International Journal of Manufacturing, Materials, and Mechanical Engineering (IJMMME)
Volume 2, Issue 1, January-June 2024, pp. 24-40, Article ID: IJMMME_02_01_003
Available online at https://iaeme.com/Home/issue/IJMMME?Volume=2&Issue=1
Journal ID: 2940-6442, DOI: https://doi.org/10.17605/OSF.IO/2BZD8

SECURE DATA TRANSMISSION AND MESSAGE AUTHENTICATION CODES FOR INDUSTRIAL AUTOMATION AND CONTROL SYSTEMS

Hima Bindu Lekkala
Manufacturing Engineer, Iowa, USA

Vishnu Vardhan Bandari
Manufacturing Engineer, Nebraska, USA

ABSTRACT

It is challenging to secure communication of systems like these, which span home automation, industrial, and automotive applications, and include a multitude of protocols, limited resources, and sometimes high demands in real-time. It is possible to use the idea of a detached MAC to guarantee the genuineness and security of data transfers between nodes in a network. This is especially helpful for older, less modern parts of the network that are still actively communicating with one another. The article explains the technology's workings via the lens of an evaluation simulation model. In it, the likelihood of discovering an attack is laid out to the message authenticating overhead. Confidentiality, integrity, and authenticity are three of the most important security concerns of data transferred in IACSS when subjected to deception attacks. System stability and performance may be severely compromised by deception attacks. To safeguard IACSS against these threats, this study presents a secure transmission method that combines the DES algorithm, the MD5 algorithm, and a timestamp technique. Data sent between the controller and the plant may be securely encrypted and decrypted using DES. To ensure that the data is valid and intact, the MD5 algorithm and a timestamp are used. All control factors are considered by the model, which uses random data flow for measurements. Even with a little communication overhead, the statistical analysis shows that a high assault detection rate is achievable. To prove that the suggested methods work, we conducted tests where we controlled the velocity of a DC motor via the Internet.

Keywords: Message Authentication Codes, Secure Data Transmission, Industrial Automation and Control Systems, DES and MD5

Cite this Article: Hima Bindu Lekkala and Vishnu Vardhan Bandari, Secure Data Transmission and Message Authentication Codes for Industrial Automation and Control Systems, International Journal of Manufacturing, Materials, and Mechanical Engineering (IJMMME), 2(1), 2024, pp. 24-40.
https://iaeme.com/Home/issue/IJMMME?Volume=2&Issue=1

I. INTRODUCTION

The contemporary world could not function without critical infrastructure, which includes things like water and power distribution networks. To ensure the safe and dependable functioning of CIs, industrial control and automation systems are crucial. Air-gapped IACSs are now open to cyber-attacks because of the proliferation of industrial Ethernet protocols for communications like Modbus-over-TCP (Modbus/TCP) [1]. When targeting industrial control systems, it is common for attackers to take advantage of weak security measures. Firewalls, detection systems for intrusions, and related appliances provide necessary checks, but how well they work relies on whether attackers can circumvent these middleboxes [2]. It is common for attacks towards ICSs to take advantage of weak authentication procedures. To stop unauthorized or hacked devices from injecting dangerous data or commands, make sure the messages you receive are complete and come from trusted sources. Nevertheless, the most significant obstacle is the implementation of message authentication for different ICS communication types, such as multicast or broadcast, that have a messaging rate reaching thousands of transactions per second and very tight latency requirements [3]. Because electric substations rely on automated control and communication, there is an inherent risk of cyberattacks that might undermine the security of the communications sent and received. There is no specific direction on how to implement message authentication methods, however, they are required by the IEC 62351 standard [4]. A growing number of crucial production processes rely on industrial control as well as automation technologies. Such systems rely on a vast amount of streaming data collected in real-time by a network of Internet of Things devices. While the problem of data authenticity in streaming may be solved with verifiable data streaming, the majority of VDS systems are inefficient, heavy, and unable to be utilized since they do not provide range querying [5]. One of the fastest rapidly expanding areas of technology right now is the IoT sector. The proliferation of gadgets and their increasing capabilities has ensured their pervasiveness in every facet of modern life, from buildings to healthcare. With the proliferation of wireless connection and industrial automation, it is now possible to network all building equipment [6]. The deployment of IIoT gadgets for processing, monitoring, and control has skyrocketed with the advent of 5G networks. Ensuring data security during production may be achieved using biometric-based user authentication, which can prevent unwanted access to IIoT equipment. The lack of template security in the majority of IIoT biometric authentication solutions puts at risk the raw biometric data kept as templates in centralized databases or devices in the IIoT [7].

1.1. Preliminary Knowledge of IACSs

Layered network designs using numerous protocols comprise an ICS, which in turn incorporates several loops of control, remote diagnostics, management tools, and user interfaces.

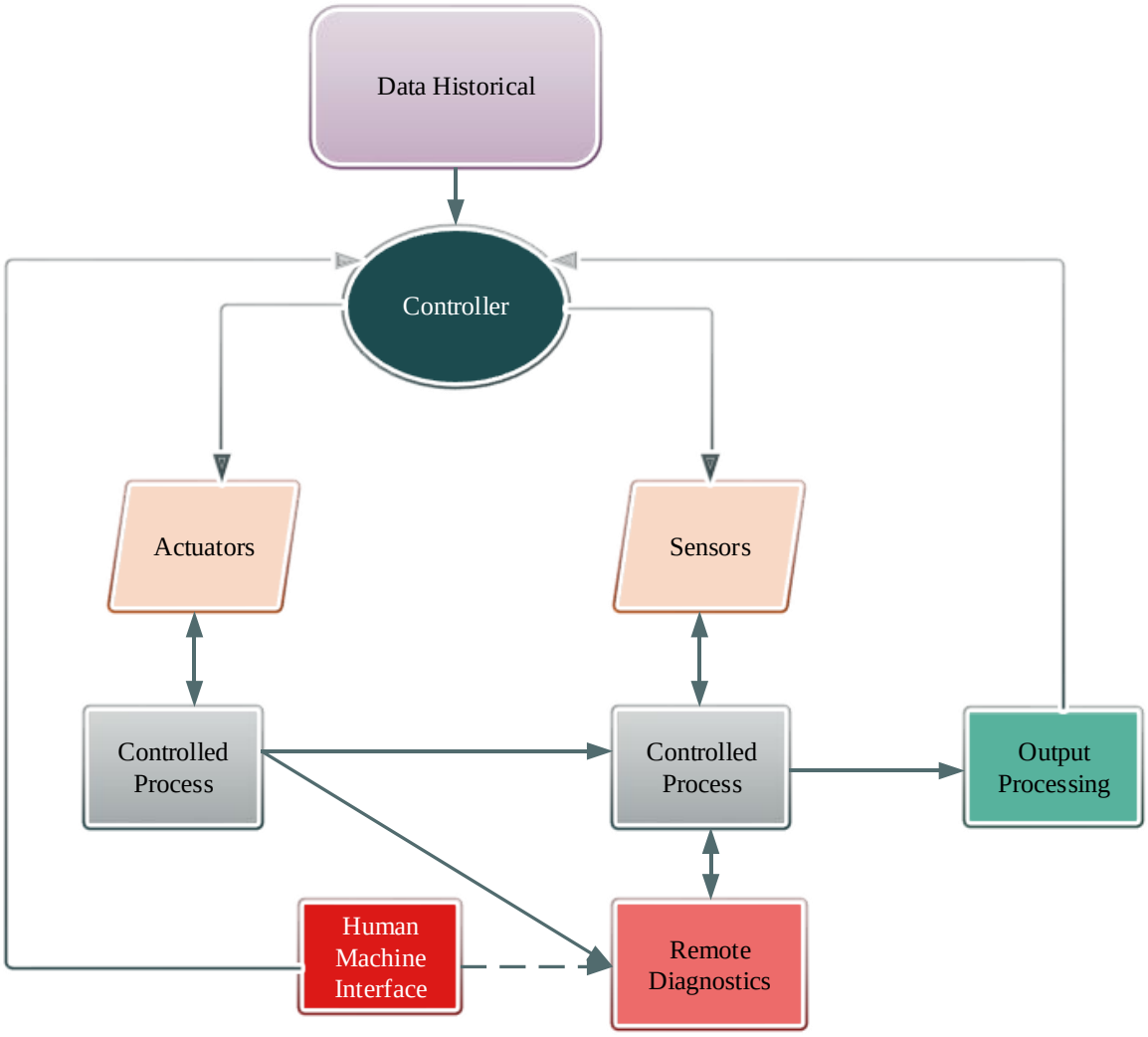


Fig.1. IACS using MAC.

Figure 1 provides an overview of the main parts and operation of an ICS.

- A control loop utilizes sensors, actuators, as well as controllers or PLCs to automatically change the output values to the desired set point.
- A process is a series of actions that lead to the intended output. A sensor takes readings from its surroundings and relays them to the controller as controlled variables.
- The controller then utilizes the targeted set point as well as control algorithms to create the necessary output variables and deliver them to the actuators.
- Machines use actuators, also called movers, to control and regulate mechanisms. These elements include control valves, device breakers, switches, and motors.
- HMIs, or human-machine interfaces, are tools that show process status information and allow users to configure controller parameters.
- RDM applications perform real-time diagnosis and maintenance, such as identifying, preventing, as well as recovering from abnormal activities or failures. All process data within an ICS context is stored in a centralized database called a Data Historian. The recorded data is sent to the company's IS for analysis, control, as well as planning purposes related to process data.

The host network nodes cannot communicate with remote networks like the internet or autonomous systems without the use of a communications gateway device. Either software or hardware may be used to implement this gateway. To prevent harmful assaults, it guides the network traffic along and may even block certain types of data. Additionally, it controls which machines on the network may communicate with the outside world.

Critical infrastructures throughout the country rely on ICS such as SCADA (supervisory control and data acquisition) systems to keep an eye on and manage a wide range of process industries. To share field data with third-party diverse systems like business resource planning and third-party SCADA systems, among others, they are connecting to the internet and highly connected corporate networks. Sharing data for system monitoring and control is helpful, but it also makes systems more vulnerable to cyberattacks. The cyber defenses of these systems for SCADA control must be beefed up [8]. Traditional MACs cannot be used to ensure the authenticity and integrity of messages in new applications like intelligent vehicle systems, the IoT, as well as industrial control systems because of the enormous scope of the MAC output [9]. The fast advancements in automation and intelligence, together with the widespread usage of the Internet of Things and other technologies in industrial production, have led to the idea of the IIoT. Ensuring the integrity of data, confidentiality, and anonymity is crucial, as the IIoT continues to encounter several network security risks. Data breaches involving personally identifiable information have been known to occur when semi-trusted third parties, such as servers in the cloud or on the edge, are used [10]. The latest generation of industrial control and automation systems are equipped with sophisticated connectivity functions, made possible by the rapid expansion of the Industrial Internet of Things. When industrial electronic devices' equipment connections are linked with a SCADA system using a Modbus protocol, the SCADA (Supervisory Control and Data Acquisition) network becomes an open as well as highly interconnected network. With SCADA and Modbus, control and monitoring are made easy, which greatly improves operational efficiency and the ability to link systems [11]. To facilitate interaction between humans and machines, an HMI system has been developed. The system is trained to interpret basic instructions, even when given at odd times, and the server may utilize that data to anticipate the user's next move, creating an intelligent workplace. All parameter values are pushed to the dataset whenever the hardware detects them [12], which stores the history. Sensors, networks, and amenities make up the IIoT, which is used to link and manage production systems. Monitoring the supply chain and detecting machine failures are two of its many advantages. But there are a lot of weak spots, such industrial espionage as well as sabotage. The use of conventional security services is further hindered by the fact that many IIoT devices have limited resources. Through authentication, devices can trust one another's identities, which in turn prevents certain security breaches [13]. The need for adaptable connections in industrial automation systems is being transformed by both technological developments and the ever-changing expectations of businesses. A service-oriented approach may help with these kinds of requirements by providing protocol-specific interfaces and a controller via connection service middleware. Many IoT devices communicate with one another via the Message Queuing Telemetry Transporter protocol [14].

The system's primary control is a Smart Relay, a kind of control system widely used in commercial and industrial settings. By replacing traditional control relays with smart ones, you can cut down on system writing and control relay use. You may operate the system and send messages using the smart relay's GSM-SMS. Messages and controls may only be made to the designated amount in the system [15].It is unclear, however, how well the suggested algorithm can identify an intruder given that sampled data is just an approximate estimate of the real thing.

To effectively control the bandwidth, it is crucial to alter the factors involved in packet sampling. Concerns about the validity, integrity, and secrecy of sensor and management data conveyed in IACSs are addressed in this work. Modifying data, delaying, or replaying data, or using a misleading sender identity are all examples of deception attacks that compromise data integrity and authenticity. Encrypting data and detecting deception attacks are two components of a secure transmission method (STM), which aims to prevent unwanted access and guarantee the authenticity and integrity of transmitted data. The DES algorithm is used to encrypt data. The MD5 algorithm with the timestamp approach is included in the DES cryptosystem to identify deception attempts. Subsequently, experimental results demonstrate the STM's functionality, proving the technology's viability and efficacy.

The following is the outline for the remainder of the paper: In Section II, we learn how the built-in plug-in device method works in the system. Section III explains the assessment paradigm that has been suggested. The outcomes of the simulations that were run are discussed in Section IV. Section V wraps up the report with a brief conclusion and a look at what's to come in the continuing research.

II. RELATED WORK

A new authentication approach based on MACs is presented in the study [16] to improve the cybersecurity of Modbus/TCP-based IACSs. The authors provide a new monitoring device that examines transmitted messages and confirms the validity of protected messages to offer partial security even while interacting with older Modbus/TCP peers. A CPS for water treatment was integrated into a programmed logic controller to serve as a digital twin to conduct experimental verification of the protection approach. The Chaskey-12 lightweight MAC described in IEC 29192-6 is the underlying MAC. The programming languages described in IEC 61131-3 were used to implement it in the PLC program. One more thing: the given approach safeguards communication between PLCs as well as other Modbus/TCP peers in preexisting IACSs without requiring firmware or hardware changes. The findings show that the approach can defend IACSs against network assaults while keeping performance relatively unchanged, which bodes well for the practicality of that kind of security. To ensure the security requirements are met, use the Timed Efficient Streams Loss-Tolerant Authenticating low-resource multiplex authentication protocols with redundant disjunct message routing to tolerate link failures, as described in [17]. They assume that TSN's time-sensitive traffic class uses schedule tables (referred to as Gate Control Schedules, GCLs) in the network's switches for task dispatching and that messages are sent via a static cyclic scheduling table. A setup includes job scheduling tables, message disjoint routes, and group control lists. They provide a formulation based on Constraint Programming that may be used to discover the best answer about our cost function. They also suggest a metaheuristic based on simulated annealing that can effectively solve big test cases. Multiple test scenarios are used to assess the two methods. To verify the whole delivery route of a message and any operations done on it, the authors of [18] suggested a provenance solution.

Cryptographically verifiable proof that a communication has arrived at its destination from a valid source and passed all required checks is provided by quick and adaptable provenance verification. Since it is transparent and uses a bump-in-the-wire architecture, F2-Relies on lightweight cryptographic elements and can adapt to different communication settings as well as protocols that are used in ICS. In that paper, they define formal variables and cryptographically demonstrate that F2-Pro is secure.

The provenance chain begins with a human user providing instructions, thanks to F2-Pro's multi-factor authentication system, which allows humans to communicate alongside ICS via a field services device. Through compatibility testing on a smart power grid testbed, they were able to demonstrate that a small ARM Cortex-A15 CPU results in a latency overhead per communications hop that is less than one millisecond. Both CMA and its multicast variation, CMMA, are proposed in the study as lightweight message authentication methods that use precomputation as well as caching to authenticate subsequent messages [19]. The C(M)MA algorithm removes all costly cryptographic operations performed by the recipients after receiving a message and all cryptographic operations performed by the sender after the message has been sent, with very little precomputation and transmission overhead. For even quicker confirmation of those with the greatest time-critical communications, C(M)MA considers the criticality profile (or probability) of a group of future messages. Based on a smart grid substation automation system, they show that C(M)MA is feasible in an ICS environment. In two separate smart grid and IIoT situations, an automated log analysis method based on neural network classifier training is implemented in the study [20]. Actual utility businesses in northern Italy along with a SIMATICS71500 PLC system were used to define and verify the technique. Using acceptable low bandwidth usage to retain the timing features of the industrial real-time ethernet, results demonstrate that the technique can operate in both situations. In the smart grid scenario, thousands of devices can transmit messages per second. In the IIoT scenario, up to 50 devices can send messages per second. An expanded version of the PBTree with a chameleon authentication tree, a chameleon identification tree using prefixes is introduced in [21]. Our system is ideal for devices with limited resources since it is lightweight, permits dynamic expansion, and allows for verified range queries in data streaming. They break down the algorithms used by the PCAT into four distinct steps: setup, data appending, query, as well as verification. Our research shows that the PCAT is fully compliant with VDS's security standards. The performance assessment and efficiency analysis also show that our scheme is very efficient and provides lightweight data streaming authentication, making the PCAT more suitable for use in industrial control and automation systems. The paper suggests using temperature, humidity, and pressure data to construct a system for energy management system monitoring [22]. The core components of the system are a BME280 sensor, a wireless network, an ESP8266 microprocessor, and the Messaging Queue Telemetry Transport (MQTT) communications protocol. For remote control and monitoring, the actuators and sensors are linked to the ESP8266, as well as an MQTT broker based on Mosquitto is installed on the RPi. Additionally, a novel method for displaying data in the Grafana framework and a database system specifically designed for time series, InfluxDB, were shown. In 2022, the suggested system was constructed in a controlled environment to track and manage energy use in real-time, considering the weather conditions in Poland. Using the SCADA (Supervisory Control and Data Acquisition) system to monitor plant information securely is suggested in [23]. Keys of a size of 4096 bits and 512 bits, respectively, are produced using the suggested modified asymmetric as well as hash algorithms. The encryption and decryption of data are handled by the ARM Cortex A53 CPU, which is used to implement the suggested security method.

It ensures that process information is valid and intact when sent over the Internet. Achieving almost 95% efficiency, it delivers a data transmission rate of 300 Mbps. That suggested approach enables safe monitoring of plant information from distant locations and may be used to protect internet-enabled industrial automation processes. The suggested big key size in asymmetrical algorithms improves the security of important process parameters. Damage to industrial equipment caused by illegal access or modification may be prevented by that suggested security algorithm.

It safeguards plant operators and guarantees that operations will run smoothly. The authors of the aforementioned research devised a novel approach to secure data transmission between data collection servers and PLCs by creating Secured Modbus Gateway Server along with Client modules [24]. The RSA along with AES algorithms were used to provide non-repudiation and secrecy in that approach, while the SHA algorithm was used to ensure message integrity. These modules are equipped to handle authentication and authorization as well. To further safeguard against replay attempts, the Modbus frame additionally contained and communicated a timestamp. Integrity, secrecy, non-repudiation, authorization, and authentication are all necessary aspects for secure data transport, and these modules and techniques support all of them. In addition, they provide functions that activate alarms in reaction to exceptions, as well as time stamps and frame filtering. In addition to being simply deployed in existing legacy systems, these modules also offer interoperability. To protect sensitive information, maintain user anonymity, and facilitate group signature and proxy re-encryption, researchers presented a new method of message authentication [25]. The authors demonstrate our scheme's security via theoretical analysis and efficiency comparison. Further, they apply our approach to a real-life publish/subscribe system, with the experimental outcomes validating its viability. That study presents an IoT design that utilizes the IOTA Tangle network to address the issue of cloud-based IoT storage centralization. It also uses the MAM (Masked Authenticated Messages) technique to track WSN data while ensuring data confidentiality and preservation [26]. It is not feasible to do proof-of-work computations in WSN edge devices due to the inadequate memory and processing power of many devices. So, to control the sensors, that study employs a logical key hierarchy-based approach and employs both asymmetric and symmetrical encryption in blockchain. Both the device's identity verification and the running cost may be efficiently accomplished. The study designs the hardware with ML and connects it to an embedded system using training datasets. It then leverages previous sensor datasets. An intelligent workspace may be created by using that data to train the system to comprehend basic instructions and then using the server's history to forecast the user's next move. In that way, they can ensure that industrial automation is safe. That work introduces an extension of the random forest method that may be used to accomplish the goals of reducing erroneous deductions, making crucial judgments, and obtaining correct results quickly. In addition to sending a warning message to the phone, it will sound an alarm if an accident is imminent. Implementing a secure sampling measured value communication in a substation automation system is discussed and analyzed practically in the study [28]. Technical Committee 57'sIEC Working Group 15 issued IEC62351 on safety for the IEC61850 profile in response to the standard's absence of such capabilities. There has been no validation or testing of computational capabilities or performance using commercial-grade equipment, and there has been no integration of authentication techniques for SV according to IEC62351 standards. Therefore, that study demonstrates the effectiveness of security feature-activated SeSV packets that are sent between control and protection devices. These packets are extended IEC61850 messages that include a MAC. The MAC-enabled SV message completely secures the process bus communications in the digital substation alongside minimum time delay, according to a prototype application on a low-cost commodities embedded device.

An intelligent automated home was created to address these issues in [29]. Methods: A gas detector, a motion detector (passive infrared (IR)), and a flame detector (to detect fire outbreaks) were the main components of the system that was created. The microprocessor was an ArduinoATMEGA328P.

To implement a smart home automation system, an ArduinoATMEGA328P served as the primary controller. The system's output is a buzzer that immediately alerts the user to anything. Additionally, using the worldwide system for mobile communications module, it notifies the user via their cell phone. In sum, the system achieved an accuracy rate of 94.44% and offered a cheap platform for the interconnection of different home gadgets and sensors via the Internet of Things. To bridge the gap between real-time network technology and the indicated scenarios, the authors of the article [30] first define IIoT scenarios and infer real-time needs along numerous axes. Here, they look back at the last five years of peer-reviewed research on real-time network technologies and how they've been used in industrial settings. We look at their potential uses in embedded devices, systems, and controllers. As a last step, they go over some of the unanswered questions surrounding the possibilities presented by real-time communication technology. Academics are showing an interest in real-time communication technologies, according to the evaluation. However, there is still no set of criteria that wireless technologies need to establish confidence in terms of safety and dependability.

III. PROPOSED WORK

A. Architecture Overview

Complete data security encompasses more than just keeping information private. The validity and integrity of transmission data is also a requirement for most IACSs, particularly in mission-critical applications.

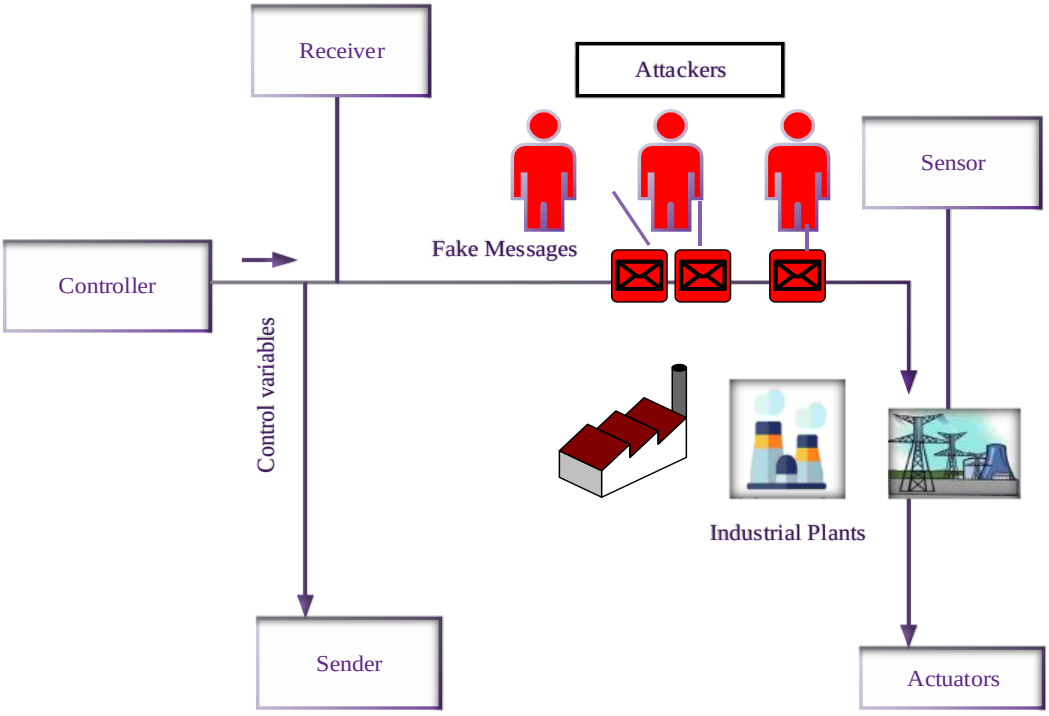


Fig.2. IASC Model The data must have maintained their integrity during transmission, and they must have come from a valid source since authenticity ensures that the data came from an authorized sender. Deception attacks, such as data alteration, misleading sender identity, and information delay/replay, occur when the integrity and authenticity of data are compromised. Rather than focusing on ways to avoid assaults, detecting measures should be examined because they pertain to actual attacks.

The two components of the secure transmission system (STM) shown in Figure 2—a secure UDP sender with a secure UDP receiver—are intended to accomplish data secrecy and the simultaneous detection of deception attempts. Each message M's header contains a timestamp T, which is used to generate the hash code H. Entire packets including the timestamp T, initial message M, with hash code H are delivered to the recipient in an encrypted format. The receiver decrypts the encrypted data packets upon arrival and then forwards them for hash and timestamp verification. Its timestamp is going to be matched to the receiver register's timestamp. Rejecting the data packet occurs when the former is not bigger than the latter. In every other case, the data packet is subjected to the MD5 technique to replicate the hash code. The data stream will be rejected if the computed hash code differs from the arriving hash code. If the two hash numbers match, the data packet, together with its date and message, will be added to the register as authentic and in order. To prevent attackers from forging messages with valid timestamps and hash codes that a secure UDP receiver may accept, these data security methods heavily depend on secrecy being enabled.

A. DES Algorithm for Encryption

After 16 iterations with a 64-bit key (really a 56-bit key), the DES algorithm reduces a 64-bit input (plaintext) to a 64-bit output (ciphertext).

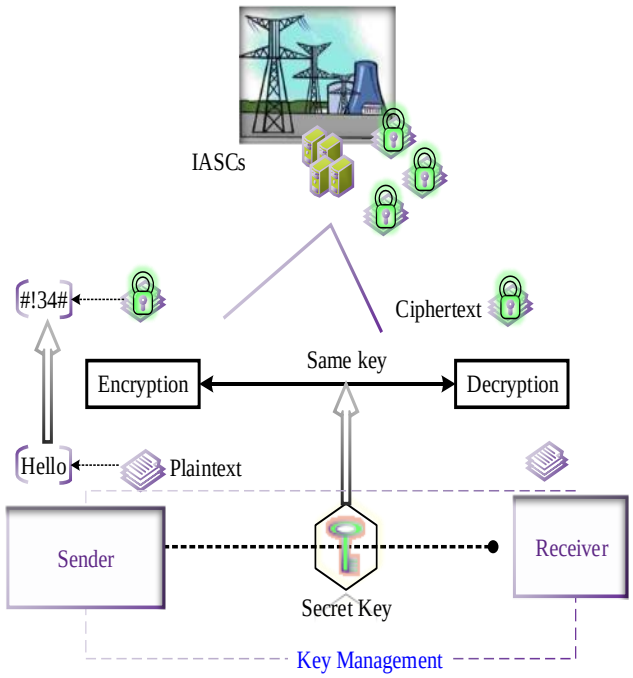


Fig.3. DES Model

There are three steps to the encryption process. The 64-bit inputs is first split into two 32-bit halves, labeled L_0 and R_0, after an initial inversion (IP). Data is processed using permutations, replacements, and XOR operations in the subsequent 16 rounds. The following is a description of each iteration:

$$\begin{cases} L_i = R_{i-1} \\ R_i = L_{i-1} \oplus f(R_{i-1}, K_i) \end{cases}$$

where ⊕ stands for the XOR operation and f is a four-operation function. To begin, a 48-bit sub-key K_i is XORed with the 32-bit right half of the 64-bit intermediate variable R_(i-1), which has been enlarged to 48 bits using an expansion permutation. Eight substitute boxes (s-box) are used to generate a 32-bit output from the result. In the end, we get the value of f by performing a permutation.

In the third phase of encryption, the 64-bit ciphertext is produced by merging the right (R_16) and left (L_16) halves of the output from the previous (sixteenth) round. This is then subjected to a final permutation (IP-1), which is the inverse of the original permutation function. The only difference between encryption and decryption is the sequence in which the sub-keys are produced. Methods for DES implementation include software tools, hardware, and software and hardware co-design. To encrypt and decode data, the DES algorithm only employs substitution-permutation operations, and to generate subkeys, it employs table look-up operations. Since hardware implementation of DES provides the fastest and most effective security, it is the optimal choice. The implementation of DES hardware, which can achieve an encryption rate of up to 290Mbit/s, has been selected for FPGA (Field Programming Gate Array) in order to satisfy the criteria of low-cost and reasonably high-performance for generic IACSs.

B. MD5 for Message Authentication

Hashing is a one-way function that may identify data modifications. It takes a message of variable size as input and produces an output of fixed size; other names for this function include message process, cryptographic checksum, and fingerprint. Changing the hash code is as simple as changing one or more bits in the message. As an example, SHA-1/256/384/512 is one of the most used secure hash algorithms, while MD5 is another popular hash function. It is nevertheless advised to use MD5 in the method shown in Figure 1, even if it does cause collisions (messages having the same hash code). So long as the DES cryptosystem remains unbroken, the MD5 algorithm is secure under this arrangement. Implementing the MD5 Algorithm in Software: MD5 generates a 128-bit hash code from messages of varying lengths. Following is a description of the MD5 operation flow. A padding operation is performed on the input message until its bit length is 448 modulo 512. Along with the padded result, we attach a 64-bit approximation of the initial message length. The final message is then split into data blocks of 512 bits. Iterative processing is applied to each data block, which is represented as 16 32-bit words. An intermediate result, referred to as a chaining variable, is computed for the first information block using a starting value of 128 bits. After that, the information provided in the input block and the prior outcome are used to update the chaining variable. When all iterations are complete, the hash code becomes the last chaining variable. You can use MD5 in both software and hardware, much as DES. This study opts for the latter. On the 180MHz 32-bit Atmel AT91RM9200 CPU running Linux 2.6.15, the MD5 software implementation utilizing C-MEXS Functions achieves a performance of 16.19Mbit/s. Identifying Changes to Data: Fig. 1 shows one use of MD5 for detecting data alteration attempts. To create a hash code, A gets a message in plaintext M ready and feeds it into MD5. Before being delivered to destination B, the hash code is appended to M and the whole block is encrypted using DES. The receiving end decrypts the incoming block and treats it as a message with a hash code attached. The hash code is then recreated by applying MD5 once again to the decryption message. A valid message will have a computed hash code that matches the one that was sent with it. Failure to do so will result in the message being considered altered while in route. Additionally, a data secrecy service is offered since DES has been used for the message plus the hash code encryption.

C. Sender Identity Detection

Most NCSs employ the UDP/IP protocol for real-time control purposes. There is an IP address specification for both the sender as well as the recipient. This means that data authenticity may be violated if attackers pose as genuine senders and deliver the recipient fake data. This type of attack may also be detected using the technique presented in Figure 1. This is because an attacker who does not know the DES secret key cannot alter data and generate a valid hash code that the rightful recipient can accept. So, the rightful recipient will be able to identify the material with the fraudulent sender's identity and delete it.

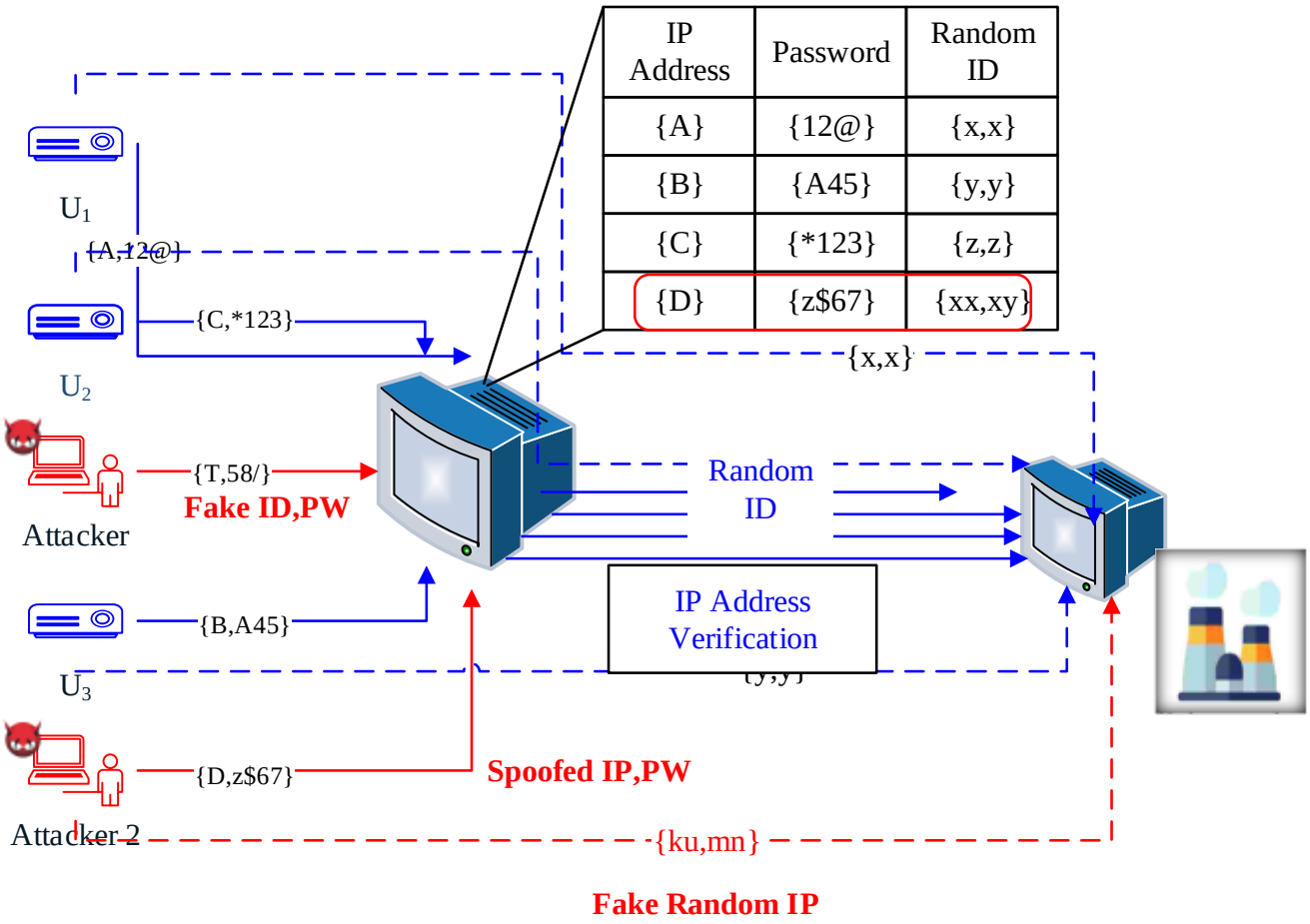


Fig.4. IP Verification

D. Data Delay/Replay Detection

There would be more network latency and data packet disorder if a data packet is intercepted afterwards replayed or delayed in the communication paths of IACSs.

Modeling of Sender Packets: Ato B traffic simulation is performed by this module. The dimension of each packet i and the amount of time that elapses between them define the packet flow. The elapsed time and

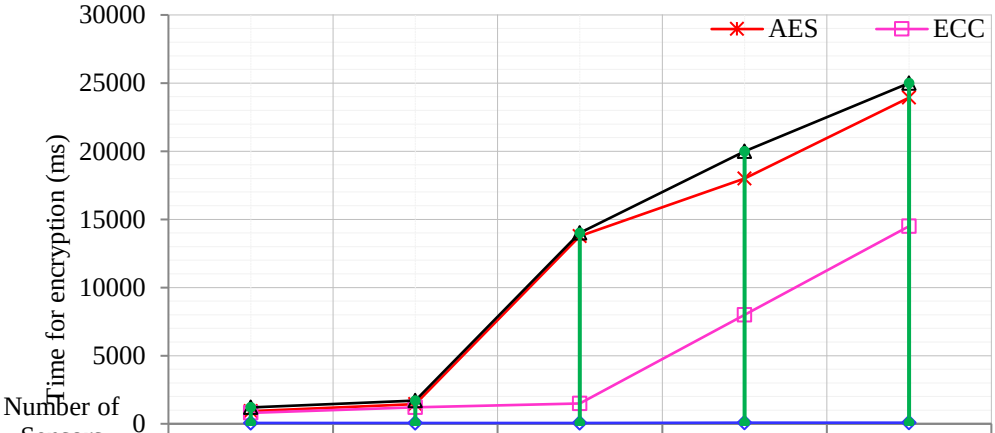
t_{gAi} =rand(tmingap_A,tmaxgap_A)

the size A_{Ai} = rand(min_packet_size_A,max_packet_size_A)

These are arbitrary numbers with predetermined limits. When the total time required to transmit a packet is more than zero, packets are created $t_{pAi} = \frac{A_{Ai}}{C}$ and the interval between each packet is about the maximum duration of the simulation. The information delay/replay attacks are undetectable by the technique shown in Figure 1 as the packets that the attackers manipulate are valid ones that have already been intercepted. Message unique identifiers are necessary for data delay/replay attack detection. A timestamp may serve as a unique identification for a communication by showing the exact moment the sender transmitted it. Along with a timestamp, a message is transmitted to the recipient. The receiver creates a register to keep track of the data packets, messages, and timestamps that arrive at the device at the previous sampled time. As soon as the receiver gets an additional information packet, it will check the timestamp against the one in the register. The information packet will be acknowledged, and the receiver's timestamp will be changed to the most recent one if the latter is bigger than the former. The information packet will be discarded if it does not comply, regardless of whether the two-time stamps are identical.

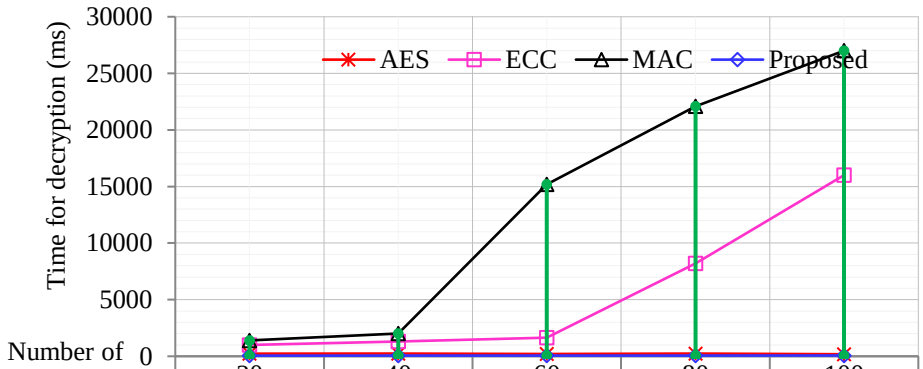
IV. RESULTS & DISCUSSION

To construct an Internet of Things (IoT) SCADA system, this research used a cryptography-based technique to implement a security mechanism that ensured a safe transmission route for all communications between SCADA field devices. Possible security components for use in preventing authentication and confidentiality threats, including suggested security implementation and calculated metrics. Whenever a session involving two or more nodes is in progress, the AES algorithm is used to build a secure channel. This means that communication takes place each time the sender and recipient nodes encrypt and decode their shared key using the given session consolidated.



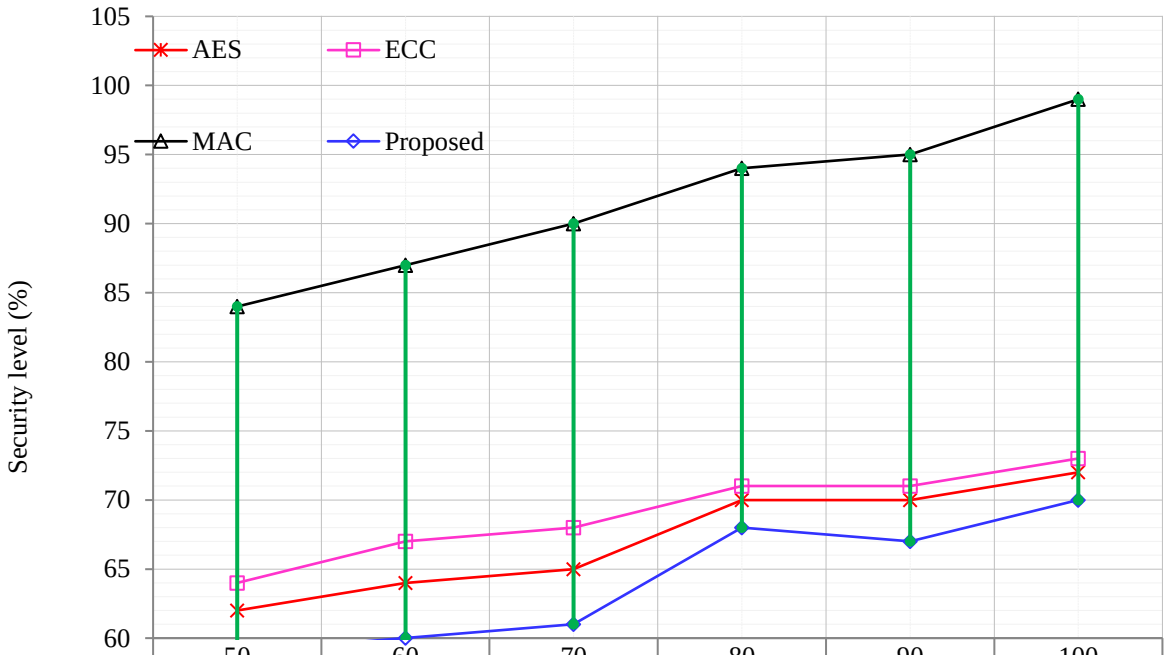
Number of Sensors	20	40	60	80	100
AES	927	1454	13760	18000	23933
ECC	800	1200	1500	8000	14500
MAC	1200	1700	14000	20000	25000
Proposed	61	68	70	75	80

Fig.5. Encryption Time Analysis



Number of Sensors	20	40	60	80	100
AES	220	240	200	240	180
ECC	1000	1300	1650	8200	16000
MAC	1400	2000	15200	22100	27000
Proposed	53	58	61	65	70

Fig.6. Decryption Time Analysis



	50	60	70	80	90	100
AES	62	64	65	70	70	72
ECC	64	67	68	71	71	73
MAC	84	87	90	94	95	99
Proposed	59	60	61	68	67	70

Fig.7. Analysis of security level

Each packet in the Internet of Things (IoT) SCADA system is encrypted with a secret key that has a session duration of 20 seconds. The target node uses the same secret key to decode the packets, and the transmission frequency is 50 times random size. If the 20-second session timer goes off, a new secret key will be generated and encrypted with the old one to prevent unauthorized parties from eavesdropping on the connection.

Comparing the performance of suggested and current systems in terms of encryption time, decryption time, and security level is the purpose of this computation.

The implementation of the DES and MD5 methods necessitates the existence of encryption keys on any device that can execute this algorithm. Because the safe and secure distribution of the keys is beyond the purview of this work, our present proposal is that these keys simply appear as input parameters to the SCADA IACSs that are doing the encryption. The challenge of securing data of the technical process state and equipment during the interchange among instrumentation and control devices SCADA for process control systems is brought up by the ways that are currently in use. Among the many approaches that are often used to guarantee the integrity of data is the use of cryptographic hash functions. Regrettably, the findings of a few research indicate that the implementation of well-known cryptographic algorithms demands a large amount of processing resources. Considering this, the most pressing challenge at hand is to create a hash function that is both reliable and lightweight, and that can perform hashing operations on devices that belong to the lower and intermediate tiers of industrial control systems. The description of a cryptographic protection tool has been provided to fulfill the urgent duty of assuring the integrity of the data in the systems that are now under consideration. This cryptography tool enables you to give a suitable degree of data security in a short period over their lifetime, while also having cheap resource costs to implement and high performance. The findings of cryptographic analysis were presented for the lightweight hash function known as "Mora," which was offered for usage. The study demonstrated that the function is cryptographically strong (which offers temporal resilience) in a particular model of the intruder. In this article, a generalized model of an intruder was developed for the devices and channels of communication that are located at the lower and intermediate levels of non-critical control systems in factories. The most harmful assaults on channels of communication were created, and the execution of such attacks to interrupt the process was outlined.

V. CONCLUSION

This work outlined a method for protecting IACSs during transmission against deception attacks, with a focus on protecting the authenticity, integrity, and secrecy of data. By combining the DES method with the MD5 algorithm and the timestamp approach, the STM can ensure the privacy of transmitted data and verify its validity and integrity. The suggested method is put to the test by constructing an online networked DC motor management test rig. To prove that the STM works, practical trials have also been conducted. It demonstrates that innovations in both areas of technology may enhance the IACS quantitative evaluation by around 10%. This article provides important recommendations for the cryptography implementation of industrial control systems based on the findings of quantitative analysis; these recommendations should serve as a benchmark for future work in this area.

Future enhancements are as follows:

- Incident Response and Remote Continuous Monitoring: reduce the need for human involvement by detecting and mitigating cyber threats faster via the implementation of effective incident response plans and continuous tracking of ICS networks.
- Intelligent Hardware Security: Improve the ICS components' security by creating and implementing hardware security features such as secured boot, cryptographic processors, as well as physical tamper detection.

- Machine learning algorithms should be taught to do varied jobs so they can solve many security situations.
- Develop diverse models. Retrained machine learning models can only be used for the same or related-tasks. When it comes to specific security problems, AI may streamline the response process. Security orchestration powered by AI can do things like detect compromised systems, stop harmful traffic, and start response procedures.

REFERENCES

[1] Young, J., Rasheed, A.A., Heshemi, R.R., & Bagabas, A. (2020). A Methodological Framework for Validating ZKP Authentication Process. 2020 IEEE 17th International Conference on Smart Communities: Improving Quality of Life Using ICT, IoT and AI (HONET), 37-43.

[2] Kant, D., Creutzburg, R., & Johannsen, A. (2020). Investigation of risks for Critical Infrastructures due to the exposure of SCADA systems and industrial controls on the Internet based on the search engine Shodan. MOBMU.

[3] Brandão, R.D. (2020). A blockchain-based protocol for message exchange in a ICS network: student research abstract. Proceedings of the 35th Annual ACM Symposium on Applied Computing.

[4] (2020). Iot Based End to End Solutions for Industrial Surveillance using Raspberry Pi. International Journal of Innovative Technology and Exploring Engineering.

[5] Abotaleb, M. (2023). Authenticated WiFi-Based Wireless Data Transmission from Multiple Sensors Through a Laboratory Stand Based on Collaboration Between ATMEGA2560 and ESP32 Microcontrollers. Scientific Journal of Gdynia Maritime University.

[6] Vijayakumaran, C., Muthusenthil, B., & Manickavasagam, B. (2020). A reliable next generation cyber security architecture for industrial internet of things environment. International Journal of Electrical and Computer Engineering, 10, 387-395.

[7] Rubinovitz, H.H., & Hahn, A. (2020). Industrial Control System Security (ICSS) Workshop.

[8] Erós, E., Dahl, M., Hanna, A., Gotvall, P., Falkman, P., & Bengtsson, K. (2020). Development of an Industry 4.0 Demonstrator Using Sequence Planner and ROS2. Studies in Computational Intelligence.

[9] Elumalai, G., Nallavan, G., & Ramakrishnan, R. (2021). Smart Industry Monitoring and Controlling System Using IoT. Advances in Parallel Computing.

[10] Hong, J., Karnati, R., Ten, C., Lee, S., & Choi, S. (2021). Implementation of Secure Sampled Value (SeSV) Messages in Substation Automation System. IEEE Transactions on Power Delivery, 37, 405-414.

[11] Oluwafemi, I.B., Bello, O.O., & Obasanya, T. (2023). Design and implementation of a smart home automation system. Innovare Journal of Engineering and Technology.

[12] (2022). Home Automation Using Internet Of Things modernh.

[13] Urooj, A., Khan, S., Shafiq, S., Ahmed, B., Basit, A., & Ansari, S. (2020). IoT-based fluid management automation system using Raspberry Pi and ultrasonic sensors. 3C Tecnología_Glosas de innovación aplicadas a la pyme.

[14] Deebak, B.D., & Al-turjman, F.M. (2021). Secure-user sign-in authentication for IoT-based eHealth systems. Complex & Intelligent Systems, 1-21.

[15] Lang, S., & Musah, T. (2024). Jitter-Based Authentication for Automotive Wireline Networks. IEEE Access, 12, 810-823.

[16] Katulić, F., Sumina, D., Groš, S., & Erceg, I. (2023). Protecting Modbus/TCP-Based Industrial Automation and Control Systems Using Message Authentication Codes. IEEE Access, 11, 47007-47023.

[17] Reusch, N., Craciunas, S.S., & Pop, P. (2021). Dependability-Aware Routing and Scheduling for Time-Sensitive Networking. IET Cyper-Phys. Syst.: Theory & Appl., 7, 124-146.

[18] Esiner, E., Tefek, U., Mashima, D., Chen, B., Kalbarczyk, Z.T., & Nicol, D.M. (2023). Message Authentication and Provenance Verification for Industrial Control Systems. ACM Transactions on Cyber-Physical Systems, 7, 1 - 28.

[19] Tefek, U., Esiner, E., Mashima, D., Chen, B., & Hu, Y. (2022). Caching-based Multicast Message Authentication in Time-critical Industrial Control Systems. IEEE INFOCOM 2022 - IEEE Conference on Computer Communications, 1039-1048.

[20] Bellagente, P., Flammini, A., Depari, A., Pasetti, M., Sisinni, E., Ferrari, P., Rinaldi, S., & Brandão, D. (2023). Applying Automatic System Log Analysis to Industrial Automation Systems for IoT Integration. 2023 IEEE International Workshop on Metrology for Industry 4.0 & IoT (MetroInd4.0&IoT), 7-12.

[21] Xu, J., Meng, Q., Wu, J., Zheng, J.X., Zhang, X., & Sharma, S. (2020). Efficient and Lightweight Data Streaming Authentication in Industrial Control and Automation Systems. IEEE Transactions on Industrial Informatics, 17, 4279-4287.

[22] Manowska, A., Wycisk, A., Nowrot, A., & Pielot, J. (2022). The Use of the MQTT Protocol in Measurement, Monitoring and Control Systems as Part of the Implementation of Energy Management Systems. Electronics.

[23] Prasath, J.S. (2021). Compound Cryptography for Internet of Things Based Industrial Automation. Internet of Things.

[24] Rajesh, L., & Satyanarayana, P. (2023). Design and Development of Secure Data Transfer Modules in Industrial Control Systems. Wireless Personal Communications, 132, 2667 - 2692.

[25] Cui, J., Wang, F., Zhang, Q., Xu, Y., & Zhong, H. (2021). Anonymous Message Authentication Scheme for Semitrusted Edge-Enabled IIoT. IEEE Transactions on Industrial Electronics, 68, 12921-12929.

[26] Lin, I., Chang, C., & Chang, Y. (2022). Data Security and Preservation Mechanisms for Industrial Control Network Using IOTA. Symmetry, 14, 237.

[27] Kotti, J. (2020). Industrial Automation with Safety Aspects using Machine Learning Techniques. Safety in Extreme Environments, 2, 183 - 188.

[28] Hong, J., Girdhar, M., Ten, C., Lee, S., & Choi, S. (2022). Cybersecurity of Sampled Value Messages in Substation Automation System. 2022 IEEE Power & Energy Society General Meeting (PESGM), 1-1.

[29] Oluwafemi, I.B., Bello, O.O., & Obasanya, T. (2023). DESIGN AND IMPLEMENTATION OF A SMART HOME AUTOMATION SYSTEM. Innovare Journal of Engineering and Technology.

[30] Behnke, I., & Austad, H. (2023). Real-Time Performance of Industrial IoT Communication Technologies: A Review. IEEE Internet of Things Journal, 11, 7399-7410.

Citation: Hima Bindu Lekkala and Vishnu Vardhan Bandari, Secure Data Transmission and Message Authentication Codes for Industrial Automation and Control Systems, International Journal of Manufacturing, Materials, and Mechanical Engineering (IJMMME), 2(1), 2024, pp. 24-40

Article Link:
https://iaeme.com/MasterAdmin/Journal_uploads/IJMMME/VOLUME_2_ISSUE_1/IJMMME_02_01_003.pdf

Abstract Link:
https://iaeme.com/Home/article_id/IJMMME_01_01_003

✉ **editor@iaeme.com**