep reinforcement learning security for Industrial Internet of Things. Computer Communications, 168(January), 20–32. https://doi.org/10.1016/j.comcom.2020.12.013
23. Lu, Z. (2022). Encryption Management of Accounting Data Based on DES Algorithm of Wireless Sensor Network. 2022.
24. Machado, D., Anil, A., & Kumar, A. A. (2022). Retrofitting of legacy machines in the context of Industrial Internet Retrofitting of legacy machines in the context of Industrial Internet of Things (IIoT). Procedia Computer Science 200, 200, 62–70. https://doi.org/10.1016/j.procs.2022.01.205
25. Magomadov, V. S. (2020). The Industrial Internet of Things as one of the main drivers of Industry The Industrial Internet of Things as one of the main drivers of. I O P Conference Series: Materials Science and Engineering, 862((2020) 032101), 0–4. https://doi.org/10.1088/1757-899X/862/3/032101
26. Mouapi, A. (2020). Design of 900 MHz RadioFrequency Energy Harvesting Circuit for the Internet of Things Applications.
27. Nayak, S., Ahmed, N., & Misra, S. (2021). Deep Learning-Based Reliable Routing Attack Detection Mechanism for Industrial Internet of Things. Ad Hoc Networks, 123(August), 102661. https://doi.org/10.1016/j.adhoc.2021.102661
28. Peng, C., Peng, T., Liu, Y., Geissdoerfer, M., & Evans, S. (2021). Industrial Internet of Things enabled supply-side energy modelling for re fi ned energy management in aluminium extrusions manufacturing. Journal of Cleaner Production, 301, 126882. https://doi.org/10.1016/j.jclepro.2021.126882
29. Prakash, V., Savaglio, C., Garg, L., Bawa, S., & Spezzano, G. (2022). Cloud- and Edge-based ERP systems for Industrial Internet of Things and Smart Factory. Procedia Computer Science, 200, 537–545. https://doi.org/10.1016/j.procs.2022.01.251
30. Ren, Y., Sun, Y., & Peng, M. (2020). Deep Reinforcement Learning Based

Journal of Electronics, Computer Networking and Applied Mathematics
ISSN: 2799-1156
Vol: 02, No. 05, Aug-Sept 2022
http://journal.hmjournals.com/index.php/JECNAM
DOI: https://doi.org/10.55529/jecnam25.1.22

Computation Offloading in Fog Enabled Industrial Internet of Things. 3203(c), 1–10. https://doi.org/10.1109/TII.2020.3021024

31. Senathipathi, K., Kayalvili, S., Anitha, P., & Henna, K. J. C. (2021). Blockchain integrated IIOT – Future of IOT. Materials Today: Proceedings, xxxx, 17–20. https://doi.org/10.1016/j.matpr.2020.12.1051
32. Sengupta, J., Ruj, S., & Bit, S. Das. (2019). A comprehensive survey on attacks, security issues and blockchain solutions for IoT and IIoT. Journal of Network and Computer Applications, 102481. https://doi.org/10.1016/j.jnca.2019.102481
33. Serror, M., Hack, S., Henze, M., Schuba, M., & Wehrle, K. (2020). Challenges and Opportunities in Securing the Industrial Internet of Things. 3203(c), 1–12. https://doi.org/10.1109/TII.2020.3023507
34. Shimei, L. (2020). Design of Industrial Internet of Things Gateway with Multi-source data Processing. 232–236. https://doi.org/10.1109/ICCEA50009.2020.00058
35. Shuai, M., Xiong, L., Wang, C., & Yu, N. (2020). A secure authentication scheme with forward secrecy for industrial internet of things using Rabin cryptosystem. Computer Communications. https://doi.org/10.1016/j.comcom.2020.06.012
36. Singh, I., Centtea, D., & Elbestawi, M. (2019). IIoT and Cyber-Physical Systems Integration in the SEPT Learning Factory. Procedia Manufacturing, 31, 116–122. https://doi.org/10.1016/j.promfg.2019.03.019
37. Thundat, T. G. (2020). Wireless Power-Data Transmission for Industrial Internet of Things : Simulations and Experiments. 187965–187974.
38. Zhang, D., Chan, C. C., & Zhou, G. Y. (2018). Enabling Industrial Internet of Things (IIoT) towards an emerging smart energy system. Global Energy Interconnection, 1(1), 39–47. https://doi.org/10.14171/j.2096-5117.gei.2018.01.005
39. Zhao, Y., Wang, N., Li, Y., Zhou, R., & Li, S. (2020). A meta-analysis. 0(0). https://doi.org/10.1111/bjet.13002
40. Zhao, Y., Wang, N., Li, Y., Zhou, R., & Li, S. (2021). A meta-analysis. 52(1). https://doi.org/10.1111/bjet.13002

Table 3. Innovative trends for IIoTs adoption

S/N	Title	Application Purpose	Trend	Benefits	Source
1	A secure authentication scheme with forward security for IIoTs using Robin Cryptosystem	To prevent a malicious adversary from altering the data which may lead to have negative effect on decision	Secure Authentication Scheme using Cryptosystem	Security	(Shuai et al., 2020)
2	IIoTs forensic: The forgotten concept in the race towards industry 4.0	To examine appropriate methods, standard or processes for deploying IIoTs	IIoTs forensics	security	(Kebande, 2022)

Journal of Electronics, Computer Networking and Applied Mathematics
ISSN: 2799-1156
Vol: 02, No. 05, Aug-Sept 2022
http://journal.hmjournals.com/index.php/JECNAM
DOI: https://doi.org/10.55529/jecnam25.1.22

		forensic technology			
3	Cloud-and Edge-based ERP (C-ERP and E-ERP) systems for IIoTs and Smart factory	To underpin benefits & limitations associated with C-ERP & E-ERP	Cloud-and Edge-based ERP system	Ease of use, resource balancing, bandwidth, cost saving & higher security	(Prakash et al., 2022)
4	Retrofitting od legacy machines in the context of IIoTs	To retrofit the existing legacy with sensors to establish IIoTs	Retrofitting of legacy machines	Automation and upgrade	(Machado et al., 2022)
5	Blockchain enabled optimal Hopfield Chaotic Neural Network based secure encryption technique for IIoTs environment	To integrate staged logistic & tent maps	Blockchain enabled shark smell optimization (SSO) & Hopfield Chaotic Neural Network (HCNN)	Security & Optimization	(Khayyat et al., 2022)
6	IIoTs enabled supply-side energy modelling for refined energy management in aluminium extrusions manufacturing	To specifically assign production events calculate energy consumption of the production among others	Supply-side Energy Modelling	Energy (power)	(Peng et al., 2021)
7	Upgrading the manufacturing sector via applications of IIoTs	To provide an overview on IIoTs & technologies underpinned it	Upgrading old system (automation)	Automation, monitoring, reliability	(M. Javaid et al., 2021)
8	Verifiable & auditable authorizations for smart industries & IIoTs	To prevent voluntarily or unintentional damage cause misbehaving by authorized parties	Verifiable and auditable authorizations	security	(Ferretti et al., 2021)
9	A Blockchain-based secure transaction model for distributed energy in IIoTs	To improve real-timeliness security and intelligence	Credit value of Blockchain,	Improve intelligence, real-timeliness,	(Hu & Li, 2021)

Journal of Electronics, Computer Networking and Applied Mathematics
ISSN: 2799-1156
Vol: 02, No. 05, Aug-Sept 2022
http://journal.hmjournals.com/index.php/JECNAM
DOI: https://doi.org/10.55529/jecnam25.1.22

			Distributed energy	security, transparency security, transaction efficiency	
10	Deeping learning-based reliable routing attack detection mechanism for IIoTs	To propose a reliable DL-based routing attack detection scheme using Generative adversarial network-classifier (GEN-C) model	Deep learning routing	Security, improve performance	(Nayak et al., 2021)
11	On deep reinforcement learning (DRL) security for IIoTs	To design DRL-based controller and investigate malicious behavious of adversaries with 2 attacks (function-based attacks and performance-based attacks)	Deep reinforcement learning	Security	(X. Liu et al., 2021)
12	A secure & efficient data sharing scheme based on Blockchain in IIoTs	To ensure secure & efficient data sharing between concerned parties	Data sharing scheme using Blockchain	Data sharing security & efficiency	(Chi et al., 2020)
13	Open source machine learning framework for IIoTs	To examine the open source machine learning and aligned with industrial domain	Machine learning	Optimization, Query control	(Khan & Al-badi, 2020)
14	Intelligent manufacturing production line data monitoring system IIoTs	To ensure improvement in system performance	Wireless sensor & radio frequency identification techniques (WSN & RFID)	System performance	(Chen, 2020)
15	Communication-efficient federated learning for digital twin systems of IIoTs	To improve communication efficiency trade-offs benefits	Federated-learning for digital twin systems	Improve communication, efficiency	(Zhao et al., 2020)

Journal of Electronics, Computer Networking and Applied Mathematics
ISSN: 2799-1156
Vol: 02, No. 05, Aug-Sept 2022
http://journal.hmjournals.com/index.php/JECNAM
DOI: https://doi.org/10.55529/jecnam25.1.22

		between computing power and energy consumption			
16	Deep reinforcement learning-based computation offloading in fog enabled IIoTs	To improve latency, energy consumption	Deep reinforcement learning	Energy efficiency, improve latency	(Ren et al., 2020)
17	Resource allocation in relay-assisted mission-critical IIoTs	To jointly optimize power allocation, position of relay, minimize the decoding errors of the devices	Smart factory, resource allocation mission-critical service	Resource allocations, minimize error in transactions	(Zhao et al., 2021)
18	IIoTs puts new pressure on traditional control systems	To integrate old system with IIoTs	Integration	System upgrade	(Duhaime, 2020)
19	Wireless Power-Data Transmission for Industrial Internet of Things: Simulations and Experiments	This study demonstrates Zenneck usage for interface waves propagating as localized charge oscillations (modes) along the metal profile.	ultrasonic-electromagnetic transducers, and Electrical power transfer using Zenneck	Efficiency, and alignment using	(Thundat, 2020)
20	A checkpoint enabled scalable blockchain architecture for IIoTs	To ensure scalability & security	Scalable blockchain architecture	Security, integrity, scalability	(Javaid et al., 2020)
21	A propagation breakdown management model for IIoTs	To integrate different communication protocols to	Propagation breakdown management	Integration (optimization) or upgrade	(Buetas et al., 2020)
22	Design of 900MHz radio frequency energy harvesting circuit ((900MHz RFEHC) for IIoTs applications	To introduce/design harvestable power supply using rectifying antenna (rectenna)	900MHz RFEHC	Harvestable power, optimization, and performance	(Mouapi, 2020)
23	Network optimization for IIoTs	To design a specific set of reference modes	Network optimization	Optimization of network	(Khalil & Saeed, 2020)

Journal of Electronics, Computer Networking and Applied Mathematics
ISSN: 2799-1156
Vol: 02, No. 05, Aug-Sept 2022
http://journal.hmjournals.com/index.php/JECNAM
DOI: https://doi.org/10.55529/jecnam25.1.22

		that minimize the network errors			
24	A propagation breakdown availability models of IIoTs wired system considering cyber attack	To investigate important reliability indicators of wired IIoTs system	Availability model (wired IIoTs)	Reliability, availability, security	(Kolisnyk et al., 2020)
25	The IIoTs are one of the main drivers of Industry 4.0	To explain what IIoTs is and how it works by companies	Industry 4.0	Prediction capabilities, revealing opportunities & challenges	(Magomadov , 2020)
26	Parallel computing and network analytics for fast Industrial Internet-of-Things (IIoT) machine information processing and condition monitoring	This paper presents a new methodology for large-scale IIoT machine information processing, network modeling, condition monitoring, and fault diagnosis	Parallel computing and network analytics	Dynamic warping algorithm, and stochastic network embedding algorithm	(Kan et al., 2018)
27	Design of IIoTs Gateway with Multi-source Data Processing	To ensure end-to end system security	Gateway	Multi-source Data Processing	(Shimei, 2020)
28	A multi-point collaborative DDoS defense mechanism for IIoT environment	To design and implement a collaborative defense model	Defense mechanism to prevent the system from DDoS	Ensure adequate information security	(Huang et al., 2022)
29	Multi-factory production planning using edge computing and IIoT platforms	To present an approach for generating production plans across multiple factories.	Multi-factory production planning using edge computing	Regulate power consumption, and adopt smart multi-factory production planning	(Dhungana et al., 2021)
30	Blockchain integrated IIOT – Future of IOT	To identify IIoTs' breakthrough	Future of IoT using	Automation	(Senathipathi et al., 2021)

Journal of Electronics, Computer Networking and Applied Mathematics
ISSN: 2799-1156
Vol: 02, No. 05, Aug-Sept 2022
http://journal.hmjournals.com/index.php/JECNAM
DOI: https://doi.org/10.55529/jecnam25.1.22

		capabilities using blockchain technologies	Blockchain technologies		
31	A comprehensive survey on attacks, security issues and blockchain solutions for IoT and IIoT	To highlight some security issues and countermeasures	Blockchain solution	Security	(Sengupta et al., 2019)
32	IIoT and Cyber-Physical Systems Integration in the SEPT Learning Factory Learning Factory L8S Industry	To designing, prototyping, manufacturing, and testing processes of IoT and IIoT	Cyber-physical system integrations	Support operation using cyber-physical components	(Singh et al., 2019)

Table 4. Innovative Trends Application and Application Purposes

IIoTs - Innovative Trend	Application Purposes	Sources
Deep/Machine Learning Related Trends	Security Managing Energy Consumptions Performance and Optimization	(Zhao, Li, Liu, Fan, & Lin, 2020)
Federated Learning for Digital Twin System		(Ren et al., 2020; Liu et al., 2021)
Deep Reinforcement Learning Based on Fog Computing		(Khan & Al-badi, 2020; Singh et al., 2019)
Machine Learning		(Nayak et al., 2021)
Deep Learning - Based Reliable Routing for Attack Detection		
Blockchain Related Trends	Security Managing Energy Consumptions Efficiency, Reliability and Availability	(Javaid et al., 2020)
Blockchain Architecture for a Checkpoint Enabled		(Chi et al., 2020)
Blockchain for a Secured & Efficient Data Sharing Scheme		(Hu & Li, 2021)
Blockchain - Based Secure Trasaction Model for Distributed Energy		(Khayyat et al., 2022)
Blockchain Enabled Optimal Hop Field Chaotic Neural Networkfor encryption Technique		
Security Related Trends	Security Integration and Upgrade Efficiency, Reliability and Availability	(Ferretti et al., 2021)
Varifiable & Auditable Authentications for Smart Industries		(Shuai et al., 2020)
Robin Cryptosystem for Secured Authentication Scheme		(Kebande, 2022)
Forensics		

Journal of Electronics, Computer Networking and Applied Mathematics
ISSN: 2799-1156
Vol: 02, No. 05, Aug-Sept 2022
http://journal.hmjournals.com/index.php/JECNAM
DOI: https://doi.org/10.55529/jecnam25.1.22

Gateway with Multi-Source Data Processing		(Shimei, 2020)
Propagation Breakdown Availability Models for Preventing Cyber Attack		(Kolisnyk et al., 2020)
Upgrade for Secured Smart Manufacturing		(Javaid et al., 2021; Shimei, 2020)
Energy Related Trends	Managing Energy Consumptions Efficiency, Reliability and Availability	
IIoTs Enabled supply-sided Energy Management for Aluminium Extrusions		(Peng et al., 2021)
Smart Energy System		(Zhang et al., 2018)
Wireless Power-data Transmision		(Oruganti, Khosla & Thundat 2020
Smart Factory Ralated	Security Managing Energy Consumptions Integration and Upgade Latency and Throughput Performance and Optimization Efficiency, Reliability and Availability	
Propagation Breakdown Availability Models for Preventing Cyber Attack		(Buetas et al., 2020)
Automation of Traditional Control Systems		(Duhaime, 2020; Khalil & Saeed, 2020)
Resource Allocation in Relay-Assisted Mission - Critical		(Ning, Wang, Chen & Liu, 2020)
Cloud and Edge-based ERP System for Smart Factory		(Prakash et al., 2022)
Retrofitting of Legacy Machines		(Kolla, et al. 2022)
Industry 4.0 for IIoTs		(Magomadov 2020) (Duhaime, 2020)