Review of Internet of Things System on Atmospheric Corrosion Monitoring

Muhammad Awwaludin[1,a], Sri Hastuty[2,b], Akhmad Sarif[1,c], Makmuri[1,d], Mustasyar Perkasa[1,e]. Mochamad Hapis Paturahman[3,f], Andre Rifat Ariq Girasto[3,g], Nauval Bagus Maulana[3,h], Fatwa Khoirrun Nadhor[2,i]

[1] Research Center for Structural Strength Technology, National Research and Innovation Agency, Tangsel 15314, Indonesia.
[2] Department of Mechanical Engineering, Faculty of Industrial Engineering, Universitas Pertamina, Jakarta 12220, Indonesia.
[3] Department of Mechanical Engineering, Faculty of Engineering, Universitas Pamulang, Tangsel 15417, Indonesia.

[a]muha112@brin.go.id
[b]sri.hastuty@universitaspertamina.ac.id
[c]akhm011@brin.go.id
[d]makm001@brin.go.id
[e]must011@brin.go.id
[f]mochamadhapis@gmail.com
[g]andre.rifat2604@gmail.com
[h]nauvalbagus17@gmail.com
[i]fatwanadhor9a@gmail.com

Corresponding Author: muha112@brin.go.id, sri.hastuty@universitaspertamina.ac.id

***Abstract*— The Internet of Things (IoT) is used widely in daily life, including smart homes, industrial automation, and environmental monitoring. IoT devices are also utilized in industrial settings for real-time equipment performance and predictive maintenance monitoring. Utilizing IoT to make atmospheric corrosion monitoring easier. The IoT on atmospheric corrosion monitoring is essential because it can provide real-time data on corrosion rates, enabling proactive maintenance and preventing costly damage to infrastructure caused by corrosion. Integrating IoT and corrosion monitoring remains relatively uncommon, with numerous parameters necessitating consideration by the environment in which it would be placed for effective implementation, such as sensor placement, data accuracy, and connectivity reliability. Here, we demonstrate a comparative analysis between cloud and field protocols based on existing studies, specifically focusing on utilizing Arduino ATmega 328 and Node MCU8266 microcontrollers for atmospheric corrosion monitoring through IoT integration. This study offers a more comprehensive understanding of the suitability and effectiveness of Arduino ATmega 328 and Node MCU8266 microcontrollers for corrosion monitoring. This study aims to be a foundational step towards establishing integrated Internet of Things systems for corrosion monitoring in industrial settings, paving the way for proactive maintenance strategies and enhanced infrastructure reliability.**

***Keywords*— IoT, Atmospheric Corrosion, Monitoring**

I. Introduction

The foundation of the Internet of Things (IoT) traces back to the notion of "ubiquitous computing" or distributed computing, initially proposed by Mark Weiser in the early 1990s. This concept states that computers can be invisibly incorporated into everyday life, allowing for more natural interactions between humans and technology. Furthermore, the term "Internet of Things" was first used by Kevin Ashton in 1999 while working at the Auto-ID Center at MIT. Ashton stated in a 1999 article in the RFID Journal magazine: "Imagine if we had a computer that comprehensively understood its environment and our informational needs; it could facilitate deeper insights, enhance connectivity, and foster greater reliance on our surroundings."

Internet of Things (IoT) is a concept that aims to expand the internet which is continuously connected [1], [2]. The term "Internet of Things" (IoT) was coined by Kevin Ashton at a presentation before the Gaming Trustees & Board in 1999. He was one of the founders of the Automatic Recognition Lab at the Massachusetts Institute of Technology. He pioneered RFID (used in barcode detectors) technology in the field of supply chain management. He also founded Zensi, a company that produces energy sensing and monitoring technology. The Internet of Things is a growing topic in the fields of technical, social, economic, consumer products, durable goods, cars and trucks, industrial components and facilities, sensors, and other everyday objects that are connected to the internet and have advanced data analysis capabilities that promises and changes the way we live and work.

The Internet of Things (IoT) applications encompass various functionalities such as data sharing, remote control, and sensor integration across objects. For instance, electronic devices and machinery are interconnected to local and global networks through embedded sensors, facilitating active monitoring and control [3], [4]. As networking technologies advance and the demand for data exchange grows, these implementations enhance processes or systems across domains like offices, commerce, residences, and personal usage. Data exchange primarily occurs through local network connectivity, utilizing LAN or WiFi configurations interconnecting seamlessly [5]–[7]. The accumulation of IoT has permeated numerous sectors, including energy and security, with the integration of cloud computing playing a pivotal role in streamlining data processing [8]. This convergence not only expands the scope of big data but also augments capabilities in data analysis [9], [10].

Various instances of IoT implementation on devices include pioneering efforts dating back to 1990, when John Ramkey and Simon Hackett collaborated to devise a toaster connected to the internet via TCP/IP network, controlled through SNMP Management Information Base (MIB), albeit requiring human intervention for bread insertion. Subsequent advancements in 1999 involved augmenting this device with an interop or small robot crane, enabling internet-controlled bread handling. Simultaneously, Kevin Ashton, Executive Director of MIT's Auto ID Center, catalyzed the inception of the Internet of Things, alongside the invention of global RFID-based systems, marking a significant stride in IoT commercialization. LG, a multinational from South Korea, announced plans in 2000 for a smart refrigerator capable of autonomously assessing food replenishment needs. The proliferation of RFID gained momentum in 2003 within the US military industry through the Savi Program, subsequently extending to widespread retail adoption. By 2005, mainstream media outlets such as The Guardian and Boston Globe featured numerous articles on IoT. The IPSO Alliance emerged in 2008 to advocate for IP integration in Smart Object networks, coinciding with the FCC's approval of white space spectrum usage. The release of IPv6 in 2011 spurred substantial growth in the IoT domain, buoyed by initiatives from industry giants like IBM, Cisco, and Ericsson, underscoring the symbiotic relationship between computers and humans in the IoT landscape.

In today's digital age and with the rise of Industry 4.0, the Internet of Things (IoT) has become a key player across different fields, reshaping how we oversee and handle intricate systems. A standout application of this technology is its ability to monitor things in real time, especially in industries and security sectors. Here, IoT plays a crucial role in enhancing monitoring practices' accuracy, efficiency, and accountability.

Using IoT for real-time monitoring requires various approaches that rely on sensor tech, wireless connections, and intelligent data analysis. IoT links up physical gadgets through the internet, enabling data sharing and automated control, which evolves alongside tech advancements, communication, and intelligent concepts.

II. Methodology

In this study, an exhaustive review of the literature pertaining to the implementation of IoT for monitoring purposes was conducted. However, a need for more literature specifically addressing corrosion monitoring through IoT was identified. Consequently, the search was expanded through consultations with domain experts. These consultations involved discussions with researchers affiliated with the National Research and Innovation Agency and Pertamina University.

III. IoT Technologies in Corrosion Monitoring

This paper describes the application of corrosion monitoring with a variety of different specimens, and the focus of this paper is analyzing field protocols and cloud protocol from literature. Where the most popular field protocols used include LoRaWAN, Bluetooth, Zigbee, Wi-Fi, Near Field Communication (NFC), Sigfox, Narrowband IoT, Hypertext Preprocessor (PHP), 3G/4G/5G. The most popular cloud protocols are Message Queue Telemetry Transport (MQTT), Hypetext Transfer Protocol (HTTP), User Datagram Protocol (UDP), Table 1 shows the comparison.

TABLE I
TYPES OF FIELD PROTOCOLS AND CLOUD PROTOCOLS USED

REFERENCE	DEVICE	ADVANTAGES	DISADVANTAGES	PRICE (IDR)
[11]	NodeMCU 8266	1. Affordable Prices 2. Active Community 3. Flexibility 4. Built-in WiFi 5. Sufficient Memory	1. GPIO Limitations 2. Limited Performance 3. Lack Of Security 4. Limited Official Support 5. Power Consumption	Rp 30.000 – 300.000
[12]	Raspberry Pi	1. Affordable 2. Small 3. Low Power Consumption 4. Suitable For Small Tasks and Limited Pupose 5. Easy To Use	1. Limited Functionality 2. Slow 3. Not Ideal For Multitasking 4. Poor For Larger Tasks	Rp 500.000 – 1.500.000
[13]	Bluetooth HC-05	1. Affordable Prices 2. Easy To Use 3. Wide Compatibility 4. Low Power Consumption	1. Limite Data Transfer Speed 2. Feature Limitations 3. Does Not Support Bluetooth Low Energy (BLE)	Rp 37.000 – 130.000

		5. Decent Range	4. Requires Additional Programming For Configuration 5. Limitations in Compatibility	
[14]	MQTT	1. Low Bandwidth Overhead 2. Limited Resources 3. Connection Reliability 4. Easy To Learn an Use	1. Security 2. Scalability 3. High Latency 4. Broker Dependency	Undefined
[15]	Arduino uno (ATmega328)	1. Easy To Use 2. Sensor Support 3. Wide Community 4. Flexibility 5. Affordable Prices	1. Perfomance Limitations 2. I/O Limitations 3. Communication Limitations 4. Conncectivity Limitations 5. Dependence On External Resources	Rp 120.000 – 300.000
[16]	Wifi module (ESP8266)	1. High Connectivity Capability 2. Small and Light Module Size 3. Low Power Consumption 4. Flexibility In Programming Languages 5. Programmable With Arduino IDE 6. Support For Python Programming Language 7. High Modularity 8. Affordable Prices 9. Strong Community Support 10. Capabilities Available In The Market	1. High Power Consumption 2. GPIO Pin Limitations 3. Limited Capabilities 4. Memory Limitations 5. Dependence On WiFi Network	Undefined
[16]	ThinkSpeak	1. Easy To Use 2. Data Visualization 3. Integration With Various Platforms 4. Monitoring and Notifications 5. Flexibility	1. Dependence On Internet Connection 2. Data Privacy and Security 3. Limitations On The Amount Data 4. Limitations On Free Features 5. Limitations In Data Processing	Undefined
[16], [17]	Arduino IDE	1. Easy To Use 2. Free and Open Source 3. Wide Support 4. Compability With Multiple Platforms 5. Integration With Arduino Board	1. Feature Limitations 2. Limitations In Professional Development 3. Regulatory Limitations 4. Performance and Speed 5. Dependence On The Ecosystem	Undefined
[18]	Module NB-IoT	1. Because It Uses Cellular Wireless Network, It Offers Better Scalability, Quality Of Service, and Security Compared To Unlicensed LPWA Networks Such As Lora/Sigfox 2. It Offers Long Battery Life Due To Low Power Consumption Or Current Consumption 3. Provides Wider Coverage Compared To GSM/GPRS System 4. Various Network Operators In Europe and Asia Support It 5. It Transmit Data At Low Bit Rates Over Long Distance. The Range Is Better Than GSM and LTE 6. NB-IoT ModulesAre Expected To Be Available At Affodable Prices 7. They Offer Better Fabric Penetration and Better Data Rates Compared To Unlicensed Bandbased Standards (e.g. LoRaWAN and Sigfox).	Undefined	Undefined

		8. It Coexists With Other Legacy Cellular System Such As GSM/GPRS/LTE. NB-IoT Enabled Device Can Be Deployed/Scheduled In Any Legacy LTE Network. This Helps Them Share Capacity As Well As Other Cell Resources With Other Wirelessly Connected Device		

IV. CASE STUDIES AND FIELD APPLICATION

Based on study conducted by S. Samsugi, et al (2020), the study was designing and concepting for emergency button in motorcycly to prevent hijacking [7]. This study utilizing 2 devices, namely, Arduino ATmega 328 and Node MCU8266. The Arduino ATmega 328 itself has several advantages, including being easy to use because it has a user-friendly interface and is easy to program using the Arduino IDE. In terms of sensors, Arduino Uno supports various sensors that can be used to monitor various parameters such as temperature, humidity, pressure, and others. Furthermore, in terms of flexibility, Arduino Uno can be easily connected with various additional devices (shields) and communication modules such as WiFi or Ethernet, which allows users to send data in real-time to servers or other platforms. Apart from the advantages of the Arduino ATmega328, this type has several disadvantages including limitations in performance, the ATmega 328 has limitations in terms of speed and memory capacity, which can be an obstacle for applications that require intensive data processing in real-time. Furthermore, I/O limitations, the limited number of I/O pins on the Arduino Uno can limit the number of sensors or devices that can be connected directly, requiring additional thought in monitoring system design. Then there are communication limitations, Arduino Uno has limitations in speed and type of communication. In terms of connectivity, this type has connectivity limitations, sometimes, the Wi-Fi or Ethernet connection available for the Arduino Uno can be limited in terms of range or availability. And the final drawback is dependence on external resources, Arduino Uno requires an external power source, such as a power supply, which must be considered carefully, especially for real-time monitoring applications that require continuous operation. Meanwhile, the Node MCU8266 has general advantages, namely, in terms of price, the Node MCU8266 has a relatively cheaper price compared to several other IoT development platforms. In terms of use, it is very easy to use, because information about use is easy to get. The MCU8266 node is very easily integrated with WiFi which allows your device to connect to a WiFi network and communicate with other devices via the internet. And the Node MCU8266 has enough memory to store code and data for relatively simple IoT applications. The MCU node also has several disadvantages if it cannot be used on a large scale which uses many GPIO (general purpose input/output) pins due to the limited number of pins. When compared with the ESP32 for processor performance, the ESP8266 has limited performance. In terms of security, although the ESP8266 supports WiFi security protocols such as WPA2, implementing strict security is often the user's responsibility. This can be a problem in projects that require a high level of security. And the power consumption of the Node MCU8266 is still higher than some alternatives, especially in sleep or power saving mode.

In a study by Zhuolin, Li, et al. (2019), atmospheric corrosion monitoring was investigated by employing an IoT-based ACM system. This system integrated an electrical resistance sensor and relative humidity and temperature sensors [19]. The electrical resistance sensor was based on ASTM B829-09 standards. Its functionality involved voltage comparison before and after corrosion (VA/VB), enabling computation of corrosion product thickness based on voltage ratio. The sensor exhibited superior measurement accuracy, striving for uniform corrosion. The IoT ACM was constructed using industrial-grade components to withstand harsh environments. At its core lies a pivotal hardware device encompassing core control, data acquisition, transmission, and power supply functions. This hardware device ensures real-time, high-precision, and efficient operations. The electrical resistance sensor acquires corrosion data via lead wires connected to the hardware device, which are logged hourly. The study findings indicate that the acquired corrosion data is effective and normal, suitable for real-time monitoring and remote measurement.

V. CHALLENGES AND LIMITATIONS

The Internet of Things (IoT) is a line for inter-device communication, leveraging the Internet as its primary communication medium. However, the proliferation of internet-connected devices renders them susceptible to various cyber threats, including hacking, data breaches, and malware incursions, constituting a significant challenge in IoT system utilization. Consequently, ensuring robust data security and privacy measures becomes imperative. Data security and privacy protocol advancements are indispensable in addressing this challenge effectively. As a result, initiatives to bolster data security within IoT systems, such as integrating blockchain technology, are gaining traction as viable solutions over time.

The harsh environmental conditions associated with corrosion pose significant challenges for the application of IoT technology. These conditions have the potential to adversely affect IoT devices, thereby influencing the accuracy and reliability of the acquired data. Consequently, careful consideration must be given to the design of IoT devices to mitigate these challenges. Utilizing robust materials with excellent corrosion resistance and high-strength properties can bolster the durability and resilience of IoT devices, enhancing their performance in corrosive environments.

VI. Conclusion

Addressing the evolving landscape of the Internet of Things (IoT) is crucial to data security and privacy. As IoT permeates various aspects of daily life, the complexities confronting information technology infrastructure grow increasingly convoluted. Hence, safeguarding data and privacy is essential for ensuring the longevity and effectiveness of implementing secure and dependable IoT systems. Deploying robust security solutions is a fundamental prerequisite for establishing resilient IoT ecosystems, with blockchain technology offering a compelling avenue in this endeavor. Through blockchain integration, data transmission among IoT devices can be fortified, curbing the vulnerabilities associated with data manipulation, cyber intrusions, and privacy breaches. This trajectory sets a sturdy foundation for nurturing a secure and trustworthy IoT environment, paving the way for its sustainable evolution and widespread adoption.

In Corrosion Monitoring using IoT, careful consideration of various parameters is imperative, particularly regarding the application environment. Given the dynamic nature of IoT tools, the design of IoT devices must prioritize resilience to withstand harsh environmental conditions. Factors such as temperature, relative humidity, pressure, and exposure to corrosive chemical compounds necessitate thorough consideration in designing and deploying IoT devices for effective corrosion monitoring.

V. References

[1] M. I. Hafidhin, A. Saputra, Y. Rahmanto, and S. Samsugi, "(in Indonesia) Alat Penjemuran Ikan Asin Berbasis Mikrokontroler Arduino UNO," *J. Tek. dan Sist. Komput.*, vol. 1, no. 2, pp. 59–66, Dec. 2020, doi: 10.33365/jtikom.v1i2.210.

[2] A. Wantoro, "(in Indonesia) Sistem Monitoring Perawatan dan Perbaikan Fasilitas Gardu PT PLN Area Kota Metro," *J. Tekno Kompak*, vol. 15, no. 1, p. 116, Feb. 2021, doi: 10.33365/jtk.v15i1.903.

[3] A. N. Kholidi, A. Trisanto, and E. Nasrullah, "(in Indonesia) Rancang Bangun Alat Pemberi Pakan dan Pengatur Suhu Otomatis untuk Ayam Pedaging Berbasis Programmable Logic Controller pada Kandang Tertutup," *J. Rekayasa dan Teknol. Elektro*, vol. 9, no. 2, pp. 87–95, 2015.

[4] S. Hani and G. Santoso, "(in Indonesia) Pembasmi Serangga Menggunakan Energi Solar Cell Untuk Meningkatkan Produktifitas Tanaman Padi," *J. Simp. Nas. RAPI XVII*, vol. 8, no. 4, pp. 31–36, 2018.

[5] A. Mulyanto and Rikendry, "(in Indonesia) Sistem kontrol pergerakan robot beroda pemadam api," *Semin. Nas. Apl. Teknol. Inf. 2007 (SNATI 2007)*, vol. 2007, no. Snati, pp. 1–4, 2007.

[6] T. Widodo, B. Irawan, A. T. Prastowo, and A. Surahman, "(in Indonesia) Sistem Sirkulasi Air Pada Teknik Budidaya Bioflok Menggunakan Mikrokontroler Arduino UNO R3," *J. Tek. dan Sist. Komput.*, vol. 1, no. 2, pp. 34–39, 2020, doi: 10.33365/jtikom.v1i2.12.

[7] S. Samsugi and W. Wajiran, "(in Indonesia) IoT: EMERGENCY BUTTON SEBAGAI PENGAMAN UNTUK MENGHINDARI PERAMPASAN SEPEDA MOTOR," *J. Teknoinfo*, vol. 14, no. 2, p. 99, 2020, doi: 10.33365/jti.v14i2.653.

[8] S. Samsugi, Ardiansyah, and A. Suwantoro, "(in Indonesia) Pemanfaatan Peltier dan Heater Sebagai Alat Pengontrol Suhu Air Pada Bak PenetasanTelur Ikan Gurame," *Conf. Inf. Technol. Inf. Syst. Electr. Eng.*, pp. 295–299, 2018, [Online]. Available: http://arduino.cc.

[9] A. P. Zanofa, R. Arrahman, M. Bakri, and A. Budiman, "(in Indonesia) PINTU GERBANG OTOMATIS BERBASIS MIKROKONTROLER ARDUINO UNO R3," vol. 1, no. 1, pp. 22–27, 2020.

[10] D. E. Kurniawan, M. Iqbal, J. Friadi, R. I. Borman, and R. Rinaldi, "Smart Monitoring Temperature and Humidity of the Room Server Using Raspberry Pi and Whatsapp Notifications," *J. Phys. Conf. Ser.*, vol. 1351, no. 1, p. 012006, Nov. 2019, doi: 10.1088/1742-6596/1351/1/012006.

[11] I. E. K. Mekki, A. Kessar, and R. Mouaz, "Design of a Printed Circuit Board for Real-time Monitoring and Control of Pipeline's Cathodic Protection System via IoT and a Cloud Platform," *Int. J. Eng.*, vol. 36, no. 10, pp. 1667–1676, 2023, doi: 10.5829/IJE.2023.36.09C.11.

[12] O. Prokhorov, V. Prokhorov, A. Khussanov, Z. Khussanov, B. Kaldybayeva, and D. Turdybekova, "Complete Integrated Automation of the Electrochemical Corrosion Protection System of Pipelines Based on IoT and Big Data Analytics," *Computation*, vol. 10, no. 7, 2022, doi: 10.3390/computation10070123.

[13] W. Z. Taffese, E. Nigussie, and J. Isoaho, "Internet of Things based Durability Monitoring and Assessment of Reinforced Concrete Structures," *Procedia Comput. Sci.*, vol. 155, pp. 672–679, 2019, doi: 10.1016/j.procs.2019.08.096.

[14] M. R. Indra, N. Purwasih, M. A. M. Batubara, G. F. Nama, and N. Kasai, "Design and Implementation of Real-Time Reading System of Atmospheric Corrosion Sensor on Metal Material Using Internet of Things (IoT) Technology," in *2021 International Conference on Converging Technology in Electrical and Information Engineering (ICCTEIE)*, 2021, pp. 25–30, doi: 10.1109/ICCTEIE54047.2021.9650633.

[15] V. Fachriza Sukma, E. Kurniawan, and D. Faisal Budiman, "(in Indonesia) Sistem Pemantauan dan Perlindungan Korosi Logam Besi dengan Metode Impressed Current Cathodic Protection Berbasis Internet of Things (Iron Corrosion Monitoring and Protection System with Impressed Current Cathodic Protection Method Based on," pp. 154–161, 2022.

[16] S. Zafar, G. Miraj, R. Baloch, D. Murtaza, and K. Arshad, "An IoT Based Real-Time Environmental Monitoring System Using Arduino and Cloud Service," *Eng. Technol. Appl. Sci. Res.*, vol. 8, no. 4, pp. 3238–3242, 2018, doi: 10.48084/etasr.2144.

[17] N. Rohmalia, G. F. Nama, and N. Purwasih, "Dashboard Monitoring Atmospheric Corrosion Sensor in Material Metal Using Laravel Framework," *J. Eng. Sci. Res.*, vol. 3, no. 1, pp. 121–126, 2021, doi: 10.23960/jesr.v3i1.52.

[18] W. Z. Taffese and E. Nigussie, "Autonomous corrosion assessment of reinforced concrete structures: Feasibility study," *Sensors (Switzerland)*, vol. 20, no. 23, pp. 1–25, 2020, doi: 10.3390/s20236825.

[19] Z. Li *et al.*, "Application of An Electrical Resistance Sensor-Based Automated Corrosion Monitor in the Study of Atmospheric Corrosion," *Materials*, vol. 12, no. 7. 2019, doi: 10.3390/ma12071065.