Journal of Theoretical and Applied Information Technology
30th April 2026. Vol.104. No.8

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

ENHANCING CLOUD SECURITY IN INDUSTRY 4.0: A ROBUST IDENTITY AUTHENTICATION SYSTEM

[1]USHA V, [2]SRIDHAR M

[1]Research Scholar, Department of Computer Science, Sri Ramakrishna College of Arts & Science, Coimbatore, Tamil Nadu
[2]Assistant Professor and Research Supervisor, Department of Computer Technology, Sri Ramakrishna College of Arts & Science, Coimbatore, Tamil Nadu, India

[1]ushaswaminathen3012@gmail.com, [2]sridhar@srcas.ac.in

ABSTRACT

Solid cloud security could be a squeezing concern within the setting of Industry 4.0, which is characterized by the meeting of advanced and fabricating innovations. The need of dependable personality identification procedures in industrial transmission environments is discussed in this study as a significant barrier to progress in the manufacturing sector. Currently, there is no identity authentication in the system's architecture. Here, the omnipresent data collectors that make up the IoT send their data to a backend server via the time-tested Modbus protocol. Carefully designed to strengthen data security in the complex fabric of industrial settings, this identity identification system is a labour of love. Two main servers, the Register Server (RS) both the Backend Data Analysis Server (BDAS), the foundation of this system. A trusted authority, RS not only verifies the authenticity of IoT terminal devices but also registers their identities and generates JWT tokens. Beginning their trip with a registration request to RS, terminal IoT devices are then issued their own temporary identifiers (TIDi) by RS. Concurrently, RS produces tokens for effective devices, acting as a portal for encrypted data transfer. The methodology of the system breaks down the procedure into four discrete parts, including identity registration, first-stage authentication, token acquisition, and data transmission, each carefully divided to meet the highlighted difficulties. There are also three distinct phases to the authentication procedure: setup/initialization, identity registration, and authentication. In the first phase of identity registration, the registration server disseminates crucial information. There are five stages to the identity registration process, beginning with a registration request from the terminal IoT device and ending with information sharing and the coordination of individual TIDi identities. The identity identification phase is the most crucial, and it requires a comprehensive 13-step verification process that is broken down in detail from the point of view of various devices. As a whole, this article proposes a well-thought-out identity authentication methodology to strengthen cloud security in the Industry 4.0 scenario, providing a methodical means of dealing with the problems that have been highlighted.

Keywords: *Industry 4.0, Cloud security, Manufacturing sector, Cryptography, Security*

1. INTRODUCTION

Automation, exchange of information and sophisticated manufacturing solutions and technologies have collided to bring about a new wave of industrial transformation- usually referred to as Industry 4.0- that is marked by the convergence of digital and physical solutions. Although an agreement of higher productivity, flexibilities and competitiveness can be reached, the cybersecurity threats are equally high due to this change. Protecting sensitive data and making sure that the critical infrastructure is reliable have become the priorities of the modern world which is both highly connected; and data-driven.

The security of the cloud-based technologies that facilitate the industrial processes is a key issue in the Industry 4.0 setting. Increasing data storage, processing, and analytics in organizations are moving toward cloud platforms, which makes it vital to protect the privacy, integrity and availability of the systems. An attack on a cloud infrastructure may have dire impacts which include loss of data as well as slack of operation and significant financial losses. This is why it is of paramount importance to ensure that

cloud-based systems are secured by addressing possible cyber threats that are going to develop.

One major problem here is the absence of robust and secure processes of identity authentications in data transmissions settings within industries. High vulnerability to unauthorized access and data breaches is because several operational systems have weak or no device-level identification procedures. In most instances IoT gadgets send data to the backend provides through protocols like Modbus without authenticating them meaning that they can be spoofed and intercepted [1].

The proposed research seeks to solve these issues by coming up with an elaborate identity authentication solution to improve cloud security in Industry 4.0. The proposed system enhances data confidentiality and integrity by providing them with a secure data exchange in an industrial setting [2]. It has a major component, which is the Registration Server (RS) and the Backend Data Analysis Server (BDAS).

The RS is a trusted party and it registers the endpoint IoT devices that have authentication requests and produces the JSON Web Tokens (JWTs) to the devices that passed the initial authentication phase. This is initiated by a registration request by an IoT device to the RS. On a successful registration, the RS resort to temporary ID (TIDi) appointment and provides tokens that act as reliable entry points to encrypted data transmission [3].

The BDAS is implemented like a control server and authenticates token exchanges by the IoT devices being managed and authenticates the initial step of identity authentication of devices registered by the server. Once a device has successfully gone through this initial check, the BDAS will perform a second-stage verification procedure that will introduce a set of tokens that verify authenticity of the device and accuracy of the transmitted industrial data [4].
To contextualize the contribution of this work, the scope and boundaries of the study are defined as follows.

This paper specifically aims at coming up with and testing a lightweight identity authentication protocol with Industrial IoT devices that transfer data to cloud based systems. It is also confined to the registration of devices, mutual authentication, token verification and transmission of data in a secure manner. The suggested framework fails to deal with the rest of the cybersecurity factors like intrusion detection, anomaly classification, firmware update with security, and access control by users. In addition, the assessment uses authentication performance as a representative data(power-usage) and does not reflect on multi-tenant cloud systems or distributed industrial networks.

The system works on a number of realistic assumptions as applies in industrial setups. It is based on the assumption that the Registration Server (RS) and Backend Data Analysis Server (BDAS) has reliable connectivity and is trusted. IoT devices are expected to be safe repositories of private keys and with enough computing power to execute Elliptic Curve Cryptography (ECC) operations. Notwithstanding these assumptions, the study is limited: the solution has been tested only in a controlled testbed, primarily the evaluation is on authentication latency and cryptographic resistance and no post authentication processes like anomaly detection or threat mitigation are considered.

The objective of this project is to design a safe, effective and scalable identity authentication system which enhances confidence of devices in industry 4.0 systems. The system should be able to meet the following objectives; fast mutual authentication, low computational overhead and high resistance to impersonation, replay and unauthorized data injection. The major finding of the research proves that the integration of the ECC-based identity verification and the JWT-based secondary authentication lead to a lightweight but quite effective security system in industrial data transfer. The innovation of the described approach is that it combines temporary identity management, multi-stage authentication, and token verification- a rather unusual union, in comparison with the current industry IoT authentication options.

Even though Industry 4.0 systems are based on a heavy utilization of cloud-connected IoT devices, the majority of data transmission protocols that prevail in the market do not feature robust identity authentication, making the critical infrastructure vulnerable to device spoofing and data manipulation. The critical issue that this research is going to effect is the definition of the device identity before and during the communication of data. Based on this, the following questions are

investigated in the research:

RQ1: How can IoT devices in industrial environments be authenticated using a lightweight and computationally efficient method?
RQ2: How can multi-stage authentication be designed to ensure secure and trustworthy data transmission in cloud-based Industry 4.0 systems?

This paper is summarized as follows. Section 2 provides the literature review of the application of AI in cybersecurity to Industry 4.0, referring to the related work on encryption and cloud-based data protection. Section 3 explains why identity confirmation is not used in data transmission of industrial IoT and proposes the proposed system. Part 4 explains the identity registration, and authentication approach with the focus on Elliptic Curve Cryptography. In section 5, there is an account of the experimental set up and the authentication procedures. The resistance of the system to the usual threats of the network is given in Section 6 as the security analysis of common threat. Lastly, in Section 7, there is the closing of the importance of the proposed authentication system in enhancing Industry 4.0 cloud security.

2. LITERATURE REVIEW

The rapid development of Industry 4.0 has hastened the use of connected devices, cyber-physical systems (CPS), and cloud networks, which led to an enormous increase in the amount of cybersecurity threats requiring highly sensitive AI-focused protection frameworks. The studies on the hybrid cryptographic techniques, intelligent intrusion-detection systems, and adaptive authentication tools have been widely available to overcome the weakness of industrial networks. As an example, K. R. Sajay et al. [5] suggested a hybrid method of encryption that would combine Blowfish and Homomorphic Encryption to improve the confidentiality of data contained in a cloud. Their model minimizes exposure to access by unauthorized persons, but its computational cost as well as its real-time applicability in speedy industrial settings is unclear. Equally, Vikas K. Soman et al. [6] examined hybrid methods of so-called cryptographic security of cloud storage to give valuable information on encryption security but do not provide much analysis about scalability when large streams of sensor-driven data need to be processed. Prasanta Kumar Mohapatra et al. [7] contrasted a number of cloud encryption algorithms that are popular and emphasized on the increasing need to protect multimedia-data and notably image-based archives. But the effectiveness of these algorithms practically in cloud environments in an industry has not been thoroughly tested, and frameworks can be developed to ensure the safety of both structured and unstructured data at a large scale. There have also been significant studies on authentication strategies. The location-based authentication scheme described by Francis K. Mupila et al. [8] is intended to produce encrypted certificates and tokens that are related to the geographical location of the user. This is a promising approach to reducing access control violations, but the experiment does not examine the variation in performance under changing network conditions, which is typical of industrial systems with dense industrial IoTs. In line with this, Disha H. Parekh et al. [9] investigated the requirements in cloud-security and offered a supplementary PKI-based model to overcome key threats. Although their work has a systematic view on the concept of trust and identity management, it fails to discuss the problem of interoperability as well as the administrative burden in deploying PKI in the context of large Industry 4.0 worlds. Further, to the improved performance of DNN-based intrusion-detection, Zouhair Chiba et al. [10] suggested a hybridization method, where an Improved Genetic Algorithm (IGA) and Simulated Annealing Algorithm (SAA) are used. Although the approach is shown to be more accurate in detecting anomalies, they have not been tested in a real industrial network with much more heterogenous and unpredictable traffic.

The field of authentication strategies has also experienced significant research activities. Francis K. Mupila et al. [8] have presented a location-based authentication system that aims at creating encrypted certificates and tokens that are dependent on the geographical context of the user. The approach is a potential solution to reducing unauthorized access, but the researchers do not investigate how performance can change in response to changing network conditions that are frequently encountered in IoT-intensive industrial systems. Added to this, Disha H. Parekh et al. [9] reviewed the requirements of cloud-security and suggested a model of PKI to prove against the most important threats. Although their study is structured in terms of the management of trust and identity, it does not discuss issues of interoperability and administrative burdens when

PKI is implemented into the complex ecosystem of Industry 4.0. Also, Zouhair Chiba et al. [10] suggested that a hybrid optimization algorithm could be based on the application of an Improved Genetic Algorithm (IGA) and Simulated Annealing Algorithm (SAA) that would improve the detection and accuracy of intrusions by DNN-based identification. Although the approach has shown better results in detecting anomalies, it has not been tested on actual industrial networks whereby the traffic is invariably more heterogeneous and unpredictable.

Encryption and access-control systems are at a constant developmental stage because scientists are trying to maintain a balance between the aspects of security and computation speed. Binita Thakkar et al. [11] came up with a multilevel encryption system that integrates DES, transposition methods, and Blowfish to enhance the security of cloud-data. Even though multi-layer encryption can greatly enhance defence against brute-force attacks, the additional encryption duration can be problematic to industrial applications with limited latencies. Urvashi Rahul Saxena et al. [12] dealt with access control by proposing a role-based encryption model that combines Identity-Based and Broadcast Encryption so that the data owners can implement fine-grained access control measures. Although it is behaviorally appropriate in a cloud environment, the influence of the high frequency of role transitions, which can common in dynamic industrial teams, on encryption overhead is also not studied. Additionally, P. Chinnasamy et al. [13] explored ECC-Blowfish hybrid encryption model that has the ability to ensure safety of healthcare and industrial data sets. Although ECC offers the benefit of minimizing key size without compromising the effectiveness of its security, its performance in the real time setting with large-scale industrial communication challenges is under adequate evaluation. Ahmar et al. [14] referred to the issues of cybersecurity in the IoT-based Industry 4.0 environment and proposed a resistance to blockchain to enhance privacy and confidence. Nevertheless, blockchain has latency issues, energy consumption, and scalability that makes its usage in high-speed industrial automation doubtful.

Security approaches that are powered by AI have become dominant as the industrial sphere moves towards automated and interconnected processes. Alohali et al. [15] suggested a multi-model intrusion-detection system based on RNN, LSTM, and DBN, which had a higher detection accuracy than other models. However, its computational intricacy can limit real-time execution on minimal resource edge devices. Barton et al. [16] reviewed the literature on SMEs embracing AI in the IoT context of manufacturing, and highlighted that one of the factors hindering adoption is the concern of cybersecurity, as associated with lack of expertise, financial limitations, and failure to integrate the system. Blanco-Medina et al. [17] conceived a DL-pipeline to classify control-panel screen shots images, which can support cyber forensic in industrial environment. Although it is useful in classification, the method fails to detect anomalies on the behavior level, which is a gap in its ability to mitigate threats on a proactive mode. Meanwhile, Chang et al. [18] examined how frauds can be detected at the Industry 4.0 finance systems with the help of ML models. Even though their work is a valuable contribution to anomaly detection in the digital payment ecosystem, it is not applicable to cyber-physical attack vectors applicable to industrial automation.

The implementation of AI, cloud system, and IoT to manufacturing ecosystems has made cybersecurity requirements ever more challenging. Chen et al. [19] have talked about the obstacles to the adoption of the smart-manufacturing systems which are largely dependent on the areas of wireless communication, robotics, and automated decision-making. Their work mentions that security-enhanced architectures would be strong but it is not empirically proven to be applicable to real-life industrial deployments. The GIS monitoring system built by Elsisi et al. [20], being IoT-enabling and utilizing ML, provides the useful contribution to the predictive maintenance. Nevertheless, communication media of sensing systems based on IoT are still vulnerable to cybercrime and the research does not comprehensively deal with these safety flaws. Lastly, Khaled et al. [21] tested ICPS security based on attack scenarios that were produced by ML and confirmed their methodology on actual environments. Despite the encouraging results the technique provides, the narrowness of the attack datasets limits its application to different Industry 4.0 areas.

Among all the examined papers, a few gaps from a whole new perspective can be identified: the absence of real-time performance assessment, a lack of cross-model comparisons, and lack of insight into the deployment of a large-

scale industrial system, the absence of combined multi-layer security architectures, and the low number of studies validated on industry-specific data. These loopholes demonstrate the necessity of an even more sophisticated, flexible, and AI-based cybersecurity model that could respond to the constantly changing threat environment of Industry 4.0 ecosystems. The current research paper seeks to follow this path, and create a consolidated framework that goes to these unmet challenges.

3. PROBLEM DEFINITION

Without an identity authentication mechanism, the system architecture is depicted in Figure 1. IoT (Internet of Things) terminal devices collect operational data, which is transmitted directly to a backend server for parsing or analysis without undergoing any identity authentication process in conventional industrial transmission scenarios. The Modbus protocol is used for data transmission.

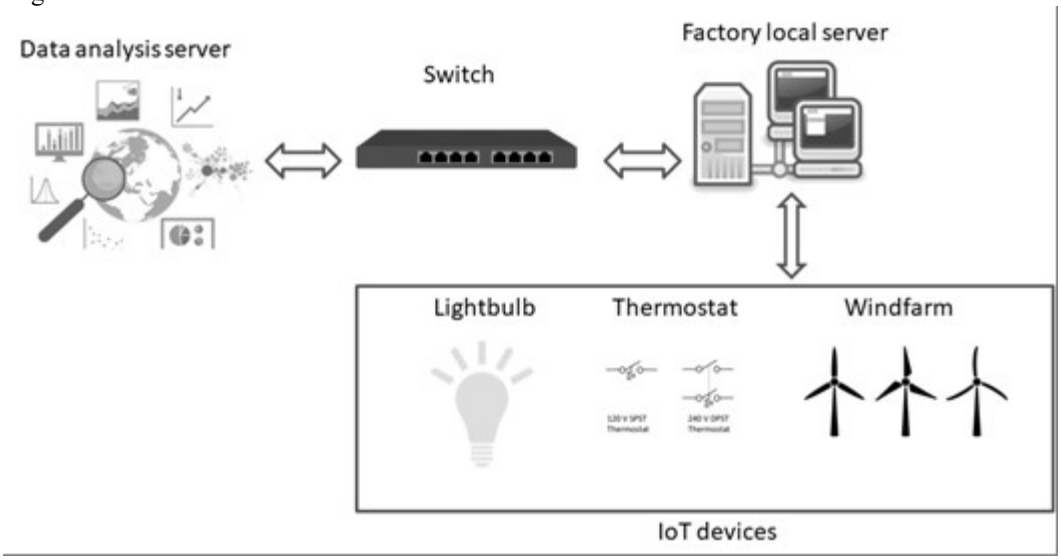

Figure 1. *The lack of verification steps in the industrial IoT system*

As can be seen in Figure 2, the proposed identity authentication system introduces a structured architecture designed to establish a secure channel for sensitive data transmission in industrial settings. The enhanced design integrates a robust authentication mechanism into the baseline system to prevent unauthorized access and ensure data integrity.

Register Server (RS):

In this paper's experimental setup, the trusted registration server performs a dual role:

- Terminals' identities must be registered with a reliable registration server.
- For devices that make it through the initial authentication phase, generate a JWT.

The terminal Internet of Things (IoT) devices in the proposed authentication system are required to initiate registration with the trusted registration server. Based on the registration request, this server generates a Temporary Identifier (TIDi) for the endpoint IoT device and relays it to both the device and the Backend Data Analysis Server (BDAS). Once the first stage of identity verification is successfully completed, the trusted registration server issues valid JWT tokens for use in subsequent encrypted data transmission. These tokens are utilized in the second stage of the authentication mechanism to confirm the legitimacy of the communicating devices and the accuracy of transmitted power data.

Backend Data Analysis Server (BDAS):

In this setup, the Backend Data Analysis Server (BDAS) emulates the role of an industrial control server, such as those used in power distribution systems. The server serves a dual purpose:

- Authenticate the identity of the IoT terminal device and establish a session key after successful registration.
- Verify the validity of the token communicated by the terminal IoT device to ensure that the received power information originates from a trusted source.

Journal of Theoretical and Applied Information Technology
30th April 2026. Vol.104. No.8

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

The terminal device's TIDi is shared with the BDAS via the trusted registration server. First-stage identity authentication is performed using TIDi and the corresponding registration data stored in the BDAS. If a device is verified as legitimate, the BDAS proceeds to the second stage of authentication by generating additional tokens to validate both device identity and data credibility.

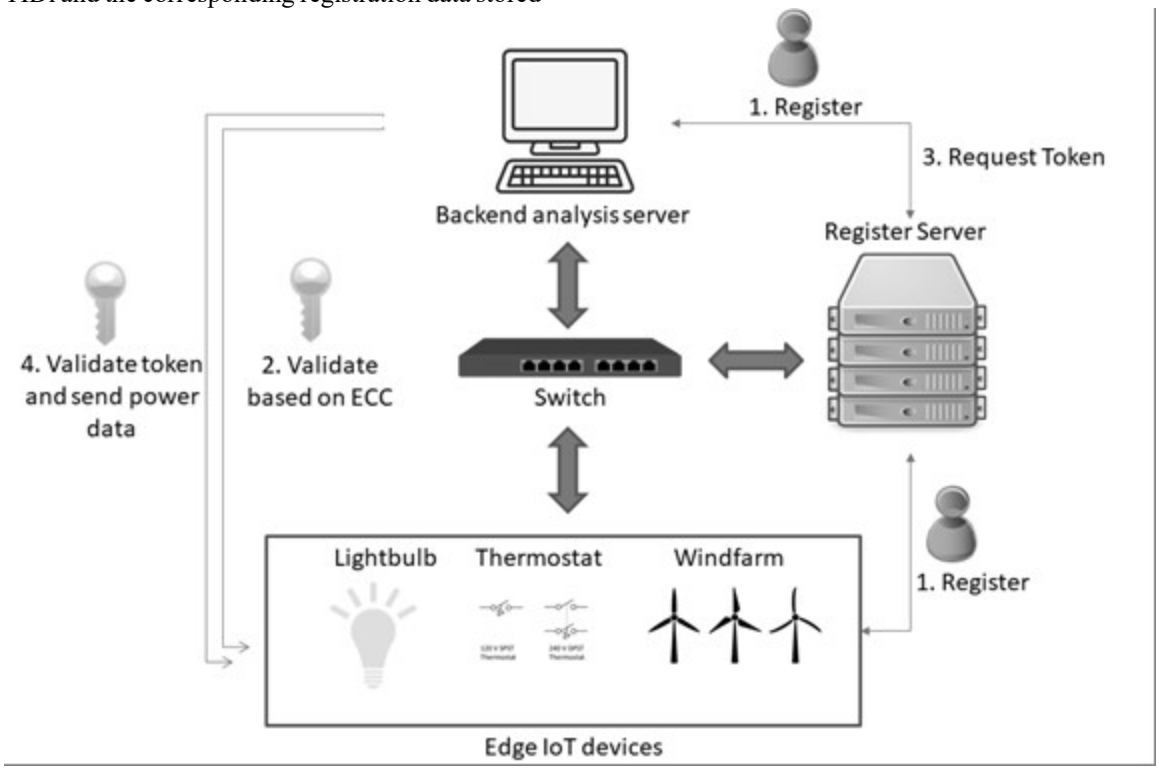

Figure 2. The proposed system

Although the trend is to utilize IoT systems connected to clouds as a part of Industry 4.0, every current data transmission system (including Modbus) has no native methods of authentication in place, which makes it prone to device spoofing, replay, and unauthorized data injection. Like the identified in the literature, most of the existing authentication systems either do not make use of computationally expensive cryptography operations or rely on token-based authentication systems that are not mutually verified, so they do not fit into the real-time industrial context. Also, not many solutions are combined to manage temporary identities with the multi-stage validation to be efficient and trustful. This paper discusses these drawbacks by presenting a hybrid identity system that integrates lightweight ECC-based mutual authentication with time-bound JWT tokens, to have a secure, speedy, and verifiable communication between IoT terminals and cloud-based backend servers.

4. METHODOLOGY OF THE PROPOSED SYSTEM

The proposed identity authentication system is structured into four sequential stages:

1. Identity Registration
2. First-Stage Authentication
3. Token Acquisition
4. Data Transmission

The stages guarantee safe and credible correspondence among IoT terminal equipment and servers in Industry 4.0 settings. The general authentication procedure involves three significant stages, which include: the initiation phase, identity registration phase as well as identity checking phase. This structured solution can be used in response to the lack of device-level authentication on industrial

transmission systems, that is, using insecure protocols such as Modbus.

Figure 3 illustrates the complete identity registration workflow, which establishes initial trust before any operational data exchange occurs.

4.1. Phases of Initialization and Individual Registration

In the setup stage, the Register Server (RS) establishes settings of the system and disseminates the necessary information needed in future identity management. This provides a stable and safe basis of registering devices.

As shown in Figure 3, the identity registration process involves five key steps:

1. The endpoint IoT device initiates registration by sending its permanent identifiers including EID_mac_address, EID_ip, EID_port, and EID_hostname to the RS.
2. Upon receiving the request, the RS generates a temporary identifier (TIDi) for the device, as defined in equation (1):

$$Select\ Temporary\_IDi\ (TIDi) = Random\ 256\ bits \quad (1)$$

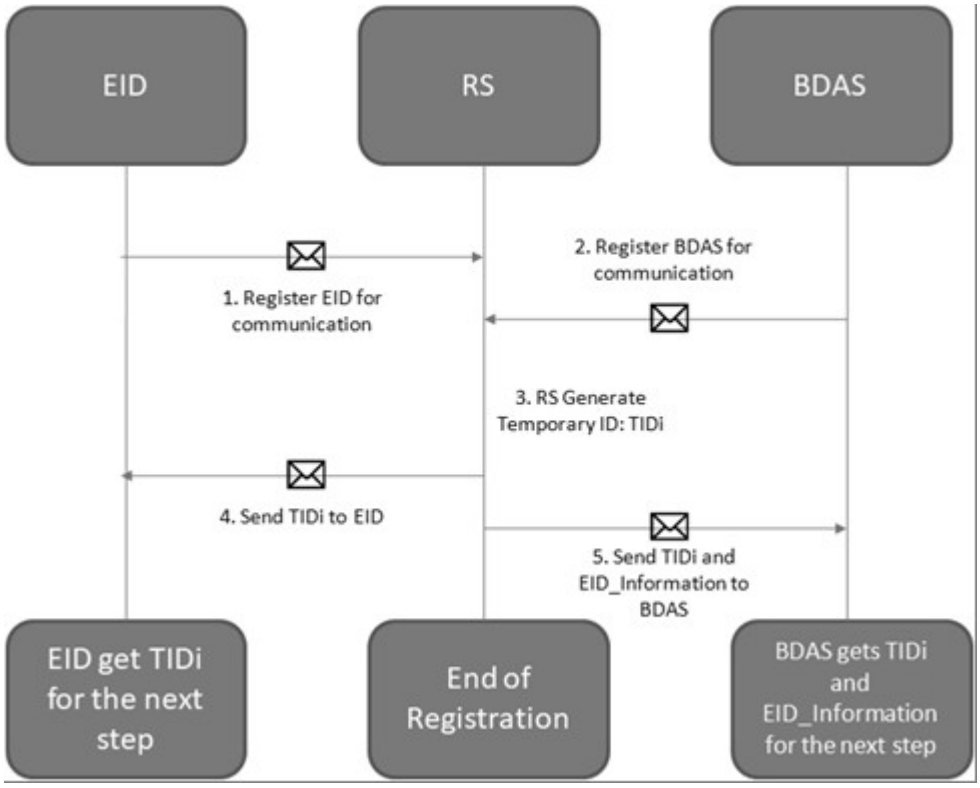

Figure 3. *The process of signing up for something.*

- This temporary ID enhances privacy and prevents long-term tracking of the device.
- The Backend Data Analysis Server (BDAS) shares its network details (BDAS_hostname, BDAS_host_ip, BDAS_mac_addr) with the RS to establish a trusted connection.
- The RS transmits the generated TIDi to the IoT terminal device.

- Simultaneously, the RS forwards the TIDi along with associated EID data to the BDAS for local storage, enabling future authentication validation during the verification phase.

This pre-authentication stage ensures that only registered devices are recognized in the system, laying the groundwork for secure mutual authentication.

4.2. Phase of Authenticating Identity

The identity authentication phase is a comprehensive verification process involving three entities: the IoT terminal device, the Backend Data Analysis Server (BDAS), and the Register Server (RS). The mechanism combines elliptic curve cryptography (ECC) for secure key exchange with JWT-based token validation to achieve strong security with minimal computational overhead making it suitable for resource-constrained IIoT environments.

Below 23 steps of equation depicts the verification procedure described in this paper for the identity authentication phase. Three devices in the verification mechanism each have their own viewpoint from which the process is described. As shown in below equations, during the authentication phase, creating a private key (ai) using elliptic curve cryptography is the first step for a local terminal IoT device. The apparatus does an elliptic curve point operation utilizing the generated private key to generate the public key (Ki). Ki, the obtained public key, is related to the X and Y coordinates (Kix and Kiy) through their respective values. An appropriate AIDi is computed by the terminal IoT device using the TIDi obtained in the registration phase. Following this, the encrypted AIDi is XOR'd with the elliptic curve public key (Ki) to derive its XY-axis values relative to AIDi. At last, the server doing the backend data analysis receives the verification notification N1. After the device has sent the N1 verification message, it will wait for the N2 verification message to be received back from the server performing the analysis of the final data. The details provided by the N2 confirmation message sent by the server doing the background analysis. By executing XOR on Wx, Wy, and AIDi in N2, the terminal IoT device can retrieve the backend server's public key for elliptic curve cryptography. To generate the session key TK_s*, the device must first acquire the public key used by the server performing the back-end data analysis. The session key is linked to the AIDi, and then Authenticate_i* is hashed to create it. The device checks for differences between Authenticate_i* and Authenticate_i. If the two values match, the device proceeds; otherwise, the connection is terminated. If validated, the device waits for a server-issued token. After receiving a token with the TK_encoded value, the target IoT device decodes it using AIDi, allowing it to retrieve the necessary data for further transmission. N4 is a message container that contains both the token and the data it represents.

$$Select\ Pri\_Key(ai) = Rand\ 256\ bits \quad (2)$$
$$Pub\_Key(Ki) = ai\ P \quad (3)$$
$$Ki = (Kix, Kiy) \quad (4)$$
$$Alice\_IDi(AIDi = \#(TIDi) \quad (5)$$
$$Encrypt\ AIDi) = Sign(AIDi) \quad (6)$$
$$Kx = Kix\ \varphi AIDi \quad (7)$$
$$Ky = Kiy\ \varphi AIDi \quad (8)$$
$$N1 =< TS_i, Kx, Ky, Sign(AIDi) > \quad (9)$$
$$N2 =< TS_s, Wx, Wy, Authenticate_i \quad (10)$$
$$Wsx = Wx\varphi RIDi \quad (11)$$
$$Wsy = Wy\varphi RDIi \quad (12)$$
$$Sessi\_Key(TK_s *) = ki.p \quad (13)$$
$$Authenticate_i *= \#(TK_S * ||AIDi \quad (14)$$
$$N4 =< TK\_enocde, Power\ data > \quad (15)$$

The server responsible for analysing data in the background is then given an account of the verification procedure. The authentication procedure of the data processing server checks the time stamp in N1. The connection is disconnected if the authentication fails. To verify the authenticity of an AIDi, the server that handles backend analysis of data employs a hash function on the TIDi received during registration. The backend data analysis server obtains the elliptic curve public key (Ki) of the IoT terminal device by performing an exclusive-or on Kx or Ky in the confirmation message N1. The backend data analysis server verifies the correct signature (AIDi) in N1 using the public key for the elliptic curve on the IoT terminal gadget. In the event that it is inaccurate, the link will be broken. In case everything checks out, the server performing the backend information examination will construct a private key (ws) for elliptic curve cryptography and then calculate the public key (Ws) by performing point multiplication on the elliptic curve. The X and Y coordinates of the public key (Ki) that was transmitted are used to derive the session key TK_s by performing elliptic curve point multiplication using the private key of the local data analytics server and the public key of the IoT endpoint gadget. At that point, the server performing the assessment of the data in the background will produce a timestamp TS_s. After the hash function is applied and the current session key TK_s and the AIDi are concatenated, the backend data analysis server will create the confirmation message Authenticate. The data in N2 is then bundled and sent to the IoT terminal for verification. As N2 is dispatched, the server analyzes the measurements within the foundation and creates N3. The N3 token is confirmed by the registration server and sent to the server for data analysis capacity. The backend data analysis server sends the encoded token TK_encoded to the IoT terminal device, which eventually sends back message N4.

$$Validate\ AIDi = decry(Sign(AIDi)) \quad (16)$$
$$Select\ BDAS\_Pri\_Key(ws) = Rand\ 256\ bits \quad (17)$$
$$BDAS\_Pub\_Key(Ws) = ws.P \quad (18)$$
$$Ws = (Wsx, Wsy) \quad (19)$$
$$Session\_Key(TK_s) = ws.Ai \quad (20)$$
$$Authenticate = \#(TK_s||AIDi) \quad (21)$$
$$N3 =< info\_EIS, TKs > \quad (22)$$

N4's token is checked against the one received by the data analysis server from its registration server. If they don't match up, the links are severed. If they match, then the information in N4 is received. Steps 8 and 9 in equations represent the verification procedure as seen by the registration server. After the information investigation server sends a message N3, the registration server checks to see whether the information_EID it contains is valid. Token requests that include any illicit data are naturally denied. The token TK_encoded, with the generation strategy portrayed in (23), is created by the registration server if acceptable.

$$TK\_encoded = jwt.encode() \quad (23)$$

This two-stage design combining ECC-based mutual authentication with JWT token validation addresses RQ1 by minimizing expensive cryptographic operations and supports RQ2 through dual verification. The use of temporary identifiers (TIDi) enhances privacy, while session-bound tokens prevent replay attacks offering a balanced, lightweight solution suitable for real-time industrial cloud environments.

5. RESULTS

5.1. Environment Setup

As can be seen in Table 1, Ubuntu 10.0 was utilised as the experimental server to construct the endpoint IoT devices, Register Server (RS), and Backend Data Analysis Server (BDAS). In Figure 4, we see a schematic representation of the experimentally fabricated real-world simulation. Figure 4 depicts the terminal smart metre and the server used to implement the authentication process, both of which were Ubuntu 10.0 computers. The data analysis server and the trusted registration server, both running Ubuntu 10.04, were

located in the meter box, while Ubuntu 10.0 served as the identification server for terminal devices. The identities of legitimate devices are registered with the trusted registration server, and the front-end devices are responsible for user authentication and data transmission to the back-end server for analysis.

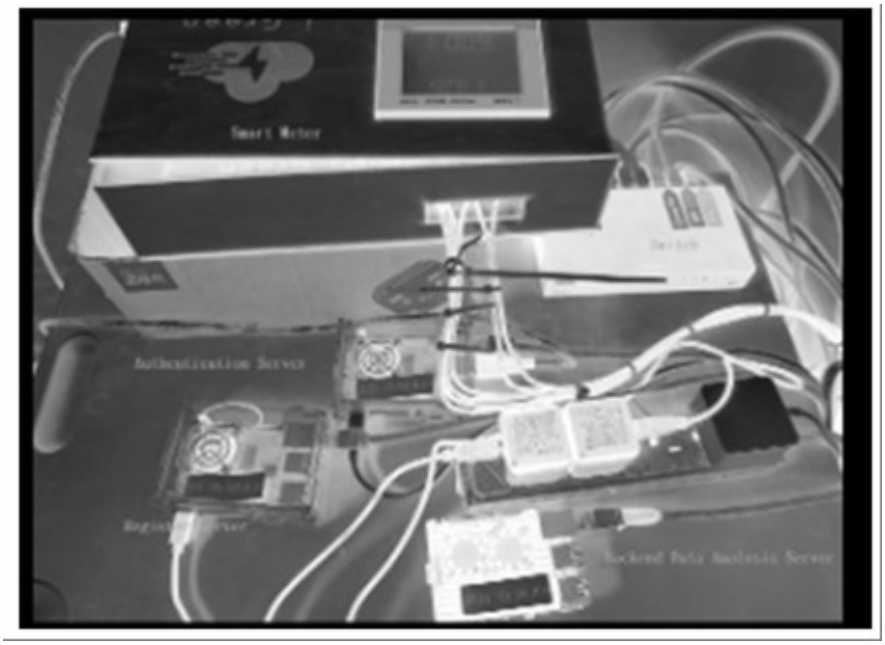

Figure 4. The Virtual Gadgets Used In The Suggested Procedure.

Table 1. Device Simulation Requirements.

	Server	OS	Storage
EID	Ubuntu 10.0	Ubuntu 10.0	64 GB
RS	Ubuntu 10.0	Ubuntu 10.0	64 GB
BDAS	Ubuntu 10.0	Ubuntu 10.0	64 GB

5.2. Elliptic Curve Cryptography Authentication Stage

In order to protect against future assaults that could compromise a lone elliptic curve cryptography or JWT verification mechanism, this study offers a verification system based on the combination of the two. Experiments with the proposed verification system are shown in Figure 5, specifically the registration and initial authentication mechanism execution phases. Figure 5 shows how the trusted registration server generates and transmits TIDi, while AIDi is generated locally by the IoT device. The endpoint of the IoT gadget and the information backend analytics server separately generate elliptic curve key pairs both private and public in the first stage, as appeared in Figure 5. An open key is utilized to encrypt AIDi at the terminal IoT gadget. Figure 5 appears that the terminal Web of Things gadget and the back-end information examination server derive session keys independently and approve AIDi for authenticity.

Figure 5. Elliptic curve cryptography refers to that method.

5.3. Phase of Authentication Using Credible Tokens

Tests with the second verification strategy, as seen from the Internet-of-Things gadget, the solid enrollment server, and the backend for information examination server, are illustrated in Figure 6. The reliable enrollment server disseminates a token to the information analytics server, which in turn gives it to an IoT gadget. The session key and AIDi are utilized by the IoT gadget to decode and approve the token's information. The server makes a request to the gadget, collects the information, bundles it, and sends it back to the server for processing. The tokens in this bundle are compared by the information investigation server within the background to see if they have been altered. The server will only recognize the package's control information if the token has not been modified in any way.

.

Figure 6. Token authentication method

5.4. Packet Encryption

In this study's authentication procedure, an IoT terminal with an exchanged data backend analytics server communication packets to confirm the identities of the parties involved (Figure 7). Because the TLSv1.3 protocol encrypts all packets

in transit, it is impossible for attackers to decipher any data included within them.

Figure 7. Packet-encryption-related data.

6. ANALYSIS

In this part, we will first go over the most frequent types of network assaults and then discuss how they might be defeated by the authentication method described in this work.

Security Analysis

6.1. Replay attack:

This study proposes an authentication mechanism that can foil replay assaults by confirming the timestamps (TSi, TSs) from both the terminal IoT gadget and the backend information examination server. In the event that the time of the confirmation ask is more seasoned than the session's termination, the framework will dismiss it as coming from a prohibited area. This implies that neither the aggressor can send any information to the terminal IoT gadget nor recover it through the backend investigation server, even if they replay already sent messages, since the timestamp will have already terminated. Unlike token-only schemes such as, which lack timestamp validation, our method ensures freshness without adding extra rounds of communication.

6.2. Attack on eavesdropping:

In this probe, the data packets in transit are encrypted using the TLS protocol. From the perspective of the attacker, the stolen packet therefore provides no insight into the contents of the packet.

6.3. Attack by a "man in the middle":

In this research, packets are encrypted using the TLS protocol. If a hacker steals a packet, they won't be able to decipher its contents and learn what was being transmitted. As a result, the attacker is unable to base on the information in the packet to alter the data. Both the IoT terminal and the server-side analysis service check the authenticity of the token if the encrypted data is modified. In other words, if the attacker alters the packet, the system will reject it as invalid. This dual-layer check TLS + token validation provides stronger protection than ECC-only methods, which do not verify application-layer tokens.

6.4. A simulated assault:

In the event that an aggressor needs to send information to the backend examination server from a false terminal IoT gadget, they will require the AIDi of the genuine gadget. In any case, since each server produces its claim AIDi, the assailant cannot

take their esteem. An aggressor who bypasses the primary confirmation step and enters the moment cannot steal the token utilized within the moment confirmation step since he or she does not have get to to the session key. In expansion, the terminal IoT device's token's legitimacy will be confirmed by the backend information examination server upon receipt of the message. Since the information investigation server is found assist absent, the aggressor cannot get to it specifically. This makes impersonation harder than in single-factor systems, where device identity is not bound to a session-specific token.

6.5. Encouragement of two-way authentication:

Common confirmation is characterized as a two-way prepare in which one party confirms the character of the other. To begin with, the endpoint IoT gadget with cloud-based information investigation server must pass a confirmation handle, this article makes utilize of AIDi, Authenticatei, and Authenticatei for personality verification. Amid the moment stage of verification, tokens are utilized to demonstrate the character of the endpoint IoT gadget to the backend information investigation server. This mutual verification is stronger than unidirectional schemes, where only the device is authenticated, leaving the server exposed to spoofing.

6.6. Support for forward secrecy:

The case of forward mystery in past session keys will stay covered up indeed in the event that the long-term fundamental key is compromised. Past communication can be protected from the hazard of crucial divulgence much obliged to forward mystery. A new session key is produced in each confirmation method underneath to scramble the information. The security of future communications isn't imperiled in case a session key is stolen from a past session. Unlike static-key protocols, which reuse session keys across sessions, our method ensures that each authentication generates a fresh key, enhancing long-term resilience.

7. ASSESSING EFFICIENCY

In this part, we compare the computing requirements of this work to those of other similar investigations. Elliptic curve cryptography, tokens generation after generation, and various other authentication-related encrypted methods have their time needs and descriptions of notation supplied in Table 2. Table 3 displays the results of our comparison of the suggested scheme to the schemes reported in numerous other studies for the purpose of performance evaluation. The authentication procedures employed in [22, 23] used elliptic curve cryptography in implementation, while relied on tokens for user authentication. Total authentication system time expenditures were weighed against those reported in. Compared to the LACKA-IoT proposed in, the TBLUA is the name given to the identity authentication protocol presented. In the anonymous authentication technique was suggested to ensure the authenticity of users without revealing their identities. There are four phases to LACKA-IOT: initialization of the system, device registration, access control, and dynamic addition of devices. It's fascinating to see how LACKA-IOT uses a combination of point addition and multiplication on elliptic curves for its verification. The trustworthiness of timestamps is checked as the first stage of cross-device verification. When adding devices on the fly, a registration identity process is also implemented. The authors of this research [23] propose a secure authentication method built on top of wireless sensor networks. In their authentication system, they utilise a fuzzy extractor to convert data about the user's biometric features into a string of constant length, and elliptic curve cryptography to perform the verification. There are four phases of TBLUA authentication: the offline registration of smart devices and the gateway, the reservation of users, the allocation of tokens to smart devices, is the last stage of login and authentication. The registering authority chooses a device ID and creates a random number of 1024 bits to be used as the gateway's ID during the off-line registration phase. In order to access the features of smart gadgets, users must first reserve their accounts with the registering authorities. Tokens are periodically distributed to a set of smart devices by the gateway during the token allocation phase. After signup is complete, users can go on to the login-authentication phase, where numerous gateways and intelligent devices will be used for mutual and individual authentication. The smart gadget establishes a session key with the user after successful authentication, granting the user access to the device's capabilities. Utilisation exclusivity is shared by user reservation, token distribution, login, and authentication OR procedures and hash functions to encrypt messages exchanged among gadgets or between devices and users, lowering time and computational costs greatly. The total validation time of [22, 23] is significantly longer than and the suggested authentication mechanism in this paper. The overall time spent using the authentication system was

calculated by averaging the timespan of fifty individual checks for this study. From the moment Up to the point when the data was supplied to the back-end processing server, the terminal Internet of Things device requested registration, the fastest of the tested authentication systems took only 29.21 milliseconds, as shown in Figure 8.

Table 2. Time-Related Notation Explained.

Notation	Description
T_{eca}	Addition of elliptic curves and its computational complexity
T_{ecm}	The complexity of multiplying elliptic curves computationally
T_h	Hash function's computational overhead
T_{xor}	Expense of computation for an exclusive OR
T_{jwt_enc}	Cost of encoding a JSON Web Token computationally
T_{jwt_dec}	Decoding a JSON Web Token's Computational Expense
T_{enc}	Symmetric encryption's per-encryption cost
T_{dec}	Symmetric cryptography's per-decryption cost

Table 3. Each procedure's time-to-completion complexity

Method	Total Cost
LACKA-IoT	3 Teca + 7 Tecm + 6 Th
Anonymous Authentication Protocol	6 Tecm + 19 Th
TBLUA [22]	42 Th + Tdec
Proposed method	4 Tecm + 5 Th + Tjwt_enc + Tjwt_dec + 8 Txor

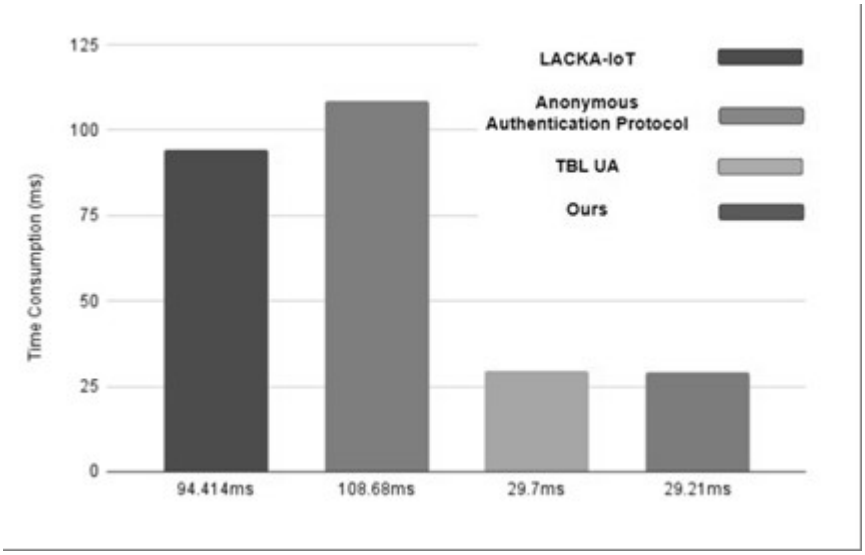

Figure 8. The Analysis Of Time Spent

8. CONCLUSION:

Industry 4.0 is changing the manufacturing and production landscape, making robust cloud security more imperative than ever. This is due to the integration of digital technology and industrial processes. The lack of strong identity confirmation methods is a genuine issue in industrial transmission situations, and this study aims to address that issue. Information is collected by terminal IoT devices and sent directly into a backend server through the Modbus protocol without legitimate security shields, as shown in Figure 2 of the current framework architecture. On the other hand, the Register Server (RS) and the Backend Data Analysis Server (BDAS) are critical to the proposed authentication scheme. One of the important functions of RS is the identification of IoT terminals and the implementation of JWT. Under such a configuration, terminal IoT devices request registration with RS which assigns temporary identities (TIDi) and tokens to the registered gadgets. Such tokens act as points of entry to confidentiality of information exchange. The paper covered the authentication process fully including registration of identities to initial authentication, obtaining of token as well as data transmission in a systematic manner in solving the problems that arise in the process. The authentication process consists of three phases namely: setup, identity registration and verification. All in all, the proposed research will enhance data integrity and confidentiality under the Industry 4.0 by developing an effective identity authentication system, which will address an essential security gap in industrial transmissions setting, and enhance cloud security.

The originality of the work is the combination of temporal identity administration (TIDi), two-way authentication with ECC and JWT, and forward secrecy with dynamically generated session keys, which have not been previously integrated in the IIoT authentication models. The main contribution is a lightweight but secure mechanism that would achieve computation efficiency and good level of trust assurance, hence suitable in industrial cloud applications which are real-time. This system would help to enhance the security of older protocols such as the Modbus in intelligent manufacturing systems by a good margin. Nonetheless, the existing implementation is restricted to a testbed controlled and presupposes the trusted RS and clock synchronization. The next steps in work may be the investigation of decentralized identity models, artificial intelligence-enhanced anomaly detection in failed logins, and post-quantum cryptography adaptations.

REFERENCES:

[1]. Liu, Y., Hassan, K. A., Karlsson, M., Pang, Z., & Gong, S. (2019). A data-centric internet of things framework based on azure cloud. *IEEE Access*, *7*, 53839-53858.

[2]. Aryavalli, S. N. G., & Kumar, G. H. (2023). Safeguarding Tomorrow: Strengthening IoT-Enhanced Immersive Research Spaces with

State-of-the-Art Cybersecurity. *Archives of Advanced Engineering Science*, 1-22.

[3]. Flatt, H., Schriegel, S., Jasperneite, J., Trsek, H., & Adamczyk, H. (2016, September). Analysis of the Cyber-Security of industry 4.0 technologies based on RAMI 4.0 and identification of requirements. In *2016 IEEE 21st International Conference on Emerging Technologies and Factory Automation (ETFA)* (pp. 1-4). IEEE.

[4]. Alani, M. M., & Alloghani, M. (2019). Security challenges in the industry 4.0 era. *Industry 4.0 and engineering for a sustainable future*, 117-136.

[5]. Sajay, K. R., Babu, S. S., & Vijayalakshmi, Y. (2019). Enhancing the security of cloud data using hybrid encryption algorithm. *Journal of Ambient Intelligence and Humanized Computing*, 1-10.

[6]. Soman, V. K., & Natarajan, V. (2021). Analysis of hybrid data security algorithms for cloud. In *Second International Conference on Networks and Advances in Computational Technologies* (pp. 231-242). Springer.

[7]. Mahapatra, P. K., Tripathy, A. R., Tripathy, A., & Mishra, B. (2020). Security model for preserving privacy of image in cloud. In *Advances in Data Science and Management* (pp. 247-256). Springer, Singapore.

[8]. Mupila, F. K., & Gupta, H. (2021). An innovative authentication model for the enhancement of cloud security. In *Innovations in Computer Science and Engineering* (pp. 447-455). Springer, Singapore.

[9]. Parekh, D. H., & Sridaran, R. (2018). Mitigating cloud security threats using public-key infrastructure. In *Cyber Security* (pp. 165-177). Springer, Singapore.

[10]. Chiba, Z., Abghour, N., Moussaid, K., & Mohamed, R. (2019). Intelligent approach to build a Deep Neural Network based IDS for cloud environment using a combination of machine learning algorithms. *Computers & Security*, 86, 291-317.

[11]. Thakkar, B., & Thankachan, B. (2022). An approach for enhancing the security of data over the cloud using a multilevel algorithm. In *Congress on Intelligent Systems* (pp. 305-318). Springer, Singapore.

[12]. Saxena, U. R., & Alam, T. (2022). Role-based access control using identity and broadcast-based encryption for securing cloud data. *Journal of Computer Virology and Hacking Techniques*, 18(3), 171-182.

[13]. Chinnasamy, P., Padmavathi, S., Swathy, R., & Rakesh, S. (2021). Efficient data security using hybrid cryptography on cloud computing. In *Inventive Communication and Computational Technologies* (pp. 537-547). Springer, Singapore.

[14]. Ahamad, B.; Khan, M.A.; Khan, J.; Alghamdi, A.A. Cybersecurity Challenges and Threats in Adoption of Industry 4.0: A Disscussion over Integration of Blockchain. *Int. J. Early Child. Spec. Educ.* **2022**, *14*, 3616–3623.

[15]. Alohali, M.A.; Al-Wesabi, F.N.; Hilal, A.M.; Goel, S.; Gupta, D.; Khanna, A. Artificial intelligence enabled intrusion detection systems for cognitive cyber-physical systems in industry 4.0 environment. *Cogn. Neurodyn.* **2022**, *16*, 1045–1057.

[16]. Barton, M.; Budjac, R.; Tanuska, P.; Gaspar, G.; Schreiber, P. Identification Overview of Industry 4.0 Essential Attributes and Resource-Limited Embedded Artificial-Intelligence-of-Things Devices for Small and Medium-Sized Enterprises. *Appl. Sci.* **2022**, *12*, 5672.

[17]. Blanco-Medina, P.; Fidalgo, E.; Alegre, E.; Vasco-Carofilis, R.A.; Jañez-Martino, F.; Villar, V.F. Detecting vulnerabilities in critical infrastructures by classifying exposed industrial control systems using deep learning. *Appl. Sci.* **2021**, *11*, 367.

[18]. Chang, V.; Doan, L.M.T.; Di Stefano, A.; Sun, Z.; Fortino, G. Digital payment fraud detection methods in digital ages and Industry 4.0. *Comput. Electr. Eng.* **2022**, *100*, 107734.

[19]. Chen, K.C.; Lin, S.C.; Hsiao, J.H.; Liu, C.H.; Molisch, A.F.; Fettweis, G.P. Wireless Networked Multirobot Systems in Smart Factories. *Proc. IEEE* **2021**, *109*, 468–494.

[20]. Elsisi, M.; Tran, M.Q.; Mahmoud, K.; Mansour, D.E.A.; Lehtonen, M.; Darwish, M.M.F. Towards Secured Online Monitoring for Digitalized GIS against Cyber-Attacks Based on IoT and Machine Learning. *IEEE Access* **2021**, *9*, 78415–78427.

[21]. Khaled, A.; Ouchani, S.; Tari, Z.; Drira, K. Assessing the severity of smart attacks in industrial cyber-physical systems. *ACM Trans. Cyber-Phys. Syst.* **2021**, *5*, 10.

[22]. Das, A.K.; Wazid, M.; Yannam, A.R.; Rodrigues, J.J.P.C.; Park, Y. Provably Secure ECC-Based Device Access Control and Key Agreement Protocol for IoT Environment. IEEE Access **2019**, 7, 55382–55397.

[23]. Li, X.; Niu, J.; Bhuiyan, M.Z.A.; Wu, F.; Karuppiah, M.; Kumari, S. A Robust ECC-Based Provable Secure Authentication Protocol With Privacy Preserving for Industrial Internet of Things. IEEE Trans. Ind. Inform. **2018**, 14, 3599–3609.