This article has been accepted for publication in IEEE Access. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2024.3351485

IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Date of publication xxxx 00, 0000, date of current version xxxx 00, 0000.

Digital Object Identifier 10.1109/ACCESS.2023.Doi Number

A New Trend in Cryptographic Information Security for Industry 5.0: A Systematic Review

Zaffar Ahmed Shaikh[1], (Member, IEEE), Fahima Hajjej[2], (Member, IEEE), Yeter Demir Uslu[3], (Member, IEEE), Serhat Yuksel[3,4], (Member, IEEE), Hasan Dincer[3], (Member, IEEE), Roobaea Alroobaea[5], Abdullah M. Baqasah[6], Uma Chinta[7], (Member, IEEE)

[1]Benazir Bhutto Shaheed University Lyari, Karachi 75660, Pakistan
[2]Princess Nourah bint Abdulrahman University, Riyadh 11671, Saudi Arabia
[3]Istanbul Medipol University, Istanbul, Turkey
[4]Lebanese American University, Beirut, Lebanon
[5]Department of Computer Science, College of Computers and Information Technology, Taif University, P. O. Box 11099, Taif 21944, Saudi Arabia
[6] Department of Information Technology, College of Computers and Information Technology, Taif University, Taif 21974, Saudi Arabia
[7] Department of Computer Science, University of Colorado, Colorado Springs, USA

Corresponding author: Zaffar Ahmed Shaikh (e-mail: zashaikh@bbsul.edu.pk).

This work was supported in part by the Princess Nourah bint Abdulrahman University Researchers Supporting Project number (PNURSP2024R236), Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia.

ABSTRACT Malicious assaults and information leakage have grown in importance in practically every area of information and communication technology (ICT) in recent years. Enterprise ledger organization, preservation, security, and protection are all greatly aided by information security (IS). To maintain their positions in the market, industries must safeguard their data and other vital assets. The main goals of this paper's systematic review, which covers the entire process of privacy protection and security, are to introduce cryptographic IS for Industry 5.0 (the Fifth Industrial Revolution) as a comprehensive solution that provides regulatory compliance and IS policies in addition to the industrial goals. The review covers the four main areas: (i) recognizing the need for frameworks to be developed for a secure Industry 5.0 lifecycle; (ii) emphasizing security guidelines, procedures, and countermeasures for Industry 5.0; (iii) applying control, access, and availability in real-time; and (iv) proposing a futuristic architecture for industrial information security. Furthermore, the analysis of previously published state-of-the-art techniques is presented in this paper. These techniques survive with various limitations and challenges, including intercommunication exchange, fine-grained control access, and interconnectivity-related issues, which affect the adoption of an IS in industrial programmes. At the end of this systematic review, we investigated a few open research problems and mentioned those that are involved in the design of cryptographic re-encryption-enabled IS for future Industry 5.0 developments.

INDEX TERMS Cryptography, Information Security, Industrial Internet of Things (IIoT), Industry 5.0, Blockchain, Hash Encryption

I. INTRODUCTION

In an industrial environment, Information Security (IS) is potentially involved in terms of protecting the information that would be preserved, processed, and shared in the interoperable connected nodes over the network [1], [2]. The concept is proposed to provide privacy in the information that is preserved or stored. In order to protect the information in the complete cycle of life, a program requires initializing the data security from where the data is generated to the final destination. Several innovations have been presented, which are mostly used for canceling, encrypting, and protecting information. In addition, each innovative technique has different types of uncovered mechanisms, such as hashing (SHA-128, SHA-256, SHA-512), Cryptographic Re-Encryption (NuCypher), Undetectable inks, and Steganography [2]-[4]. However, Cryptography is considered one of the most popular techniques to provide better information-protecting operations in the form of encryption (ciphertext) and decryption (plaintext) over the network [4], [5]. Unfortunately, these advances exhibited the uniqueness of information protection but did not hold the key constraints.

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 License. For more information, see https://creativecommons.org/licenses/by-nc-nd/4

This article has been accepted for publication in IEEE Access. This is the author's version which has not been fully edited and
content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2024.3351485

For instance, the list of techniques and their mechanisms is not always consistent, which means focusing on satisfactory security solutions. Not all mechanisms touch the level of users in almost every sort of safety problem, which is needed to accomplish the given objectives. Cryptography Re-Encryption (CRE, as mentioned in Table I) presents a mathematical-based algorithm that is designed to encrypt information in such a manner that no malicious attacker can be harmed [5], [6]. Due to this, the information remains protected in terms of covering the original text in ciphertext (a symbolic formation). Re-encryption mechanisms, especially the NuCypher Threshold Proxy, are normally utilized to secure restricted information (that is not to be polished) by creating various proxies so that the original information is protected in between the clones (Figure 1).

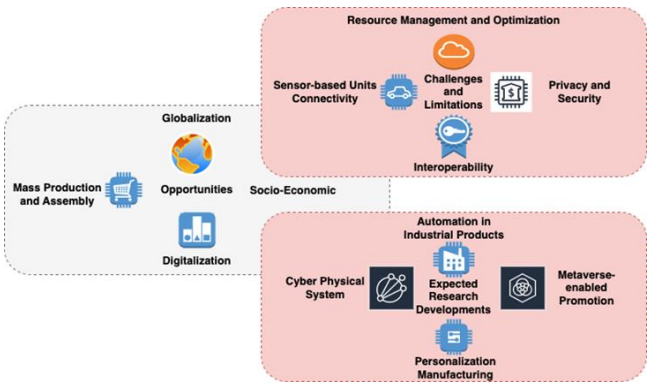


FIGURE 1. Current Scenario of the Industry 5.0.

TABLE I
DESCRIPTION OF ABBREVIATIONS

Abbreviation	Details
IS	Information Security
Industry 5.0	Fifth Industrial Revolution
ICT	Information and Communication Technology
SHA-128, SHA-256, SHA-512	Hashing Encryption
CRE	Cryptographic Re-Encryption
BDLT	Blockchain-Distributed Ledger Technology
EC	Elliptic Curve
RSA	Rivest, Shamir, and Adleman
ID	Intrusion Detection
IDS	Intrusion Detection System
Industry 4.0	Fourth Industrial Revolution
CC	Cloud Computing
CPSs	Cyber-Physical Systems
IoT	Internet of Things
AR	Augmented Reality
BCI	Brain-Computer Interaction
ICS	Industrial Control Systems
P2P	Peer-to-Peer
PRE	Proxy Re-Encryption
SMEs	Small and medium-sized Enterprises

In the recent environment, the term cryptography precipitates the data travels in such a manner that allows statistics to be stored secretly [7], [8]. The foundational bearing of modern cryptography is to split the long information into pieces and protect it through the conversion of encryption algorithms. In order to maintain secret communication, a public key is shared with the participants, who are authorized to interact and exchange information with each other in the designed system via the network connection. Almost a decade ago, the experts proposed a concept of single-type cryptography, which means an only algorithm solves data hiding and privacy-related problems that can exist for a long time and can be used for effective data security and preservation protection [8]-[10]. Behind all these, the experts realize that changing the prospect of information hiding involves steganographic embedding techniques. Instead, single-type cryptography is against being used for information transmission over the Internet. Based on this scenario, the cryptographic technique later shares the secret key concept while exchanging information in the network globe [10], [11].

On the other hand, the efficient maintenance of such cryptographic algorithms impacts the resolution of resource management in terms of extraordinary effects, such as computational power and memory. The Elliptic Curve (EC) and Rivest, Shamir, and Adleman (RSA) schemes are popular examples that ensure information security by enabling cryptographic encryption, means to convert information into cipher using an Asymmetric key technique [12]. In order to handle cipher conversions, a dynamic memory with scalability capability is required.

To implement a secure Industry 5.0 platform, it is worth noting that this environment is completely efficient and effective in terms of resource management. Recently, most cryptographic algorithms use an increased length of key encryption, which is still prone to malicious attackers, but such advancement requires more computing power [10]-[12]. Instead, these classical cryptographic algorithms have key length capability, but there is a need to transform it. The major aim of such algorithms is to be modernized in a manner that compensates for the classical one without key length increment, such as computational and storage-related resource management.

However, the list of intrusions is separate from those currently involved aspects that occur in Industry 4.0. The objective of Intrusion Detection (ID) applications is to monitor the overall network environment for analysis of suspicious activities and send alerts to the administrator. It allows information to be transferred within the inter-connected units and explicit enterprises in a robust, safe, and trusted manner. In addition, it is considered to be the upgraded version of antivirus, firewall, and other encryption-related aspects. According to the survey of Cyber Defense Magazine, more than 42% of cyberattacks are targeted at small and medium-sized enterprises, which affects approximately a value of $2.6 million [12]-[14]. It is a remarkable factor that needs to be addressed while designing new paradigms in the Industrial environment. Various intrusion detection systems are proposed that provide a dynamic monitoring hierarchy and

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 License. For more information, see https://creativecommons.org/licenses/by-nc-nd/4

This article has been accepted for publication in IEEE Access. This is the author's version which has not been fully edited and
content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2024.3351485

smart alerts, such as Snort, Bro, Sagan, McAfee, and Suricata [13], [14]. Another prospect of this research is to systematically investigate the existing processes and performance lifecycle [15], [16] and address a lack that has constantly slowed down advancement in the past few years. In order to improve the current lifecycle and related hierarchy, we need to consider these mentioned prospects in the development of secure Industry 5.0 applications as follows: (i) interoperable connectivity between industrial units and its security, (ii) highlights security procedures, guidelines, and countermeasures for Industry 5.0, (iii) applies control, access, and available in the real-time, and (iv) a futuristic industrial information security and connective units' channels.

In this paper, we present the description of the cryptographic role in IS for Industry 5.0, along with a recent gap involved in the technology and challenges issues that require experts' consideration for future perspective. In addition, this paper introduces a modern way to transform classical cryptographic algorithms, especially RSA and EC. Furthermore, a systematic investigation is presented on the fine-tuned and state-of-the-art intrusion detection systems that were recently proposed in a previous work, where all have a unique design to handle threats and provide countermeasures in terms of sending alerts and many others. The paper also systematically analyzes the process of current sharing and exchanging data between the industrial, manufacturing, and production units and is with the interoperable platforms for globalization and productivity. The major contributions of this systematic review are mentioned as follows:

- A broad dimension of cryptographic information security is covered in this paper, which systematically presents current developments, challenges, and limitations, as well as open research gaps for future points of view.
- This paper highlights what kind of level of security applies to the existing systems using classic cryptographic methods.
- The impact of malicious attacks and their investigations that occur in the network environment is mentioned.
- Along with that, the list of intrusion detection applications developed recently for securing communication is discussed in this study.
- In this paper, we propose a novel lifecycle for a secure Industry 5.0 framework that addresses the interoperable connectivity between industrial units and their security, highlights the security procedures and guidelines, and countermeasures for Industry 5.0, applies control, access, and available in real-time, and a futuristic industrial information security and connective units' channels.
- Finally, this paper highlights a list of open research issues, along with possible solutions that are required for the future development of Industry 5.0.

The rest of this systematic review is structured and organized as follows: In Section 2, the detailed discussion of current developments in IS and their importance in driving new paradigms in Industry 5.0 is highlighted. A list of cryptographic techniques is separated for the sake of securing existing as well as futuristic industrial environments in Section 3. Applicational utilization of cryptographic re-encryption mechanisms is discussed in Section 4. In Section 5, various open problems are listed that need more consideration for technological maturity in accordance with future prospects. Finally, this systematic review ends with the statement of conclusion and future direction in Section 6.

II. INFORMATION SECURITY AND INDUSTRY 5.0

The official introduction of the Fourth Industrial Revolution (Industry 4.0) means the robust involvement of Cloud Computing (CC) and Cyber-Physical Systems (CPSs) in industrial environments, such as transactional, manufacturing, and production-related units. Now, with the recent advances yet to launch the next industrial revolution, the major goal is to put the human back in the middle of industrial processes, which means transforming the human afford into machine-enabling cognitive intelligence that is now overwhelmingly digitalized [17], [18]. The factory-enabled units are connected and have been designed to enlarge and maximize production, but simultaneously, they have received enormous attacks because of the proposed surface, thus raising enormous privacy protection and security issues. It includes malware, spoofing, sniffing, ransomware, and other active malicious attacks that occur most probably on manufacturing units. However, the increment in the number of machine generation and growing rate of node connectivity in the network, especially Internet of Things (IoT) integrations, impacts the current setup of potential privacy protection and security; it is due to the increasing order of augmented reality (AR) connectivity of and brain-computer interaction-enabled interfaces.

According to the report of US Cyber Security and Digital Forensics Magazine, a total of 800+ manufacturing units of different industries were attacked by malicious in the last year [16]-[18]. On the other hand, more than 7,000 vulnerability detections are reported by the monitoring departments of these industries. It is worth noting that such issues are critical and should be tackled. Two critical scenarios that address the limitations under consideration for Industry Security 5.0 are separated as follows: (i) revamping and (ii) collaborative approach. In revamping, the production chain needs to be updated in such a manner that equips IS features itself, including the installation of the firewall for segment flow controls in accordance with the policies defined by the industry. This kind of extensibility makes the system more flexible and reliable in terms of providing transparency by avoiding risk while data is transmitted. In a collaborative approach, the system is more capable of covering security needs, such as information and cyber-related ones, by enabling the evaluation of operational constraints and analytics to investigate the compromising factors raised and mitigate them

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 License. For more information, see https://creativecommons.org/licenses/by-nc-nd/4

This article has been accepted for publication in IEEE Access. This is the author's version which has not been fully edited and
content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2024.3351485

by satisfying both the cyber and information security constraints.

A. INTEROPERABLE CONNECTIVITY BETWEEN INDUSTRIAL UNITS AND PROTECTION

The major risk in the industrial environment while connecting manufacturing units of Industry 5.0 is interoperability; due to the vast growth of interconnectivity, such as the IoT devices integration, collaboration of augmented reality headsets, and BCI interfaces require a number of security patches for the sake of efficient and effective machine operations and delivery [19], [20]. It is estimated that the rate of malicious attacks will rise to more than 25% in 2022 compared to previous years due to platform interoperability and the interconnectivity of their implicit and explicit units. In the current situation, the industry faces ransomware-based attacks, which is considered a prevalent cyber-attack that affects nearly all subsectors that connect. It is one of the higher frequency attacks that target manufacturing automobile automation and deliverance.

On the other hand, the large number of malicious attack attempts over the Industrial Control Systems (ICS) will increase up to 40% in 2022 and is expected to increase in 2023-2024 [18]-[20]. This paper investigates, evaluates, and highlights the list of most utilized information leakages, threats, and attack strategies that occur in the cyber environment for impact industrial operations as follows:

- Expended attacks on industrial surface
- Supply chain vulnerability
- IoT device security breaches
- Confidential information leakage
- Human-machine interaction-based engineering attacks

Here, Table II presents a detailed argument on the existing privacy and security procedures applied in the industrial units, especially manufacturing and production. This table elaborates on the role of classical cryptography and updated architecture in providing architectural protection and digitalization. The metrics of this systematic analysis are as follows: (i) list of scenarios discussed on the topic of IS for Industry 5.0, (ii) lack of privacy and security, (iii) possible solution presentation, (iv) open research issues, and (v) architectural update and requirement related discussion.

TABLE II
SYSTEMATIC ANALYSIS (I)

References	List of Scenario Discussion on IS for Industry 5.0	Lack of Privacy Protection and Preservation Discussion	Possible Solutions for Privacy Protection and Preservation Discussion	Available Opportunity (Year 2021-2023)	Classical Cryptographic Architectural Updates and Requirements	Major Discussions Available (Year 2021-2023)
M. Sharma et al. [21]	U	Y	N	✓	Addressed, but partially discussed.	✓
S. Deshpande et al. [22]	Y	N	Y	N/A	Need to be addressed.	N/A
M. Sverko et al. [23]	Y	Y	U	✓	Need to be addressed.	N/A
T. Nguyen et al. [24]	N	U	U	N/A	Addressed but partially discussed.	✓
S. Chawla et al. [25]	U	Y	U	✓	Need to be addressed.	✓
A. Massaro et al. [26]	Y	U	Y	N/A	Addressed, but partially discussed.	N/A
B. Bajic et al. [27]	Y	Y	Y	✓	Need to be addressed.	✓
H. Chi et al. [28]	Y	Y	U	✓	Addressed, but partially discussed.	✓

Where N = No discussion, Y = Provides in-depth details, and U = Discusses partially.

B. THE ROLE OF BLOCKCHAIN TECHNOLOGY

In industrial domains, the techniques of privacy preservation require a set of re-ductions by means of resource consumption. At the same time, data sharing and exchange, and thus, AI-driven intelligent models, would not be efficient enough to customize the property that is used as explicit information and would be converted for privacy [29]-[31]. So, a personalized optimal tradeoff of privacy and security is potentially required. However, the current protocols of privacy protections are insufficient in terms of the anomalous behavior of sensor-based nodes, which is not taken into account. For instance, if we consider the requirement of Industry 5.0, a trusted environment for information sharing is the key prospect, where the system ensures the collaboration of autonomous network management and node heterogeneity. Investigating all such scenarios, we find Blockchain is one of the potential solutions that provide integrity and transparency while information is transmitted in the heterogeneous node environment [32], [33], as shown in Figure 2. It ensures the industrial processing data and their ledger organization in a smooth manner, such as providing optimization, control, and management, as shown in Figure 2. The nature of ledger immutability in Blockchain solves the problem of dynamic process recording, log preservation, transaction details, tracking assets, and overall traceability via a Peer-to-Peer (P2P) consortium network.

Blockchain technology is considered a reliable solution to building industrial infrastructure because it provides a trusted view architecture that helps maintain an audit trail and related

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 License. For more information, see https://creativecommons.org/licenses/by-nc-nd/4

This article has been accepted for publication in IEEE Access. This is the author's version which has not been fully edited and
content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2024.3351485

regulatory compliances [33], [34]. It is the nature of Blockchain that it transforms information ledger into a regularly accumulated hierarchy based on chronological order with a chain-like structure. These information sequences are encrypted with a hash encryption mechanism called block header, which probably uses SHA-256 and can be an advanced version. Due to this advance, there is no possibility of changing the transaction if it is added to the ledger, even if it is scheduled. Suppose a particular stakeholder wants to revert their transactions or appeal to modify. In that case, the vote of participating stakeholders in the chain is countable in accordance with the policy of consensus. All such automation in this distributed environment is managed by smart contracts (chain code), a programable code that is intelligent enough to schedule, organize, manage, and optimize transactions, along with the capability to verify and validate the requests of stakeholders.

Table III presents the major components that have revolutionized the impact of blockchain technology on information security. The metric of comparison is mentioned as follows: (i) consensus protocols, (ii) decentralization, (iii) IoT protection, (iv) transactional processor, (v) identity and access management, (vi) faster settlement, (vii) consortium network, (viii) transaction scheduling, (ix) resource monitoring and management, (x) Hyperledger technology, (xi) trustworthiness, (xii) distributed ledger management and optimization, and (xiii) logs of verification and validation processes.

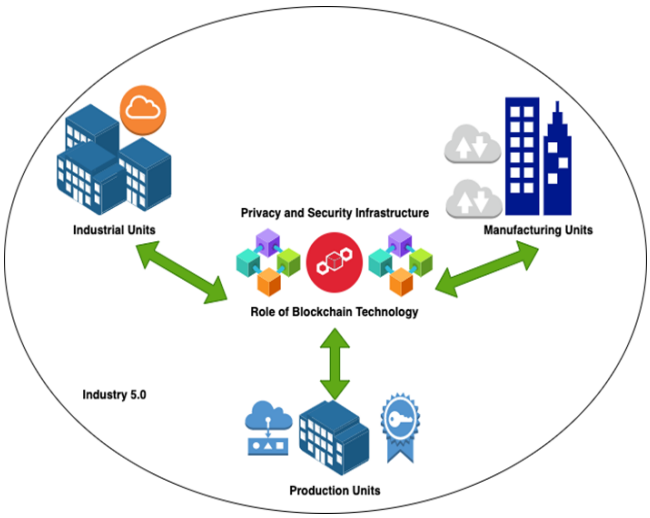


FIGURE 2. Hierarchy of Blockchain in Industry 5.0.

TABLE III
COMPONENTS OF THE REVOLUTIONIZE BLOCKCHAIN IN INFORMATION SECURITY – COMPARATIVE ANALYSIS

Categories	Years										Proposed Systematic Review
	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023	
	References										
	S. Wilkinson et al. [35]	A. Kiayias et al. [36]	S. Singh et al. [37]	H. Hou [38]	L. Liu et al. [39]	A. Gupta et al. [40]	A. Faruk et al. [41]	D. Berdik et al. [42]	B. Yang [43], X. Chan et al. [44]	Y. Zhao et al. [45], Z. Wenhua et al. [46], E.R.D. Villarreal et al. [47]	2023-2024
Consensus Protocols	✓				✓		✓		✓	✓	✓
Decentralization		✓		✓		✓		✓			✓
IoT Protection	✓	✓		✓			✓	✓	✓		✓
Transactional Processor			✓	✓		✓	✓			✓	✓
Identity and Access Management	✓		✓	✓		✓		✓			✓
Faster Settlement		✓			✓		✓	✓	✓	✓	✓
Consortium Network									✓	✓	✓
Transaction Scheduling			✓	✓		✓	✓		✓		✓
Resource Monitoring and Management		✓			✓			✓		✓	✓
Hyperledger Technology			✓		✓		✓		✓		✓
Trustworthiness	✓	✓		✓		✓		✓	✓	✓	✓
Distributed Ledger Management and Optimization										✓	✓
Logs of Verification and Validation Processes		✓	✓		✓	✓		✓		✓	✓

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 License. For more information, see https://creativecommons.org/licenses/by-nc-nd/4

This article has been accepted for publication in IEEE Access. This is the author's version which has not been fully edited and
content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2024.3351485

III. CRYPTOGRAPHIC ALGORITHMS FOR SECURING THE ENVIRONMENT OF INDUSTRY 5.0

Various cryptographic algorithms come naturally by means that are out of use in different domains, for example, the technique of secure electronic commerce, digital signature, and steganographic-based hiding information over insecure networks [48], [49]. In addition, it is evaluated that the RSA cryptographic algorithms are one of the most successfully designed, which solves integer factorization and manufactories' privacy protection and security. However, cryptography is placed in Industry 5.0 for securing the environment, where the major perspective is to detect criminal activities and allow systems to transmit illicit information without interception [49]-[51]. Most cryptographic algorithms use public key cryptosystem strategy, especially EC and RSA, which are most promptly used for securing information transmission protocols.

There are a number of well-known techniques proposed previously for information prevention in the industrial sectors, but most of the classical ones creaked; the list of creaked versions is as follows:

- Data Encryption Standard (DES)
- Rivest Cipher 4 (RC4)
- Message-Digest Algorithm (MD5)
- Secure Hash Algorithm 1 (SHA-1)

Other than that, many prominent algorithms are still used for preventing information of industrial things, such as Triple, Blowfish, Random number generators, Homomorphic encryption, Key confirmation, and Quantum cryptography [52]-[54]. These mentioned classical algorithms are not only used for protecting information but also for maintaining such logs in an organized manner while converting them into cipher. The technological advancement in cryptography is discussed in the subsection as follows:

A. RE-ENCRYPTION AND POLICIES

A method of encryption uses mathematical formulas to convert plaintext to ciphertext; not only this, but the algorithms of cryptographic encryption also aim to provide data integrity and confidentiality in a computing environment [55]. In order to maintain such privacy protection, the algorithms share encrypted keys for the sake of converting while it receives to another end. The key is designed to convert ciphertext into plaintext, which is then transmitted over the Internet and vice versa due to decrypting it on the receiver side. Most of the cryptographic encryption algorithms are used in digital marketing, commercial electronic commerce, entrepreneurship, online banking transactions, and small and medium-sized enterprises' ledger security. As we already mentioned in the list of algorithms above, the description of such schemes is as follows [55]-[57]: (i) Most of the cryptographic algorithms work on blocks, which means a block of ciphertext encrypts and decrypts as plaintext accordingly at a single time, and (ii) value encoding is done with a stream cipher of multi-characters conversion, which is completed in a single operation.

However, Symmetric and Asymmetric algorithms are separated in accordance with the operation they perform [58], [59]. An algorithm that uses the same key for managing encryption and decryption is counted as a Symmetric algorithm, where an algorithm uses two different keys simultaneously when data encrypts and decrypts, then it can be calculated as an Asymmetric algorithm. More than that, both categories use a message authentication code mechanism to ensure information confidentiality and integrity. Undoubtedly, these techniques help provide information security and related protection, but it is considered a classical algorithm due to consuming more resources, especially in terms of the cost of computation.

On the other side, a re-encryption mechanism has been proposed recently, which is now part of cryptography, most probably the algorithm of Proxy Re-Encryption (PRE) [60], [61]. The design of this newly adopted technology allows a proxy to transform into a ciphertext under the rule of encryption, which is to convert one key into an encryption of the same information with several other proxy generations, as shown in Figure 3. The main purpose is to create trust between the senders while revealing some of the information (a fake proxy) as a part of the proxy to allow the performance of PRE for translations. During very small discussions, the proxy cannot learn the keys of the participating stakeholders, and the information of this encrypted shell remains untouchable. By comparing this algorithm with the classical one, the experts receive prominent results in terms of resource consumption, information management, and optimization.

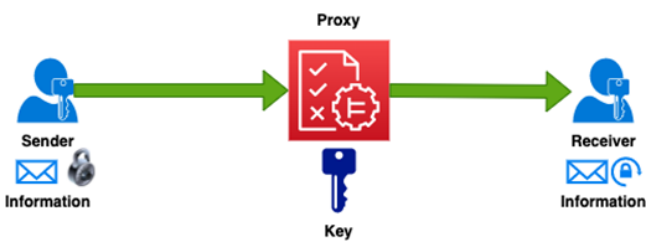


FIGURE 3. Working operation of Proxy Pre-Re-Encryption.

B. PROCEDURES, GUIDELINES, AND COUNTERMEASURES

It is critical to emphasize that Industry 5.0 is going to replace Industry 4.0, which will extend the strength that can help more enterprises in terms of getting a more agile environment and future proofs [62]. The advent of Industry 5.0 will change the net-working scenario in terms of enhancing collaborative strategies to the overall connective value chain. It also includes a close connection mechanism by creating node-to-node partnerships, such as supplies, sales, and purchases. However, the crucial aspect of this proposed technology is to address the revolution of data generation and its prevention, which must be strongly estimated and guaranteed in the landscape of this

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 License. For more information, see https://creativecommons.org/licenses/by-nc-nd/4

This article has been accepted for publication in IEEE Access. This is the author's version which has not been fully edited and
content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2024.3351485

new technological involvement. The development of Industry 5.0 offers SMEs, even all industrial units, enormous opportunities to remain unsuccessful; however, the major prospect is to transform the current scenario in the digitized world and tap into a new forum [62]-[65].

The list of cryptographic encryption procedures, guidelines, and countermeasures in the domain of IS are discussed as follows [62]-[65]:

- Artificial Intelligence Involvement: One of the reasons behind this innovation is to reduce the complementing human labor-enabled manual involvement and improve the decision-making hierarchy in SMEs. In order to replace this, three types of techniques are proposed: supervised, unsupervised, and semi-supervised. However, let us talk about performance by means of efficiency in the industrial environment. The self-learning algorithm plays a significant role in terms of optimizing the production cycle and improving quality. Another reason is to use this technology to maintain the predictive processes, which impact the hierarchy of proactive maintenance of equipment and machinery.
- Intelligence and Smart-based System Automation: It is a vital topic discussed in Industry 4.0, but it is time to transform their protocols by enabling connected systems and robotics to convert manual procedures into automated ones. Due to such developments, the collaborative strategy of AI is used, and a machine learning algorithm, especially an Artificial Neural Network, is utilized to enhance the quality of products and monitor the overall setup and production process in terms of optimization through automation. By the impact of this, the systems can reduce the computing time and cost of resource usage.
- Sensors Connectivity and Production: Automation plays a significant role, but sensory connectivity is a must to help robots connect with a distributed network environment. The major aim of these connected sensors (such as ESP32 and DHT11) is to manage production processes, organize data entries, and optimize, which can be used to achieve secure and efficient automation procedures. The security of these mentioned sensors is a critical task, and maintenance of this problem is a necessary point that can be possible by using cryptographic algorithms, as discussed above.

Table 4 presents a detailed argument on the procedures, guidelines, and countermeasures proposed in the recent IS environment using cryptography encryption mechanisms for industrial units. This table explains the role of cryptographic techniques utilized for securing the environment of Industrial Things, especially Industry 5.0. The metrics of this systematic analysis are as follows: (i) list of scenarios discussed on IS guidelines, (ii) lack of countermeasure discussion, (iii) possible solution of procedural and countermeasures of IS, (iv) gap analysis discussion, and (v) modernized cryptographic architecture and requirement related discussion.

TABLE IV
SYSTEMATIC ANALYSIS (II)

References	List of Scenario Discussion on IS for Industry 5.0	Lack of Privacy Protection and Preservation Discussion	Possible Solutions for Privacy Protection and Preservation Discussion	Available Opportunity (Year 2021-2023)	Classical Cryptographic Architectural Updates and Requirements	Major Discussions Available (Year 2021-2023)
K Singh et al. [66]	U	Y	N	✓	Addressed, but partially discussed.	✓
R. Bhaskaran et al. [67]	N	Y	N	N/A	Addressed, but partially discussed.	✓
D. Kumar et al. [68]	U	U	Y	N/A	Addressed, but partially discussed.	✓
M. Yadav et al. [69]	Y	U	N	N/A	Need to be addressed.	N/A
V. Gangwar et al. [70]	U	Y	U	✓	Need to be addressed.	N/A
P. Patel et al. [71]	N	U	U	✓	Need to be addressed.	✓
S. Sekhar et al. [72]	Y	U	U	✓	Need to be addressed.	N/A
M. Iqbal et al. [73]	N	U	Y	✓	Need to be addressed.	✓

Where N = No discussion, Y = Provides in-depth details, and U = Discusses partially

IV. APPLICATIONS OF CRYPTOGRAPHIC RE-ENCRYPTION FOR INDUSTRIAL THINGS

In this context, the paper discusses the most obvious use of cryptography encryption mechanism in IS for industrial environments, most of the frequent use of encryption in intercommunication, which is designed between the users and centralized servers [74], [75]. Email is one of the biggest examples of applicational cryptography, such as the Gmail App, where the email is sent user-to-user, server-to-server, and server-to-user. In this scenario, the email is encrypted. The strategy of end-to-end encryption, such as PGP, is designed to prove a truly secure information transmission system between sender and receiver only. It means there is no administrative involvement as well.

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 License. For more information, see https://creativecommons.org/licenses/by-nc-nd/4

This article has been accepted for publication in IEEE Access. This is the author's version which has not been fully edited and
content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2024.3351485

On the other hand, BitLocker Desktop UCL is another type of cryptography encryption solution, where the user logging in to the system is derived from accessing data that is completely secure. In addition, other drive data can be read if the stakeholders restrict it. No such data can be accessed without prior permission [76]-[78].

However, the use of hashing can change the perspective of classical encryption and produce relatively useless symbolic notations for malicious attackers [77]. When a system requires login, a password will be taken from the system if the hash is the same, then compared to the preserved hash value and allowed; otherwise, block it [77], [78], as shown in Figure 4. It is quite a good applicational solution, where at no point does the system fail in terms of attacks from the malicious site or has access to the data without a password.

The list of popular applications running in the recent environment for providing security to Industrial Things using cryptographic re-encryption mechanisms is mentioned as follows [76]-[78]:

- Mailfence
- Xx messenger
- Blockchain.com

Table 5 presents a detailed argument on the current applications designed for industrial things using cryptographic re-encryption algorithms, such as NuCypher Threshold Proxy Re-Encryption. This table defines the role of modernized cryptography and the discussion of architectural changes, along with the procedural changes that occur throughout. The metrics of this systematic analysis are as follows: (i) list of applicational discussion on the topic of cryptography re-encryption, (ii) lack of discussion on industrial things, (iii) discussion on a possible solution in procedural cryptography, (iv) available opportunities, and (v) modernized cryptography application related discussion.

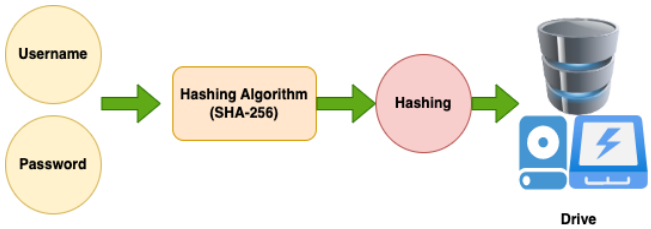


FIGURE 4. Verification and Validation Operations of Hashing Algorithms.

Table 5 presents a detailed argument on the current applications designed for industrial things using cryptographic re-encryption algorithms, such as NuCypher Threshold Proxy Re-Encryption. This table defines the role of modernized cryptography and the discussion of architectural changes, along with the procedural changes that occur throughout. The metrics of this systematic analysis are as follows: (i) list of applicational discussion on the topic of cryptography re-encryption, (ii) lack of discussion on industrial things, (iii) discussion on a possible solution in procedural cryptography, (iv) available opportunities, and (v) modernized cryptography application related discussion.

TABLE V
SYSTEMATIC ANALYSIS (III)

References	List of Scenario Discussion on IS for Industry 5.0	Lack of Privacy Protection and Preservation Discussion	Possible Solutions for Privacy Protection and Preservation Discussion	Available Opportunity (Year 2021-2023)	Classical Cryptographic Architectural Updates and Requirements	Major Discussions Available (Year 2021-2023)
A. Mazumder et al. [83]	Y	N	U	✓	Addressed, but partially discussed.	N/A
M. Ferrag et al. [84]	N	Y	U	N/A	Addressed, but partially discussed.	✓
D. Sudharson et al. [85]	Y	U	N	✓	Addressed, but partially discussed.	✓
Y. Skorenkyya et al. [86]	Y	U	U	✓	Need to be addressed.	N/A
B. Roy et al. [87]	Y	U	N	✓	Need to be addressed.	N/A
L. Espina-Romero et al. [88]	U	N	U	N/A	Need to be addressed.	✓
R. Sharma et al. [89]	Y	U	Y	N/A	Need to be addressed.	✓
P. Muthuswamy et al. [90]	Y	U	N	✓	Need to be addressed.	N/A

Where N = No discussion, Y = Provides in-depth details, and U = Discusses partially.

A. PREVIOUSLY PUBLISHED STATE-OF-THE-ART EVALUATION AND DISCUSSION

This section discusses the prominent results and uniqueness of state-of-the-art cryptographic algorithms in IS for Industry 5.0. In the evaluation, this paper distributes the number of articles in accordance with the classical and modernized use of cryptographic algorithms for securing the environment of industrial things [91]-[95]. The metric of algorithmic analysis

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 License. For more information, see https://creativecommons.org/licenses/by-nc-nd/4

This article has been accepted for publication in IEEE Access. This is the author's version which has not been fully edited and
content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2024.3351485

is as follows: (i) fluctuation in resource usage, (ii) encryption time, (iii) decryption time, (iv) overall accuracy, and (v) efficiency of the algorithm. However, the total number of algorithms used in this evaluation is defined as follows [91-95]: (i) RSA, (ii) EC, (iii) PRE, (iv) AES, (v) SHA-256, and (vi) quantum cryptography. The detailed evaluation of these mentioned state-of-the-art crypto-graphic algorithms in IS for Industry 5.0 is as follows (as mentioned in Tables 6 and 7):

TABLE VI
SYSTEMATIC EVALUATION OF STATE-OF-THE-ART MODERNIZED CRYPTOGRAPHIC ALGORITHMS IN IS FOR INDUSTRY 5.0 (1)

Evaluation Metric	RSA	EC	Proxy Re-Encryption (PRE)	Overall (%)
Fluctuation in Resource Usage	17.3%	19.7%	13.6%	2.1%
Encryption Time	15.1%	17.5%	11.33%	3.6%
Decryption Time	13.8%	15.7%	9.11%	3.3%
Accuracy	11.7%	13.81%	7.13%	1.9%
Efficiency	12.2%	14.54%	10.59%	2.9%

TABLE VII
EVALUATION OF STATE-OF-THE-ART CLASSICAL CRYPTOGRAPHY COUNTERPART WHICH SUPPORTS IS FOR INDUSTRY 5.0 (2)

Evaluation Metric	AES	Hash-Encryption (SHA-256)	Quantum cryptography	Overall (%)
Fluctuation in Resource Usage	21.77%	19.13%	27.38%	3.55%
Encryption Time	19.97%	17.34%	23.79%	3.77%
Decryption Time	17.31%	15.78%	21.59%	2.21%
Accuracy	13.11%	11.96%	17.93%	1.93%
Efficiency	18.33%	11.33%	15.47%	2.89%

B. PROPOSED FUTURISTIC ARCHITECTURE FOR INDUSTRY 5.0

Figure 5 presents a proposed architecture that can be considered in the futuristics Industry 5.0 developments. It is derived from the collaborative perspective of Blockchain, AI, IIoT, and big data. The working operations of this proposed architecture are based on nine different sections. In the first (step 1), industry 5.0 connects with the production units to convert the raw material into a well-established product, as shown in Figure 5. On the other hand, in the second step (step 2), the processing unit starts filtering raw data in a useful manner while receiving it from the production units. All of it can connect with the communication network for managing overall transactions throughout, which is completely based on distributed in nature due to blockchain involvement. In this environment, two different channels are derived; one can design for the explicit transaction and related management while the other can deal with re-quests implicitly, as shown in Figure 5 (steps 3-4). The major objective of designing this type of communication is to analyze results as output, along with the fault tolerance, as highlighted in steps 5 and 6. However, all such activities can be handled by the expert of this proposed architecture, as shown in step 4.

In step 7, this architecture uses the capability of AI, especially machine learning-enabled algorithms, for the sake of maintaining a large set of data and its organization, along with management and optimization-related activities. The major algorithms utilized for these processes are Artificial Neural Network (ANN) and Support Vector Machine (SVM). This integration helps the smart manufacturing units to manage human-less decisions in real time, as mentioned in steps 8 and 9.

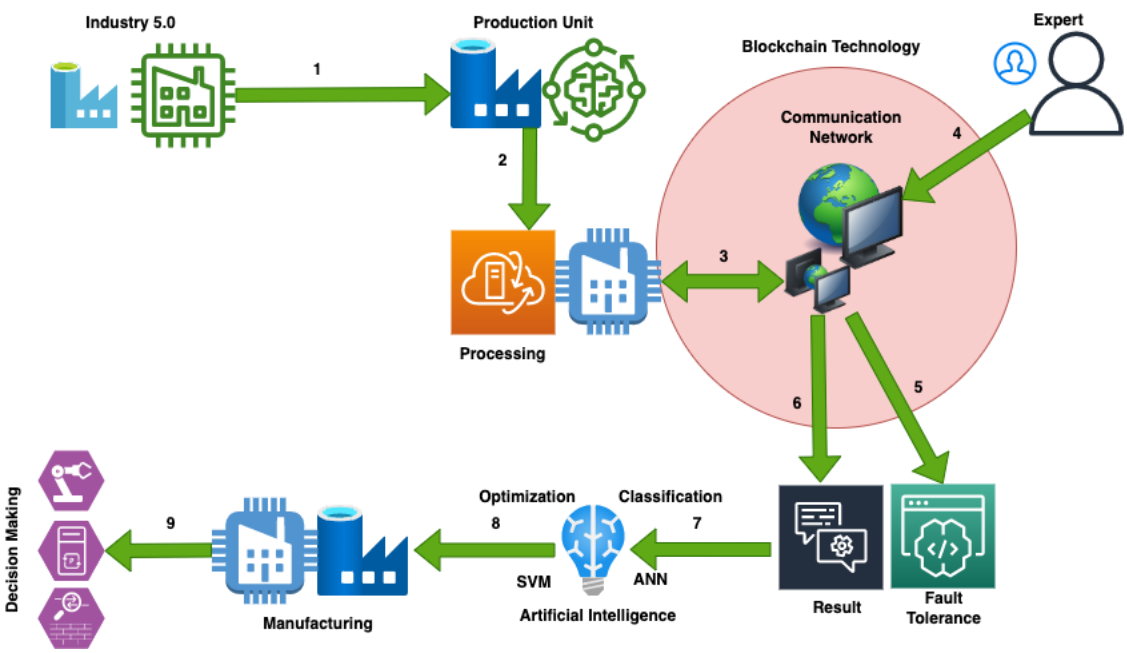


FIGURE 5. Proposed Futuristic Architecture for Secure Industry 5.0.

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 License. For more information, see https://creativecommons.org/licenses/by-nc-nd/4

This article has been accepted for publication in IEEE Access. This is the author's version which has not been fully edited and
content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2024.3351485

V. OPEN RESEARCH CHALLENGES AND LIMITATIONS

In this context, we separate the existing research gaps that are untouched, meaning yet unaddressed, which we find during the analysis of this systematic investigation. In addition, we present a few possible solutions, but these listed topics need experts' consideration for technological maturity and further developments.

A. INTRUSION, TRUSTWORTHINESS, AND MODERNIZATION

Trustworthiness presents a significant problem in the existing industrial environment. In centralization, a platform is totally based on vulnerability due to client-server architecture that causes the system to attack by means the malicious actor can exploit. It is worth noting that the need for a trusted hierarchy is mandatory that is yet to be involved in this infrastructure [96], [97]. The absence of a trusted environment in a trustless platform can make the ecosystem more challenging in terms of identifying and analyzing privacy-related breaches. In order to resolve such issues, the integration of blockchain and edge-enabling solutions with the NuCypher Threshold Proxy Re-Encryption mechanism is important because it removes the central authority to oversee the fewer computing transactions.

B. PREVIOUSLY PUBLISHED STATE-OF-THE-ART EVALUATION AND DISCUSSION

In recent times, Industrial IoT devices have generally been considered secure and protected, but it is worth noting that they are not as secure as the blockchain infrastructure [97], [98]. It is due to the weak interconnectivity between node-to-node, which makes them vulnerable and raises security breaches. The nature of such devices makes them compromised; on the other side, blockchain technology provides integrity throughout the entire network. Undoubtedly, the resource management and utilization of blockchain technology are high; in order to maintain this, the Hyperledger Indy is proposed for SMEs, where the architecture is well-tuned and perfectly matches the hierarchy of Industrial Things with the defined range of resource consumption.

C. SCOPE OF COMPUTING RESOURCE MANAGEMENT FOR INFORMATION SECURITY

The adoption of low-end Industrial IoT (IIoT) devices is critical in the environment due to its resource consumption limitations, such as computational energy, low latency and throughput, and storage [98], [99]. For this reason, such devices struggle to perform high-incentive tasks, resulting in slow transaction processing time can be received [100]. These types of challenging prospects limit the adaptation of Industry 5.0 in real time; in order to address this issue, this paper provides a possible solution by enabling the AI-driven architecture with blockchain technology, which ensures re-source optimization and protection at the same time. Due to such extensibility, the system maintains the legacy of industrial robustness that relies on low-end IIoT devices and achieves productivity.

D. FUTURISTIC INDUSTRIAL DEVELOPMENTS

The large amount of data generated from different devices connected with the industrial units presents a significant limitation for Industry 4.0, and the same can impact Industry 5.0 as well [101]-[103]. Scalability is the potential cause that creates a bottleneck in the adoption of low-end IIoT in Industry 5.0. In addition, a multi-protocol and related standardization affects the diverse range of industrial devices that could potentially impact the integration of a seamless consortium network hierarchy. It also causes the establishment of intercommunication, which provides ineffective collaboration between units. In order to solve these problems, a well-mannered CPS and Block-chain Hyperledger integration is required. Both technologies are capable of collaborating to resolve the current intercommunication hindrance, along with the solution of data scalability due to Blockchain Hyperledger using the facility of File coin (a distributed storage structure), a low-cost data preservation, organization, management, and optimization.

VI. CONCLUSION

The original focus of this work was on the potential difficulties and constraints associated with cryptographic re-encryption, as well as some potential solutions that are now necessary to construct robust IS. We examine the traditional cryptographic encryption methods, processes, plans, and procedures in the methodical analysis, which calls for higher computing power and dynamic memory. Therefore, since cryptographic encryption techniques cannot be replaced in their current state, they must be updated. Therefore, the modernization of cryptographic algorithms is a new paradigm that this study investigates. In this case, the encryption methods are updated by adjusting the cipher conversion parameters, particularly in RSA and EC. These changes impact resource utilization, which enhances the capability by means of increased privacy protection and security with a minimum cost of computation consumption while computing plain-to-cipher text and vice versa.

However, this article introduces the function of Blockchain Technology in elevating IS, as well as the security and protection of infrastructure for Industry 5.0. Applications like NuCypher Proxy Threshold Re-Encryption are among those that adhere to the cryptographic re-encryption technique. The cryptography family gains a new member who creates a proxy for the encryptions that hostile attacks are unable to track down because of fictitious duplications. Furthermore, for the sake of technological maturity and future advances, this study discusses a few potential answers to the important open research topics that need expert consideration.

REFERENCES

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 License. For more information, see https://creativecommons.org/licenses/by-nc-nd/4

This article has been accepted for publication in IEEE Access. This is the author's version which has not been fully edited and
content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2024.3351485

[1] Rani, S., & Srivastava, G. (2024). Secure hierarchical fog computing-based architecture for industry 5.0 using an attribute-based encryption scheme. Expert Systems with Applications, 235, 121180.

[2] Verma, A., Bhattacharya, P., Madhani, N., Trivedi, C., Bhushan, B., Tanwar, S., ... & Sharma, R. (2022). Blockchain for Industry 5.0: Vision, opportunities, key enablers, and future directions. Ieee Access, 10, 69160-69199.

[3] Khan, A. A., Laghari, A. A., Gadekallu, T. R., Shaikh, Z. A., Javed, A. R., Rashid, M., ... & Mikhaylov, A. (2022). A drone-based data management and optimization using metaheuristic algorithms and blockchain smart contracts in a secure fog environment. Computers and Electrical Engineering, 102, 108234.

[4] Leng, J., Chen, Z., Huang, Z., Zhu, X., Su, H., Lin, Z., & Zhang, D. (2022). Secure blockchain middleware for decentralized iiot towards industry 5.0: A review of architecture, enablers, challenges, and directions. Machines, 10(10), 858.

[5] Liu, R., Yu, X., Yuan, Y., & Ren, Y. (2023). BTDSI: A blockchain-based trusted data storage mechanism for Industry 5.0. Journal of King Saud University-Computer and Information Sciences, 35(8), 101674.

[6] Khan, A. A., Shaikh, A. A., Shaikh, Z. A., Laghari, A. A., & Karim, S. (2022). IPM-Model: AI and metaheuristic-enabled face recognition using image partial matching for multimedia forensics investigation with genetic algorithm. Multimedia Tools and Applications, 81(17), 23533-23549.

[7] Mahmood, K., Tariq, T., Sangaiah, A. K., Ghaffar, Z., Saleem, M. A., & Shamshad, S. (2023). A Neural Computing-based Access Control Protocol for AI-driven Intelligent Flying Vehicles in Industry 5.0-assisted Consumer Electronics. IEEE Transactions on Consumer Electronics.

[8] Khan, A. A., Laghari, A. A., Shaikh, Z. A., Dacko-Pikiewicz, Z., & Kot, S. (2022). Internet of Things (IoT) security with blockchain technology: A state-of-the-art review. IEEE Access.

[9] Rajabion, L. (2023). Industry 5.0 and Cyber Crime Security Threats. In Advanced Research and Real-World Applications of Industry 5.0 (pp. 66-76). IGI Global.

[10] Chander, B., Pal, S., De, D., & Buyya, R. (2022). Artificial intelligence-based Internet of Things for Industry 5.0. Artificial intelligence-based Internet of things systems, 3-45.

[11] Khan, A. A., Laghari, A. A., Li, P., Dootio, M. A., & Karim, S. (2023). The collaborative role of Blockchain, artificial intelligence, and industrial Internet of Things in the digitalization of small and medium-sized enterprises. Scientific Reports, 13(1), 1656.

[12] Guruswamy, S., Pojić, M., Subramanian, J., Mastilović, J., Sarang, S., Subbanagounder, A., ... & Jeoti, V. (2022). Toward better food security using concepts from Industry 5.0. Sensors, 22(21), 8377.

[13] Czeczot, G., Rojek, I., Mikołajewski, D., & Sangho, B. (2023). AI in IIoT Management of Cybersecurity for Industry 4.0 and Industry 5.0 Purposes. Electronics, 12(18), 3800.

[14] Khan, A. A., Laghari, A. A., Shafiq, M., Awan, S. A., & Gu, Z. (2022). Vehicle to everything (V2X) and edge computing: A secure lifecycle for UAV-assisted vehicle network and offloading with Blockchain. Drones, 6(12), 377.

[15] Maddikunta, P. K. R., Pham, Q. V., Prabadevi, B., Deepa, N., Dev, K., Gadekallu, T. R., ... & Liyanage, M. (2022). Industry 5.0: A survey on enabling technologies and potential applications. Journal of Industrial Information Integration, 26, 100257.

[16] Khan, A. A., Laghari, A. A., Shafiq, M., Cheikhrouhou, O., Alhakami, W., Hamam, H., & Shaikh, Z. A. (2022). Healthcare ledger management: A blockchain and machine learning-enabled novel and secure architecture for medical industry. Hum. Cent. Comput. Inf. Sci, 12, 55.

[17] Tyagi, A. K., Dananjayan, S., Agarwal, D., & Thariq Ahmed, H. F. (2023). Blockchain—Internet of Things Applications: Opportunities and Challenges for Industry 4.0 and Society 5.0. Sensors, 23(2), 947.

[18] Leng, J., Zhu, X., Huang, Z., Xu, K., Liu, Z., Liu, Q., & Chen, X. (2023). ManuChain II: Blockchained Smart Contract System as the Digital Twin of Decentralized Autonomous Manufacturing Toward Resilience in Industry 5.0. IEEE Transactions on Systems, Man, and Cybernetics: Systems.

[19] Kohli, P., Sharma, S., & Matta, P. (2022, December). Secured Privacy Preserving Techniques Analysis of 6G Driven Vehicular Communication Network in Industry 5.0 Internet-of-Everything (IoE) Applications. In 2022 International Conference on Smart Generation Computing, Communication and Networking (SMART GENCON) (pp. 1-8). IEEE.

[20] Yang, H., Asheralieva, A., Zhang, J., Karim, M. M., Niyato, D., & Raza, K. A. (2022, May). User-Centric Blockchain for Industry 5.0 Applications. In 2022 IEEE International Conference on Communications Workshops (ICC Workshops) (pp. 25-30). IEEE.

[21] Sharma, M., Sehrawat, R., Luthra, S., Daim, T., & Bakry, D. (2022). Moving towards industry 5.0 in the pharmaceutical manufacturing sector: challenges and solutions for Germany. IEEE Transactions on Engineering Management.

[22] Deshpande, S., & Jogdand, R. (2022). Development of IoT Middleware Broker Communication Architecture for Industrial Automation with Focus on Future Pandemic Possibilities: Industry 5.0. In Emerging Technologies in Data Mining and Information Security: Proceedings of IEMIS 2022, Volume 3 (pp. 47-58). Singapore: Springer Nature Singapore.

[23] Sverko, M., Grbac, T. G., & Mikuc, M. (2022). Scada systems with focus on continuous manufacturing and steel industry: A survey on architectures, standards, challenges and industry 5.0. IEEE Access, 10, 109395-109430.

[24] Nguyen, T., Tran, K. D., Raza, A., Nguyen, Q. T., Bui, H. M., & Tran, K. P. (2023). Wearable Technology for Smart Manufacturing in Industry 5.0. In Artificial Intelligence for Smart Manufacturing: Methods, Applications, and Challenges (pp. 225-254). Cham: Springer International Publishing.

[25] Chawla, S., & Mehta, K. (2023). Cryptocurrency Adoption in the Era of Industry 5.0: Opportunities, Challenges, and the Intellectual Landscape–SLR and Bibliometric Analysis. Opportunities and Challenges of Business 5.0 in Emerging Markets, 240-262.

[26] Massaro, A. (2023). Advanced Electronic and Optoelectronic Sensors, Applications, Modelling and Industry 5.0 Perspectives. Applied Sciences, 13(7), 4582.

[27] Bajic, B., Medojevic, M., Simeunovic, N., & Rikalovic, A. DIGITAL KAIZEN: OPPORTUNITIES AND CHALLENGES IN INDUSTRY 5.0.

[28] Chi, H. R., Radwan, A., Huang, N. F., & Tsang, K. F. (2022). Guest Editorial: Next-Generation Network Automation for Industrial Internet-of-Things in Industry 5.0. IEEE Transactions on Industrial Informatics, 19(2), 2062-2064.

[29] Joglekar, S., Kadam, S., & Dharmadhikari, S. (2023). Industry 5.0: Analysis, Applications And Prognosis. The Online Journal of Distance Education and e-Learning, 11(1), 1.

[30] Ramachandran, K. K., Nagarjuna, B., Akram, S. V., Bhalani, J., Raju, A. M., & Ponnusamy, R. (2023, January). Innovative Cyber Security Solutions Built on Blockchain Technology for Industrial 5.0 Applications. In 2023 International Conference on Artificial Intelligence and Smart Communication (AISC) (pp. 643-650). IEEE.

[31] Ray, S., Korchagina, E. V., Nikam, R. U., & Singhal, R. K. (2023). A Blockchain-based Secure Healthcare Solution for Poverty-led Economy of IoMT Under Industry 5.0. In Inclusive Developments Through Socio-economic Indicators: New Theoretical and Empirical Insights (pp. 269-280). Emerald Publishing Limited.

[32] Zizic, M. C., Mladineo, M., Gjeldum, N., & Celent, L. (2022). From Industry 4.0 towards Industry 5.0: A Review and Analysis of Paradigm Shift for the People, Organization and Technology. Energies 2022, 15, 5221. Industry 4.0—from Smart Factory to Cognitive Cyberphysical Production System and Cloud Manufacturing, 1.

[33] Lykov, D., & Razumowsky, A. (2023). Industry 5.0 and human capital. In E3S Web of Conferences (Vol. 376). EDP Sciences.

[34] Zhang, C., Wang, Z., Zhou, G., Chang, F., Ma, D., Jing, Y., ... & Zhao, D. (2023). Towards new-generation human-centric smart manufacturing in Industry 5.0: A systematic review. Advanced Engineering Informatics, 57, 102121.

[35] Wilkinson, S., Lowry, J., & Boshevski, T. (2014). Metadisk: A blockchain-based decentralized file storage application. Storj Labs Inc., Technical Report, hal, 1(11).

[36] Kiayias, A., & Panagiotakos, G. (2015). Speed-security tradeoffs in blockchain protocols. Cryptology ePrint Archive.

[37] Singh, S., & Singh, N. (2016). Blockchain: Future of financial and cyber security. *2016 2nd International Conference on Contemporary*

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 License. For more information, see https://creativecommons.org/licenses/by-nc-nd/4

This article has been accepted for publication in IEEE Access. This is the author's version which has not been fully edited and
content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2024.3351485

Computing and Informatics (IC3I), Greater Noida, India, 2016, pp. 463-467, doi: 10.1109/IC3I.2016.7918009.

[38] Hou, H. (2017, July). The application of blockchain technology in E-government in China. In 2017, the 26th International Conference on Computer Communication and Networks (ICCCN) (pp. 1-4). IEEE.

[39] Liu, L., & Xu, B. (2018, April). Research on information security technology based on Blockchain. In 2018 IEEE 3rd international conference on cloud computing and big data analysis (ICCCBDA) (pp. 380-384). IEEE.

[40] Gupta, A., Siddiqui, S. T., Alam, S., & Shuaib, M. (2019). Cloud computing security using Blockchain. Journal of Emerging Technologies and Innovative Research (JETIR), 6(6), 791-794.

[41] Farouk, A., Alahmadi, A., Ghose, S., & Mashatan, A. (2020). Blockchain platform for industrial healthcare: Vision and future opportunities. Computer Communications, 154, 223-235.

[42] Berdik, D., Otoum, S., Schmidt, N., Porter, D., & Jararweh, Y. (2021). A survey on Blockchain for information systems management and security. Information Processing & Management, 58(1), 102397.

[43] Yang, B. (2022). Prevention of business risks of internet information security platforms based on blockchain technology. Computational Intelligence and Neuroscience, 2022.

[44] Chen, X., Wei, Z., Jia, X., Zheng, P., Han, M., & Yang, X. (2022, June). Current Status and Prospects of Blockchain Security Standardization. In 2022 IEEE 9th International Conference on Cyber Security and Cloud Computing (CSCloud)/2022 IEEE 8th International Conference on Edge Computing and Scalable Cloud (EdgeCom) (pp. 24-29). IEEE.

[45] Zhao, Y., Li, Q., Yi, W., & Xiong, H. (2023). Agricultural IoT Data Storage Optimization and Information Security Method Based on Blockchain. Agriculture, 13(2), 274.

[46] Wenhua, Z., Qamar, F., Abdali, T. A. N., Hassan, R., Jafri, S. T. A., & Nguyen, Q. N. (2023). Blockchain technology: security issues, healthcare applications, challenges and future trends. Electronics, 12(3), 546.

[47] Villarreal, E. R. D., García-Alonso, J., Moguel, E., & Alegría, J. A. H. (2023). Blockchain for healthcare management systems: A survey on interoperability and security. IEEE Access, 11, 5629-5652.

[48] Abuhasel, K. A. (2023). A Zero-trust Network-based Access Control Scheme for Sustainable and Resilient Industry 5.0. IEEE Access.

[49] Fatima, Z., Tanveer, M. H., Waseemullah, Zardari, S., Naz, L. F., Khadim, H., ... & Tahir, M. (2022). Production plant and warehouse automation with IoT and industry 5.0. Applied Sciences, 12(4), 2053.

[50] Rožanec, J. M., Novalija, I., Zajec, P., Kenda, K., Tavakoli Ghinani, H., Suh, S., ... & Soldatos, J. (2023). Human-centric artificial intelligence architecture for industry 5.0 applications. International Journal of Production Research, 61(20), 6847-6872.

[51] Raja Santhi, A., & Muthuswamy, P. (2023). Industry 5.0 or Industry 4.0 S? Introduction to Industry 4.0 and a peek into the prospective Industry 5.0 technologies. International Journal on Interactive Design and Manufacturing (IJIDeM), 17(2), 947-979.

[52] Zizic, M. C., Mladineo, M., Gjeldum, N., & Celent, L. (2022). From Industry 4.0 towards Industry 5.0: A review and analysis of paradigm shift for the people, organization and technology. Energies, 15(14), 5221.

[53] Wang, Z. J., Chen, Z. S., Xiao, L., Su, Q., Govindan, K., & Skibniewski, M. J. (2023). Blockchain adoption in sustainable supply chains for Industry 5.0: A multistakeholder perspective. Journal of Innovation & Knowledge, 8(4), 100425.

[54] Natarajan, R., Lokesh, G. H., Flammini, F., Premkumar, A., Venkatesan, V. K., & Gupta, S. K. (2023). A Novel Framework on Security and Energy Enhancement Based on Internet of Medical Things for Healthcare 5.0. Infrastructures, 8(2), 22.

[55] Kohli, P., Sharma, S., & Matta, P. (2022, December). Secured Authentication Schemes of 6G Driven Vehicular Communication Network in Industry 5.0 Internet-of-Everything (IoE) Applications: Challenges and Opportunities. In 2022 IEEE 2nd International Conference on Mobile Networks and Wireless Communications (ICMNWC) (pp. 1-5). IEEE.

[56] Basu, A., Kashyap, A., & Kumar, A. (2023). Entrepreneurial Opportunities in Industry 5.0 Built on Blockchain: An Exploratory Note. IUP Journal of Computer Sciences, 17(2), 21-33.

[57] Nair, M. M., Deshmukh, A., & Tyagi, A. K. (2024). Artificial Intelligence for Cyber Security: Current Trends and Future Challenges. Automated Secure Computing for Next-Generation Systems, 83-114.

[58] Mahomad, R., Akram, S. V., Averineni, A., Babu, G. R., & Satyadeva, C. N. S. (2023, March). Innovative Cyber Security Techniques based on Blockchain Technology for use in Industrial 5.0 Applications. In 2023 10th International Conference on Computing for Sustainable Global Development (INDIACom) (pp. 1316-1320). IEEE.

[59] Sari, R. T. K., & Hindarto, D. (2023). Implementation of Cyber-Security Enterprise Architecture Food Industry in Society 5.0 Era. Sinkron: jurnal dan penelitian teknik informatika, 8(2), 1074-1084.

[60] Hu, H., Cao, Z., & Dong, X. (2022). Autonomous path identity-based broadcast proxy re-encryption for data sharing in clouds. IEEE Access, 10, 87322-87332.

[61] Kan, J., Zhang, J., Liu, D., & Huang, X. (2022). Proxy re-encryption scheme for decentralized storage networks. Applied Sciences, 12(9), 4260.

[62] Nagasree, Y., Rupa, C., Akshitha, P., Srivastava, G., Gadekallu, T. R., & Lakshmanna, K. (2023). Preserving privacy of classified authentic satellite lane imagery using proxy re-encryption and UAV technologies. Drones, 7(1), 53.

[63] Laghari, A. A., Khan, A. A., Alkanhel, R., Elmannai, H., & Bourouis, S. (2023). Lightweight-biov: Blockchain distributed ledger technology (bdlt) for Internet of vehicles (iovs). Electronics, 12(3), 677.

[64] Adel, A. (2022). Future of industry 5.0 in society: Human-centric solutions, challenges and prospective research areas. Journal of Cloud Computing, 11(1), 1-15.

[65] Leng, J., Zhong, Y., Lin, Z., Xu, K., Mourtzis, D., Zhou, X., ... & Shen, W. (2023). Towards resilience in Industry 5.0: A decentralized autonomous manufacturing paradigm. Journal of Manufacturing Systems, 71, 95-114.

[66] Singh, K. N., Baranwal, N., Singh, O. P., & Singh, A. K. (2022). SIELNet: 3D chaotic-map-based secure image encryption using customized residual dense spatial network. IEEE Transactions on Consumer Electronics.

[67] Bhaskaran, R., Karuppathal, R., Karthick, M., Vijayalakshmi, J., Kadry, S., & Nam, Y. (2022). Blockchain Enabled Optimal Lightweight Cryptography Based Image Encryption Technique for IIoT. Intelligent Automation & Soft Computing, 33(3).

[68] Kumar Dave, D. M. ADVANCING MEDICAL DEVICE MANUFACTURING: THE CONVERGENCE OF EDGE COMPUTING AND INDUSTRY 5.0.

[69] Yadav, M., Vardhan, A., Chauhan, A. S., & Saini, S. (2023, February). A Study on Creation of Industry 5.0: New Innovations using big data through artificial intelligence, Internet of Things and next-origination technology policy. In 2023 IEEE International Students' Conference on Electrical, Electronics and Computer Science (SCEECS) (pp. 1-12). IEEE.

[70] Gangwar, V. P., & Reddy, D. (2023). Hospitality Industry 5.0: Emerging Trends in Guest Perception and Experiences. Opportunities and Challenges of Business 5.0 in Emerging Markets, 185-211.

[71] Patel, P. H., Angrish, A. K., & Nadda, V. (2023). A Cross-Sector Comparison of Industry 5.0: Digital Technologies in Supply Chain Management of FMCG and the Automotive Sector. In Opportunities and Challenges of Business 5.0 in Emerging Markets (pp. 99-123). IGI Global.

[72] Sekhar, S. M., Singh, R. P., Sinha, L. A., & Manvi, S. S. (2022). Cyber-Security in Society 5.0. In Society 5.0: Smart Future Towards Enhancing the Quality of Society (pp. 69-86). Singapore: Springer Nature Singapore.

[73] Iqbal, M., Lee, C. K., & Ren, J. Z. (2022, December). Industry 5.0: From Manufacturing Industry to Sustainable Society. In 2022 IEEE International Conference on Industrial Engineering and Engineering Management (IEEM) (pp. 1416-1421). IEEE.

[74] Wagan, A. A., Khan, A. A., Chen, Y. L., Yee, P. L., Yang, J., & Laghari, A. A. (2023). Artificial Intelligence-Enabled Game-Based Learning and Quality of Experience: A Novel and Secure Framework (B-AIQoE). Sustainability, 15(6), 5362.

[75] Sriman, B., Sh, A. S., & Nishaalu, S. (2022, July). Blockchain Industry 5.0: Next Generation Smart Contract and Decentralized Application

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 License. For more information, see https://creativecommons.org/licenses/by-nc-nd/4

This article has been accepted for publication in IEEE Access. This is the author's version which has not been fully edited and
content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2024.3351485

Platform. In 2022 International Conference on Innovative Computing, Intelligent Communication and Smart Electrical Systems (ICSES) (pp. 1-8). IEEE.
[76] Agarwal, A., & Alathur, S. (2023). Metaverse revolution and the digital transformation: intersectional analysis of Industry 5.0. Transforming Government: People, Process and Policy, 17(4), 688-707.
[77] Javeed, D., Gao, T., Kumar, P., & Jolfaei, A. (2023). An Explainable and Resilient Intrusion Detection System for Industry 5.0. IEEE Transactions on Consumer Electronics.
[78] Kiruthiga Devi, M., & Padma Priya, M. (2023). Evolution of Next Generation Networks and Its Contribution Towards Industry 5.0. Resource Management in Advanced Wireless Networks, 45, 45.
[79] Svaigen, A. R., Boukerche, A., Ruiz, L. B., & Loureiro, A. A. (2023). Security in the Industrial Internet of Drones. IEEE Internet of Things Magazine, 6(3), 110-116.
[80] Adel, A. (2023). Unlocking the Future: Fostering Human–Machine Collaboration and Driving Intelligent Automation through Industry 5.0 in Smart Cities. Smart Cities, 6(5), 2742-2782.
[81] Narayanan, M., Poongothai, T., & Saravanan, B. (2022). Crypto-Based Secure Outbound Supply Chain Authentication for Industry 4.0. In Cyber Security and Operations Management for Industry 4.0 (pp. 33-45). CRC Press.
[82] Tran, T. A., Ruppert, T., Eigner, G., & Abonyi, J. (2022). Retrofitting-based development of brownfield industry 4.0 and industry 5.0 solutions. IEEE Access, 10, 64348-64374.
[83] Mazumder, A., Banerjee, P. S., Karmakar, A., Ghosh, P., De, D., & Song, H. (2023, February). Digital Twin for Industry 5.0: A Vision, Taxonomy, and Future Directions. In Doctoral Symposium on Human-Centered Computing (pp. 246-259). Singapore: Springer Nature Singapore.
[84] Ferrag, M. A., Maglaras, L., & Benbouzid, M. (2023). Blockchain and Artificial Intelligence as Enablers of Cyber Security in the Era of IoT and IIoT Applications. Journal of Sensor and Actuator Networks, 12(3), 40.
[85] Sudharson, D., Bhuvaneshwaran, A., Kalaiarasan, T. R., & Sushmita, V. (2023, March). A Multimodal AI Framework for Hyper Automation in Industry 5.0. In 2023 International Conference on Innovative Data Communication Technologies and Application (ICIDCA) (pp. 282-286). IEEE.
[86] Skorenkyya, Y., Zolotyya, R., Fedaka, S., Kramara, O., & Kozaka, R. Digital Twin Implementation in Transition of Smart Manufacturing to Industry 5.0 Practices.
[87] Roy, B., Mukherjee, S., Bhattacherjee, N. K., Samanta, S., & Gupta, S. (2023, February). Performance Analysis of Professional Higher Education Programmes Driven by Students Perception: A Latent Variable Computation Model for Industry 5.0. In Doctoral Symposium on Human-Centered Computing (pp. 223-234). Singapore: Springer Nature Singapore.
[88] Espina-Romero, L., Guerrero-Alcedo, J., Goñi Avila, N., Noroño Sánchez, J. G., Gutiérrez Hurtado, H., & Quiñones Li, A. (2023). Industry 5.0: Tracking Scientific Activity on the Most Influential Industries, Associated Topics, and Future Research Agenda. Sustainability, 15(6), 5554.
[89] Sharma, R., & Arya, R. (2022). UAV based long range environment monitoring system with Industry 5.0 perspectives for smart city infrastructure. Computers & Industrial Engineering, 168, 108066.
[90] Muthuswamy, P. (2023). Industry 5.0 or Industry 4.0 S? Introduction to Industry 4.0 and a peek into the prospective Industry 5.0 technologies. International Journal on Interactive Design and Manufacturing (IJIDeM), 1-33.
[91] Adeniyi, E. A., Falola, P. B., Maashi, M. S., Aljebreen, M., & Bharany, S. (2022). Secure sensitive data sharing using RSA and ElGamal cryptographic algorithms with hash functions. Information, 13(10), 442.
[92] Blanc, S., Lahmadi, A., Le Gouguec, K., Minier, M., & Sleem, L. (2022). Benchmarking of lightweight cryptographic algorithms for wireless IoT networks. Wireless Networks, 28(8), 3453-3476.
[93] Thabit, F., Can, O., Alhomdy, S., Al-Gaphari, G. H., & Jagtap, S. (2022). A Novel Effective Lightweight Homomorphic Cryptographic Algorithm for data security in cloud computing. International Journal of Intelligent Networks, 3, 16-30.
[94] Sudharson, K., & Arun, S. (2022). Security Protocol Function Using Quantum Elliptic Curve Cryptography Algorithm. Intelligent Automation & Soft Computing, 34(3).
[95] Alabdulrazzaq, H., & Alenezi, M. N. (2022). Performance evaluation of cryptographic algorithms: DES, 3DES, blowfish, twofish, and threefish. International Journal of Communication Networks and Information Security, 14(1), 51-61.
[96] Khan, A. A., Wagan, A. A., Laghari, A. A., Gilal, A. R., Aziz, I. A., & Talpur, B. A. (2022). BIoMT: A state-of-the-art consortium serverless network architecture for healthcare system using blockchain smart contracts. IEEE Access, 10, 78887-78898.
[97] Oliveira, M., Chauhan, S., Pereira, F. A., Felgueiras, M. C., & Carvalho, D. V. (2023). Blockchain Protocols & Edge Computing Targeting Industry 5.0 Needs.
[98] De, D., Karmakar, A., Banerjee, P. S., Bhattacharyya, S., & Rodrigues, J. J. (2022). BCoT: Introduction to Blockchain-Based Internet of Things for Industry 5.0. In Blockchain based Internet of Things (pp. 1-22). Singapore: Springer Singapore.
[99] Kumar, N., Sharma, B., & Narang, S. (2022, July). Emerging Communication Technologies for Industrial Internet of Things: Industry 5.0 Perspective. In Proceedings of Third International Conference on Computing, Communications, and Cyber-Security: IC4S 2021 (pp. 107-122). Singapore: Springer Nature Singapore.
[100] Ayub, M. F., Li, X., Mahmood, K., Shamshad, S., Saleem, M. A., & Omar, M. (2023). Secure Consumer-Centric Demand Response Management in Resilient Smart Grid as Industry 5.0 Application With Blockchain-Based Authentication. IEEE Transactions on Consumer Electronics.
[101] Khan, A. A., Shaikh, A. A., & Laghari, A. A. (2023). IoT with multimedia investigation: A secure process of digital forensics chain-of-custody using blockchain hyperledger sawtooth. Arabian Journal for Science and Engineering, 48(8), 10173-10188.
[102] Singh, S. K., Yang, L. T., & Park, J. H. (2023). FusionFedBlock: Fusion of Blockchain and federated learning to preserve privacy in industry 5.0. Information Fusion, 90, 233-240.
[103] Abishek, B. A., Kavyashree, T., Jayalakshmi, R., Tharunkumar, S., & Raffik, R. (2023, June). Collaborative Robots and Cyber Security in Industry 5.0. In 2023, the 2nd International Conference on Advancements in Electrical, Electronics, Communication, Computing and Automation (ICAECA) (pp. 1-6). IEEE.



ZAFAR AHMED SHAIKH (Member, IEEE) received the M.Sc. degree in computer science from University of Sindh, Jamshoro, Pakistan, in 2000, the M.S. degree in computer science from Iqra University, Karachi, in 2009, and the Ph.D. degree in computer science from IBA-Karachi, Pakistan, in 2017. Dr. Shaikh was a visiting Doctoral Fellow at the Ecole Polytechnique Fédérale de Lausanne, Switzerland, in 2014. His research interests include expert systems, artificial intelligence, recommender systems, large language models, machine learning methods, learning environments, Blockchain, and educational technologies. To date, Dr. Shaikh has published more than 60 research articles in reputed journals, many of them are indexed in SSCI, SCI-Expended, and Scopus.

FAHIMA HAJJEJ (Member, IEEE) received a Ph.D. in computer science from the Faculty of Sciences of Sfax in 2017. She is currently an Associate Professor with the Department of Information Systems, College of Computer and Information Sciences, PNU, Saudi Arabia. She is also a member of the Research Laboratory in Technologies of Information and Communication and Electrical Engineering (LaTICE). Her research interests include the modeling concepts of Education technology, artificial intelligence, big data, and deep learning.

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 License. For more information, see https://creativecommons.org/licenses/by-nc-nd/4

This article has been accepted for publication in IEEE Access. This is the author's version which has not been fully edited and
content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2024.3351485



YETIR DEMIR USLU (Member, IEEE) is a professor and the head of the Department of Health Management at Istanbul Medipol University. She has a Ph.D. and a master's degree in related fields from reputable universities. She has been working in the academic and professional fields of health for more than 20 years. She is also the director of two centers at Istanbul Medipol University that focus on research and education. She has a rich publication record, with more than 50 articles, books, and book chapters. She is a member of various associations and editorial boards that are relevant to her field. She has also been involved in many projects and conferences as a coordinator, researcher, and speaker. She is a dedicated and passionate professor with a mission of contributing to the health sector and society.



SERHAT YÜKSEL (Member, IEEE) is Associate Professor of finance in İstanbul Medipol University. Before this position, he worked as a senior internal auditor for seven years in Finansbank, Istanbul-Turkey, and one year at Konya Food and Agriculture University as an assistant professor. Dr. Yüksel has a BS in Business Administration (in English) from Yeditepe University (2006) with a full scholarship. He got his master's degree in economics from Boğaziçi University (2008). He also has a Ph.D. in Banking from Marmara University (2015). His research interests lie in energy economics, banking, finance, and financial crisis. He has more than 200 scientific articles, and some of them are indexed in SSCI, SCI, Scopus, and Econlit. Also, he is the editor of some books published by Springer and IGI Global.



HASAN DİNÇER (Member, IEEE) is Professor of Finance at Istanbul Medipol University, Faculty of Economics and Administrative Sciences, Istanbul-Turkey. Dr. Dincer has BAs in Financial Markets and Investment Management from Marmara University. He received his Ph.D. in Finance and Banking with his thesis entitled "The Effect of Changes on the Competitive Strategies of New Service Development in the Banking Sector." He has work experience in the finance industry as a portfolio specialist, and his major academic studies focus on financial instruments, performance evaluation, and economics. He is the executive editor of the International Journal of Finance and Banking Studies (IJFBS) and the founder member of the Society for the Study of Business and Finance (SSBF). He has about 400 scientific articles, and some of them are indexed in SSCI, SCI-Expended, and Scopus. In addition to them, he is also editor of many different books published by Springer and IGI Global.



ROOBAEA ALROOBAEA (Member, IEEE) received a bachelor's degree (Hons.) in computer science from King Abdulaziz University (KAU), Saudi Arabia, in 2008 and a master's degree in information systems and a Ph.D. degree in computer science from the University of East Anglia, U.K., in 2012 and 2016, respectively. He is currently an Associate Professor at the College of Computers and Information Technology, Taif University, Saudi Arabia. His research interests include human–computer interaction, software engendering, cloud computing, the Internet of Things, artificial intelligence, and machine learning.



ABDULLAH M. BAQASAH (Member, IEEE) is with the College of Computers and Information Technology, Taif University, Ta'if, Saudi Arabia. He has published more than 40 papers in several reputed journals related to knowledge management and AI. He is also a senior contributor to AI at the same university for the last two years.



UMA CHINTA (Member, IEEE) is currently pursuing a Ph.D. in Computer Science with a focus on facial expression analysis in individuals in individuals with autism spectrum disorder using multimodal data. She is a published author and recipient of numerous academic awards and fellowships. She is actively engaged in several ongoing research projects, including code comprehension, facial expression analysis, and multimodal emotion recognition.

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 License. For more information, see https://creativecommons.org/licenses/by-nc-nd/4