International Journal of New Media Studies (IJNMS), ISSN: 2394-4331
Volume 7 Issue 2, July-December, 2020, Impact Factor: 6.789

A Review of Industrial Internet of Things

Sunil Jhangid

IECIIT Institute, India

Abstract

AI, IIoT, Sensors, ML, VR, AR sort of technologies enables industrial machines, management systems and products to connect to the internet, enabling manufacturers to collect and process data about them for improved efficiency, reliability, flexibility and safety. Additionally, it provides opportunities for automation, predictive maintenance and process optimization. Industry 4.0 and IIoT cyber security can help businesses protect their equipment, data, and systems. By understanding the threats and risks associated with IIoT and Industry 4. 0 systems, organizations can identify, assess and mitigate security risks before they become a major problem. With the help of AI platform, businesses can use intelligent analytics to detect threats and gain real-time insights into their network and systems, enabling them to act quickly when an attack is detected. Organizations are also able to detect any suspicious behaviour in various components of their system and apply the right security measures to protect their data.

Keywords: IIOT, Industry 4.0, Cyber Security, 5G, Cyber Physical Systems

Introduction

Industry 4. 0 sets the foundations for the evolution of traditional factories into smarter manufacturing plants. This concept emphasizes the use of data and analytics to enable the automation, decentralization and flexibility of industrial manufacturing processes.

It promotes the use of sensors, machine learning, AI, and virtual reality/augmented reality (AR/VR) to gather real-time data, automate processes, optimize quality and improve the safety of products and personnel. Additionally, it enables the customization of product offerings, which allows manufacturers to better meet customer demands. Industry 4. 0 allows for the integration of IT systems, resulting in higher efficiency, better decision making and improved data processing speeds.

Industry 4. 0 and Industrial Internet of Things (IIoT) share similar foundations and objectives. Both paradigms are centered around the use of advanced technologies to monitor, control and optimize the performance of industrial systems, processes, and products in real time. In particular, the use of sensors, ML, AI, and AR/VR to collect and analyze data is a common foundation across both paradigms.

The main difference between the two is that IIoT focuses on interconnecting physical items, such as machines and other types of hardware, to the internet. Meanwhile, Industry 4. 0 is more focused on using technology and data to optimize manufacturing processes and enable customization of products. Therefore, while the two paradigms may share some common foundations, their end goals are slightly different.

Augmented/Mixed/Virtual Reality (AR/MR/VR) are technologies often used in the context of Industry 4. 0 that allow for the digitization and visualization of geographical and industrial tasks. This allows for more efficient and accurate analysis of various industrial settings, enabling companies to streamline processes and better access and analyze data for optimization. AR/MR/VR are also capable of overlaying visuals and data into a real-world landscape, making it easier for human operators to understand their environment and the output requirements for specific processes. As such, AR/MR/VR are powerful tools for allowing people to interact with the physical world in ways that have never been possible before, creating a more efficient and immersive working environment.

Integration systems are technologies that are used to enable the networks and devices of a system to communicate with one another and share information. This creates more efficient and effective communication between the different parts of the system and helps optimize the performance of the system. Integration systems can also be used to connect systems which may be running different operating systems, allowing for easier sharing of data and making the systems more flexible. By utilizing integration systems, companies can more easily deploy and monitor their networks in an efficient and cost-effective manner and improve the performance of their Industry 4. 0 operations.

Simulation software is used to model and analyze industrial processes, evaluate potential design solutions or strategies, and define project objectives.
AI predictive technologies are used to ensure the accuracy of the predictions made by the system when experience or data is insufficient.

Cloud processing is a technology that allows businesses to store, manage and access data and applications remotely. This offers flexibility, scalability and cost savings [1].

5G connectivity is the fifth-generation mobile network, which has higher bandwidth, low latency and is able to serve a greater number of devices simultaneously [2]. This enables faster data transmission between devices, creating an environment suitable for Industry 4. 0 [3].

Additive Manufacturing, also known as 3D printing, is a key technology of Industry 4. 0. The technology enables rapid fabrication of three-dimensional parts from computer-aided design (CAD) data using specialized printing machines. It enables operation with limited resources, quicker product development and production, and lower production costs. Additive Manufacturing is also beneficial since it allows for components to be produced with complex shapes and various materials in order to build up a finished product layer-by-layer. This technology is very useful for printing parts in the automotive, aerospace, and medical industries. Additionally, the technology can be used to create components quickly by reducing inventory and transportation costs, as well as decreasing the lead time for standing out in the market [4].

The goal of industrial CPS is to improve the efficiency, accuracy, and safety of industrial processes. It involves the exchange of data and information among machines, sensors, data analysts, and personnel as well as the conversion of physical parameters (e. g. temperatures and pressures) into digital representations (e. g. digital twins). Industrial Cyber-Physical Systems enable real-time monitoring and control of various processes and activities, resulting in faster response times, improved operational safety, increased operational efficiency, and enhanced performance [5].

Big Data is one of the most important technologies involved in the implementation of Industry 4. 0. Big Data technology refers to the collection and analysis of extremely large amounts of digital data, such as from connected devices, IoT sensors, social media platforms, and other sources [6]. By utilizing Big Data, companies are able to gain valuable insight into customer behavior, process patterns, and trends. This data can then be used to improve products and services, enhance supply chain management, and automate many industrial processes. Additionally, Big Data technology can be used to optimize usage of resources and make predictive analytics viable [7].

An automated guided vehicle (AGV) is a type of robot designed to be able to move materials around a manufacturing or warehouse environment without requiring any direct human supervision [8]. An AGV is typically outfitted with sensors that enable it to move autonomously around the environment and interact with other robots and machines. AGVs also reduce risk for human workers by decreasing the need for direct manual labor in hazardous or difficult working environments, like overhead crane or machine loading/unloading. Additionally, using AGVs to manage inventory can provide valuable insights into production processes and further automate the supply chain [9].

Recent Technologies like block chain Blockchain is a distributed ledger technology that delivers a tamper-proof system of recordkeeping, wherein data is stored across a distributed network of computers. It is used to quickly and securely transfer digital information, including the execution and settlement of various financial contracts [10]. In industrial systems, blockchain-based decentralized autonomous systems can be used to record transactions, manage and enable access to resources, and enable traceability of physical and/or digital assets. For example, blockchain can enable proactive supply chain management, making it possible for all stakeholders of the chain, both up streams and down streams, to access the same, authentic data sourced from approved sources [11]. Additionally, blockchain can be used to enable the automation and optimization of industrial processes, acquire right-in-time access to machinery and equipment, manage digital data storage, and create innovative payment methods [12].

Many IIoT devices are vulnerable to cyber-attacks due to weak security implementations or to the lack of a proper security configuration. Many IIoT networks contain legacy systems and software that often have inadequate security controls. For example, embedded devices and unlatched systems may be open to attack because their manufacturers are oblivious to the importance of such measures [13]. Moreover, the rise of IoT devices has made the challenge even more daunting, as the data that these devices collect or transmit can become a new target for malicious actors. The use of blockchain technology can provide a secure and trusted platform for IIoT networks by providing a secure and immutable ledger for recording and verifying transactions. Blockchain can also help protect connected devices by providing a trust layer that makes it difficult for malicious actors to access data or control the network. Finally, blockchain can also be used to automate the various functions associated with data gathering, analysis, and storage, enabling IoT devices in a secure, decentralized manner [14].

Challenges

When implementing the Internet of Things (IoT), Scalability refers to how easily the system can be expanded to accommodate increased data. This means that it should be capable of adding new data sources or sensors without requiring a major overhaul of the system. Security is crucial to ensure the system is protected from malicious actors and hackers. Availability refers to the system's ability to respond and meet the needs of users quickly and consistently [15]. This means that the system should have 24/7 access with minimal downtime in order to provide quick and efficient service.

Legacy systems are still widely used by manufacturing companies because they are reliable, economical, and provide a stable platform for their operations. However, these systems may not have adequate security protocols in place to guard against outside threats or network intrusions. As such, it is important for manufacturing companies to regularly assess their security infrastructure and update it accordingly in order to ensure that they stay ahead of new vulnerabilities that may arise [16]. Additionally, they should consider upgrading their system to a more secure, modern platform in order to ensure that their data and processes remain secure.

The rise of smart devices has spurred a dramatic increase in the number of potential security vulnerabilities. Smart devices utilize internet connectivity and increasing levels of automation, making them easy targets for malicious actors. As the number of connected devices continues to grow, so does the potential for unauthorized access to a company's data, networks and systems. Additionally, the use of smart devices introduces the risk of data breaches as sensitive information can be collected or accessed through them. Companies must be aware of this and take steps to safeguard their data by implementing security procedures and best practices for their connected devices [17].

Cyber security is essential because security threats are constantly evolving in sophistication and scope. Cyber criminals are continually adapting their tactics and technologies, and organizations need to be prepared to protect their data and networks. As new threats emerge, it’s not enough just to be aware of them - companies also need proactive strategies and solutions to prevent, detect and respond to attacks. Companies need to ensure that their security measures are constantly updated in order to stay ahead of potential threats and remain secure. Cyber security is a game of cat and mouse, and organizations need to be continually assessing and adapting to protect their sensitive data and networks [18].

A security operations center, or SOC, is designed to help organizations detect and respond to threats before, during and after they occur. The SOC is responsible for consolidating security operations and activities into one central location. This allows organizations to quickly respond to events, detect anomalies and potential threats, identify potentials vulnerabilities or weaknesses in infrastructure, systems, and applications, and track and analyze data to help provide insight into any potential threats [19]. Additionally, the SOC can help coordinate and manage the incident response process should an incident occur. The SOC also typically offers distributed analytics, reporting, and threat intelligence services to help organizations better secure their networks and detect any suspicious activity. By providing these services, the SOC is able to help protect organizations from a wide range of malicious activities [20-21].

As industries shift to new technologies, they must be prepared to face risks which they may not have had to deal with before. New technologies come with new and unknown vulnerabilities in infrastructure, systems, and applications. Additionally, they may lack the experience and resources to be able to properly identify and respond to threats before, during, and after they occur [22]. The security operations center can help provide industry with the expertise and resources required to detect and mitigate these risks, preventing damaging incidents before they occur. By providing centralized monitoring, analytics, reporting, and threat intelligence services, the SOC can help protect a wide variety of industries from malicious activities [23].

Conclusion

As more and more devices are connected, industries must be prepared to face any potential security risks and the security operations centre provides an essential service for industry in helping to reduce these risks by providing centralized intelligence and monitoring.

The security operations centre provides a centralized platform for the monitoring and handling of these potential threats. It does this by providing an analytical and operational intelligence gathering base for anything related to the security of the IoT devices. This can include the monitoring of threats, the identification and neutralization of vulnerabilities, the tracking of malicious actors, the protection of data, and the enforcement of security measures.

Security operations centres can also act as a critical node of communication between IT departments and other members of the organization. They can ensure proper coordination and oversight of IT procedures and protocols, allow for better collaboration between teams, provide real-time access to threats, and provide detailed reports on the security posture of networks, systems, and applications.

Lastly, using a security operations centre can create an effective line of defence for the security of internet of things infrastructure. By proactively monitoring for any suspicious activity or potential threats, the security operations centre can help organizations prevent a damaging breach or attack. By deploying the most up-to-date tools and processes, the security operations centre is an essential component in the effort to protect industry from malicious actors.

References

[1]. Rathore, R.S., Sangwan, S., Adhikari, K. and Kharel, R., 2020. Modified echo state network enabled dynamic duty cycle for optimal opportunistic routing in EH-WSNs. *Electronics*, *9*(1), p.98.

[2]. Rathore, R.S., Sangwan, S., Mazumdar, S., Kaiwartya, O., Adhikari, K., Kharel, R. and Song, H., 2020. W-GUN: Whale optimization for energy and delay-centric green underwater networks. *Sensors*, *20*(5), p.1377.

[3]. Rathore, R.S., Sangwan, S., Prakash, S., Adhikari, K., Kharel, R. and Cao, Y., 2020. Hybrid WGWO: whale grey wolf optimization-based novel energy-efficient clustering for EH-WSNs. *EURASIP*

Journal on Wireless Communications and Networking, *2020*(1), pp.1-28.

[4]. Singh, U.P. and Rathore, R.S., 2013. Distributed Hierarchical Group Key Management using Elliptic Curve and Hash Function. *International Journal of Computer Applications*, *61*(19).

[5]. Singh, U.P. and Rathore, R.S., 2012. An efficient distributed group key management using hierarchical approach with ECDH and symmetric algorithm. *J. Comput. Eng. Intel. Syst*, *3*(7), pp.32-41.

[6]. Bali, V., Rathore, R.S. and Sirohi, A., 2010. Routing Protocol for MANETs: A Survey. *IUP Journal of Computer Sciences*, *4*(3).

[7]. Bali, V. and Rathore, R.S., 2010. A NEW HIERARCHICAL TRANSACTION MODEL FOR MOBILE ADHOC NETWORK ENVIRONMENT. *International Journal on Computer Science and Engineering*, *2*(3).

[8]. Singhal, S. and Rathore, R.S., 2015. Detailed Review of Image Based Steganographic Techniques. *IJCST*, *6*, pp.93-95.

[9]. Kumar, V. and Rathore, R.S., 2018, October. Security issues with virtualization in cloud computing. In *2018 International Conference on Advances in Computing, Communication Control and Networking (ICACCCN)* (pp. 487-491). IEEE.

[10]. Sharma, P. and Rathore, R.S., 2015. Three Level Cloud Computing Security Model. *International Journal of Computer Applications*, *119*(2).

[11]. Bali, V., Rathore, R.S., Sirohi, A. and Verma, P., 2009, August. Information Technology Architectures for Grid Computing and Applications. In *2009 Fourth International Multi-Conference on Computing in the Global Information Technology* (pp. 52-56). IEEE.

[12]. Bali, V., Rathore, R.S. and Sirohi, A., 2010. Performance analysis of priority scheme in ATM network. *International Journal of Computer Applications*, *1*(13), pp.26-31.

[13]. Bali, V., Rathore, R.S., Sirohi, A. and Verma, P., 2009, December. A Framework to Provide a Bidirectional Abstraction of the Asymmetric Network to Routing Protocols. In *2009 Second International Conference on Emerging Trends in Engineering & Technology* (pp. 1143-1150). IEEE.

[14]. Dixit, R., Gupta, S., Rathore, R.S. and Gupta, S., 2015. A novel approach to priority based focused crawler. *International Journal of Computer Applications*, *116*(19).

[15]. Tomar, R. and Rathore, R.S., 2016. Privacy Preserving in TPA using Secured Encryption Technique for Secure Cloud. *International Journal of Computer Applications*, *138*(8).

[16]. Tomar, R. and Rathore, R.S., 2016. A Survey on Privacy Preserving in TPA Using Secured Encryption Technique for Secure Cloud. *International Advanced Research Journal in Science, Engineering and Technology*, *3*(4), pp.83-86.

[17]. Bali, V., Rathore, R.S., Sirohi, A. and Verma, P., 2009. Clustering Technique Approach to Detect the Special Patterns for Medical Video Mining. *Advances in Data Management*, p.140.

[18]. Bali, V., Rathore, R.S., Sirohi, A. and Verma, P., 2009. Architectural Options and Challenges for Broadband Satellite ATM networks. *Recent Developments in Computing and Its Applications*, p.155.

[19]. Srivastava, S.N., Kshatriya, S. and Rathore, R.S., 2017. Search Engine Optimization in E-Commerce Sites. *International Research Journal of Engineering and Technology (IRJET)*, *4*(5), pp.153-155.

[20]. Rattan, V., Sinha, E.M., Bali, V. and Rathore, R.S., 2010. E-Commerce Security using PKI approach. *International Journal on Computer Science and Engineering*, *2*(5), pp.1439-1444.

[21]. Bali, V., Rathore, R.S. and Sirohi, A., 2010. Adaptive Analysis of Throughput in Mobile Admhoc Network (IEEEm802. 11). *International Journal of Computer Science & Communication*, *1*(1), pp.25-28.

[22]. Kumar, V. and Singh Rathore, R., 2016. A Review on Natural Language Processing. *International Journal Of Engineering Development And Research*.

[23]. Bhatnagar, D. and Rathore, R.S.,2015. CLOUD COMPUTING: SECURITY ISSUES AND SECURITY MEASURES. *International Journal of Advance Research in Science And Engineering, 4*(01), pp.683-690.