ASIAN JOURNAL OF ELECTRICAL AND ELECTRONIC ENGINEERING
Vol. 4 No. 2 2024
E-ISSN: 2785-8189

Improving the Privacy in Wireless-Enabled 5G Networks: A Lightweight Protocol for IIoT Communications

Mamoon M. Saeed[1*], Rashid A. Saeed[2], Mohammed Suliman Elbashier[2], Elmustafa Sayed Ali[3], and Zeinab E. Ahmed[2]

[1]*Department of Communications and Electronics Engineering, Faculty of Engineering, University of Modern Sciences (UMS), Yemen*

[2] *College of Electronics Engineering, Faculty of Engineering, Sudan University of Science and Technology, Sudan*

[3] *Department of Electrical & Electronic Engineering, Faculty of Engineering, Red Sea University, Sudan*

*Corresponding author: mamoon530@gmail.com

(Received:7 August 2024; Accepted: 27 August 2024)

Abstract— The vision and major elements of the fifth generation (5G) ecosystem have previously been explored. We examine how security may impact the envisioned 5G wireless systems the challenges and potential solutions to aid in these efforts and define the security and privacy aspects of 5G networks. 5G networks have provided solutions for quicker machine control, problem identification, performance analysis, and data access. Interaction between Internet of Things (IoT) nodes occurs across an unsecured wireless channel, which has positive and negative effects. Despite being physically separated, unauthorized nodes could communicate via an unprotected wireless channel to gather data and take over industrial devices. Secure sessions can mitigate these risks, but it might be challenging to construct a secure session over a weak channel. To address this issue, the Variable Identification (VID) is used. VID offers a simple key exchange platform to authorized Industry Internet of Things (IIoT) nodes while guarding against unauthorized use. The lightweight changeable pseudonyms used by VID for trust-building are selected at random from a pool discovered in the home network and terminal devices. All IDs are chosen at random from a pool and are used to protect data against forgery, replay, alteration, impersonation, and man-in-the-middle attacks, among other things, between the home network and terminal equipment. The ProVerif tool is used to evaluate the suggested system, and the findings demonstrate that it is trustworthy and resistant to prospective attacks.

Keywords: *Wireless, Privacy, IIoT, Security threats, 5G networks*

1. INTRODUCTION

A new era of connectivity and automation in the industrial sector has been brought about by the quick development of 5G networks and the broad uptake of the Industrial Internet of Things (IIoT). However, serious privacy and security problems are raised by the widespread usage of wireless communication in IIoT systems [1, 2]. In wirelessly equipped 5G network environments, there is an increased danger of illegal access, data breaches, and privacy leaks due to continuous connectivity and data sharing across devices. Thus, to protect sensitive data in IIoT communication, it is imperative to design strong privacy-enhancing methods, especially lightweight protocols [3].

DOI: https://doi.org/10.69955/ajoeee.2024.v4i2.62

5G networks, which are wirelessly enabled, present a variety of privacy challenges. The widespread collection of data and the extensive use of sensors and actuators increase the risk of privacy violations. Furthermore, communicating via wireless creates weaknesses that bad actors can take advantage of. Innovative approaches that balance resource limitations, energy efficiency, and privacy protection are needed to meet these problems [4].

In 5G network environments, privacy risks have been reduced by utilizing established privacy-enhancing strategies such as access control methods, authentication protocols, encryption algorithms, and anonymization techniques [5]. However, these methods frequently come with a high processing cost, connection latency, and scalability issues, which makes them less appropriate for IIoT devices with limited resources. It is therefore essential to build lightweight protocols, especially for IIoT communication.

To improve privacy in wirelessly enabled 5G networks, this literature review will examine the state of research and developments in this area, with an emphasis on the creation of lightweight protocols for IIoT communication. The review will look into the privacy issues that wireless-enabled IIoT systems present, examine current privacy-enhancing strategies, and assess how well they work to solve privacy issues. It will also explore the developments in lightweight protocols that are suited to the particular needs of IIoT communication, taking into account things like resource optimization, energy efficiency, and privacy preservation [6 – 8].

This study aims to shed light on the state of privacy in wirelessly enabled 5G networks by undertaking an extensive literature review. It seeks to highlight new trends and technologies, point out the advantages and disadvantages of current methods, and suggest possible directions for further study and invention [9]. To ensure privacy and security in the wirelessly connected 5G networks era, the ultimate goal is to encourage the development of effective and privacy-preserving protocols that can be effortlessly integrated into IIoT communication [10, 11].

The remainder of this work is arranged in the following manner. In Sect. 2, network security architecture in mobile wireless is discussed. Sect. 3 presents privacy-preserving in mobile wireless, followed by Sects. 4 and 5 discussions of the related works system model, and adversary model., Sects. 6 and 7 discuss the proposed scheme and analyze the key features of the proposed solution. Finally, Sect 8 presents the conclusion.

2. NETWORK SECURITY ARCHITECTURE IN MOBILE WIRELESS

Mobile networks have relied on the physical storage of symmetric keys in a subscriber identity module, also known as a subscriber identity module (SIM) card, since the beginning of digital mobile communication in 2G. Additional cryptographic procedures for mutual authentication were implemented, and encryption algorithms shifted from customary to international standards. However, the security approach of 5G is still heavily reliant on SIM cards [12]. Even though SIM cards have shrunk in size (to the "micro" size), they still need to be inserted into devices, limiting their applicability to IoT. The development of eSIMs somewhat addresses this issue, although physical size issues remain. iSIMs, which are now in development, could be used in future devices as part of the System-on-chip concept, while operators are opposed owing to the potential loss of control [13].

2.1 The requirements for a wireless network security architecture model

Traditional SIM cards use tried-and-true symmetric key encryption that has grown to billions of users. However, it has flaws with IoT, privacy, network authentication, and bogus base stations. One important topic is whether symmetric cryptography will give way to asymmetric public/private keys. This has never been done on such a large scale before. 5G aims to provide authentication via a public-key infrastructure in addition to SIM (PKI) [14]. The core of 5G will be a collection of microservices that communicate over HTTPS. Transport Layer Security (TLS) uses elliptic curve cryptography (ECC) to enable authentication, confidentiality, and integrity for such communication. However, this has not yet been implemented and can be put off until 6G [15].

This section answers some of the most frequently asked questions about the 6G security concept. Will physical SIM cards still be used in devices? Will the majority of IoT devices have software SIM clones or Trusted Platform Modules? Although certificate revocation and Certificate Authority (CA) break-ins are possible, a

certificate system for the WWW works. The Domain Name Scheme Security Extensions (DNSSEC) is an example of an asymmetric key system being gradually deployed. A critical prerequisite for asymmetric encryption is the prevention of man-in-the-meddle attacks. Using an IPsec Virtual Private Network (VPN) can enable rudimentary isolation of user traffic; however, the more advanced use of network slicing techniques in 6G will be an open research subject, as it may expose the network to new vulnerabilities [16].

2.2 Evolution of Mobile Security

Cloning, unlawful physical attacks, eavesdropping, encryption issues, authentication and authorization problems, and privacy issues plagued the first generations of mobile networks (i.e., 1G, 2G, 3G) [7]. Then, the security threat landscape transformed with increasingly advanced attack scenarios and powerful attackers. Fig. 1 depicts the progression of the telecommunication network security landscape from 4G to the envisioned 6G future. The execution of wireless applications posed a security and privacy danger to 4G networks. Media access control (MAC) layer security threats (e.g., denial of service (DoS) attacks, eavesdropping, and replay attacks) and malware applications are common examples (e.g., viruses, tampering with hardware).

Security and privacy risks pose problems in 5G access, backhaul, and core networks [18]. The most prevalent security challenges in 5G are cyberwar and critical infrastructure threats, Network Functions Virtualization (NFV) and Software-Defined Networking (SDN) related threats, and cloud computing-associated threats [19 - 22]. SDN can pose a security risk in several ways, including exposing important Application Programming Interfaces (APIs) to unwanted software, introducing Open Flow, and centralizing network control (i.e., making it vulnerable to DoS attacks) [23]. Above all, the increased linked intelligence in telecommunication networks and sophisticated networking and AI/ML technologies are the most crucial driving forces in the 6G vision. However, in many circumstances, the alliance between AI and 6G could be a double-edged sword when it comes to defending or infringing on security and privacy [24 - 27].

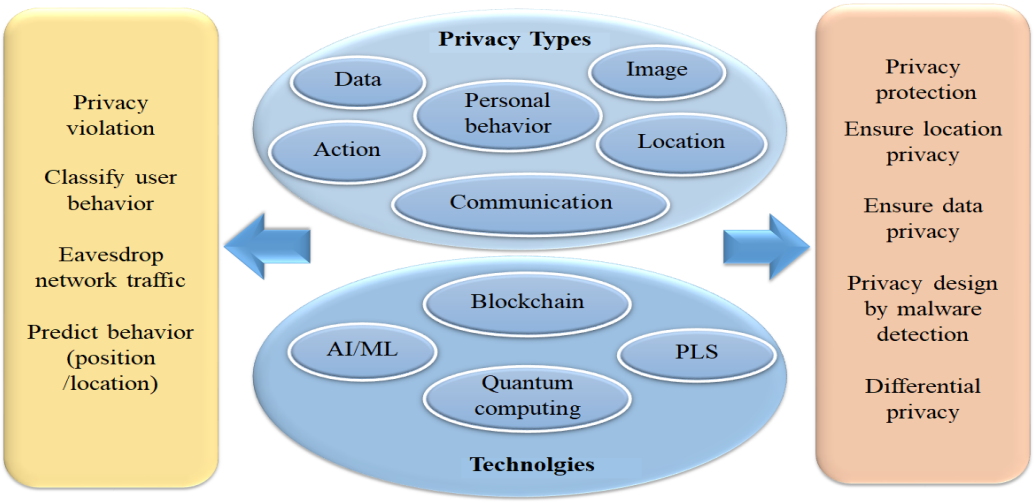

Fig. 1. Landscape of Privacy in Mobile Network.

3. PRIVACY-PRESERVING IN MOBILE WIRELESS

As 5G networks mature, AI-enabled smart applications are projected to become more prevalent, necessitating situational, context-aware, and personalized privacy solutions. Due to a wide and complicated set of unexpected privacy issues, traditional privacy-preserving techniques may not be well suited for future wireless applications [28 – 30]. Distributed ledger technologies, such as blockchain, may make it possible to deploy trustless computing between stakeholders while also providing mechanisms for network privacy protection. Among the security and privacy advantages of blockchain are immutability, transparency, verifiability, anonymity, and pseudonymity.

Blockchain can provide privacy-preserving data-sharing mechanisms, improve access control, provide key characteristics such as data integrity, traceability, and monitoring, and ensure efficient accountability mechanisms, among other things, and is seen as a viable option in Machine Type Communications in 6G [31].

When it comes to tackling important difficulties that are likely to develop in future intelligent 6G wireless applications, differential privacy (DP) approaches appear to be promising. Before sending the final output to the allocated server, DP perturbs the actual data using artificial design random noise functions [32]. This stops attackers from performing a statistical analysis of the data received and inferring personal information from a user's data. For assuring privacy protection, concepts connected to federated learning (FL) are also hot subjects in the research community. FL is a distributed machine learning technique that allows model training for enormous amounts of data to be done locally on the generated source, with each learner in the federation doing the appropriate modeling. Rather than transmitting a raw training dataset, each learner sends his or her local model to an "aggregator" to be combined into a global model. Because FL takes the approach of "bringing the code to the data, rather than the data to the code," it can address critical issues such as data privacy, data ownership, and data localization [33 - 35].

4. RELATED WORKS

Due to the utilization of an open channel for communication. The authors in [36] expressed worry about the security and privacy of Industrial IoT networks. According to the authors, existing approaches may not be suitable in an IIoT-specific setting due to significant overheads. The authors devised a biometric-based privacy-preserving authentication mechanism to counteract unwanted intrusions with minimal overheads. As a two-factor authentication system, the technique employs biometrics and smart cards. To test the protocol's behavior, it was simulated on NS2. After doing formal and informal security analyses, the authors certified their scheme resistant to a variety of assaults.

Despite using two-factor authentication, the technique fails to guard against known key attacks and maintain privacy. The obstacles in establishing security protocols were explored by Li et al. in [37], which included the open nature of the wireless medium and resource-restricted nodes. The authors suggested a three-factor user authentication technique for the WSN-IIoT context that considers these issues. The user's identity, password, and biometrics are the three factors utilized to authenticate. Only if all of the factors provide favorable results will the user be able to view the sensor's data. Although the authors claim their system is immune to impersonation, replay attacks, and other attacks, formal analysis validation is missing.

Because the resource-constrained node transmits and receives a total of 2688 bits during the key exchange procedure, the strategy is wasteful in terms of communication. As a result, the system is unsuitable for resource-constrained IIoT applications. In their paper [38] presented an authentication mechanism for M2M communications in an IIoT environment. According to the authors, traditional techniques cannot be applied in IIoT due to significant overheads that could deplete node resources. As a result, the authors created a novel security model in which only hash and ex-or operations are computed during authentication. The authors declared their approach compute-efficient because of the usage of only a few cryptographic operations. The authors went on to say that their approach has security qualities like session key agreement, and anonymity, and is immune to replay, and man-in-the-meddle (MITM) attacks, among other things. Although the system provides several security benefits, the authors did not do a vulnerability evaluation or formal analysis, therefore the scheme's behavior under compromised settings is uncertain. Furthermore, the technique wastes a lot of energy delivering big mutual authentication and key exchange messages, making it inefficient in terms of energy use. Because of its unpredictable behavior and high energy consumption, the proposed method is unsuitable for IIoT networks.

Xiong et al presented an ECC-based authentication scheme for IIoT in [39]. The authors stressed the importance of an authentication system in WSN to avoid unauthorized access due to the unsecured nature of the medium. Biometrics are used in their scheme to verify the entity's validity. The authors tested their technique on NS3 to see how well it worked. Despite the claimed benefits, it is discovered that the authors did not consider

Denial of Service (DoS) and MITM attacks during the security analysis, which could endanger the network's life. Due to the lack of ciphering and nonce, the system fails to provide privacy and message freshness for all transmitted messages.

Paliwal has stated his concern over data integrity and confidentiality in IIoT networks [40]. The author stressed that sensitive data acquired by sensor nodes in WSN should only be available to those who need it. The article discusses the many available authentication systems as well as their flaws. Hash is used to achieve mutual authentication and key establishment while maintaining identity anonymity. Due to minimal computations and resilience to several significant attacks, the approach is lightweight and efficient. According to the author, the method has undergone formal and informal analysis and is pronounced secure for usage in an IIoT setting. Even though the method is said to be resilient, it does not guarantee privacy. Even though the method does not employ ciphering models, the intensive usage of hashes and the enormous quantity of messages sent overburdens the scheme.

Chang et al. [41] devised an authentication system for WSNs to prevent unauthorized penetrations. Although it is said to be efficient and secure, it is complicated since it runs in two modes. By introducing a smart card-based authentication strategy for WSN, the authors have attempted to address the shortcomings of existing authentication protocols. Their suggested protocol employs two distinct algorithms to achieve two distinct sets of security features. To establish the resilience of their protocol, the authors conducted a formal security analysis using the Real-or-Random (RoR) paradigm. Their first protocol (P1) does not provide complete security solutions, whilst their first protocol (P2) is resource-intensive. Because IoT devices are typically resource-constrained, using this protocol can reduce the devices' and networks' active lifetimes.

In [42], Gope et al. focused on the obstacles to implementing Industrial WSNs (IWSN). The authors designed a new mutual authentication system for IWSN's real-time data access applications, citing security as the most crucial concern. In their approach, the authors used exclusive-or, one-way hash, and physically unclonable functions (PUF), to mention a few. The security of the credentials is the key strength noted in the article, even if the adversary physically captures the sensor nodes. The approach includes important security features, including mutual authentication and integrity. Despite the advantages, the approach requires six messages to complete the session key, which is difficult for devices with limited resources. The number of bits sent in those communications is quite large, which raises the energy consumption threshold even higher. This massive energy usage has the potential to swiftly drain the energy reserves of IIoT nodes. Furthermore, the behavior of the schemes [41, 42] under the effect of a DoS attack is not detected, allowing adversaries to attack IIoT networks via hidden vulnerabilities.

In summary, current approaches are vulnerable to well-known attacks (MITM, Known Key, and DoS, for example). They have large communication and computing costs, making them unsuitable for Industrial IoT networks. The Industrial IoT is a delicate application in which even a little incursion by an unauthorized node can result in significant and irreversible losses. As a result, a secure and efficient key exchange and mutual authentication approach must be used to protect access to the IIoT network. Table 1 summarizes the related works for security issues and applications in IIoT.

There are other research investigations on the security of IIoT based on the 6G network. The authors in [33] offer a high-level overview of the role of trust, security, and privacy in 6G networks and the associated research difficulties. About four essential components of 6G networks, such as real-time intelligent edge computing, distributed artificial intelligence, intelligent radio, and 3D intercoms, this report concisely assesses new study fields and difficulties in security and privacy. Discusses security and privacy concerns with developing technologies such as artificial intelligence (AI), blockchain, quantum communications, Tera Hertz (THz) technology, Visible Light Communication (VLC) technology, and molecular communications. However, the authors in [43] thoroughly examine machine learning and privacy in 6G to accelerate the development of 6G and privacy-protection solutions. At the same time, the authors in [44] discuss unresolved concerns about the

applicability of physical layer security (PLS) in 6G systems and provide a complete road map of significant relevant studies on PLS.

Table 1. IIoT Security Related Works Summary

Citations	Security issue	Contributions	shortcomings
Li et al [37]	Authentication for WSN-IIoT	Authentication based on user's identity, password, and biometrics	weak authentication validation
Esfahani et al [38]	M2M security in IIoT	Use hash and ex-or operations during the authentication process	inefficient energy utilization due to big mutual authentication
Xiong et al [39]	Authentication for IIoT Sensor network	avoid unauthorized access due to the unsecured nature of the medium	weak privacy and message freshness
Paliwal [40]	IIoT networks confidentiality	Using Hash for mutual authentication and key establishment	Weak privacy
Chang et al [41]	prevent unauthorized penetrations	formal security analysis using the Real-or-Random (RoR) paradigm	Reduces network device's lifetime
Gope et al [42]	authentication for real-time IIoT	Use exclusive-or, one-way hash, and PUF for mutual authentication	weak against attack via hidden vulnerabilities, and high computation energy

The security and privacy of IIoTs have been discussed by numerous researchers. To create a dependable, accessible, and secure Remote Patient Monitoring (RPM) system in the end, the authors of [45] suggested an integration of the IoT with healthcare facilities that are secure and privacy-preserving. The suggested solution offers end-to-end secure communications, secure RFID-based authentication, and privacy protection. The authors of [46] concentrated on how blockchain can assist 5G network applications in safeguarding execution integrity and proposed a low-cost and simple-to-implement blockchain-based execution protection strategy called NoSneaky. The inventors of [47] suggested a communication protocol that uses only symmetric key-based encryption, which offers incredibly lightweight yet strong encryptions to safeguard data transmissions. To fend off key reset and device capture threats, the symmetric keys created by this protocol are delegated based on a chaotic system, the logistic map.

A blockchain-based deep learning system with two degrees of security and privacy was provided by other authors [48]. To achieve the goal of security and anonymity, a blockchain system is first built in which each participating entity is registered, verified, and then validated utilizing a smart contract-based enhanced Proof of Work. Second, a deep learning system with the Bidirectional Long Short-Term Memory (BiLSTM) for intrusion detection and the Variational Auto Encoder (VAE) technique for privacy is built. The authors in [49] provided a timely discussion of how promissory 6G enabling technologies like artificial intelligence, network softwarization, network slicing, blockchain, edge computing, intelligent reflecting surfaces, backscatter communications, terahertz links, visible light communications, physical layer authentication, and cell-free massive multiple-input multiple-output (MIMO) will play a part in delivering the expected level of security and privacy.

5. PROTOTYPE MODEL (SYSTEM AND ADVERSARY)

The IIoT security based on the system prototype model consists of different IoT components in addition to the adversary model. Fig. 2 shows an internet-connected IIoT network that can be controlled and monitored. The IIoT architecture is made up of IoT sensor nodes installed on machines that connect with the CA and the cloud via a wireless bi-directional link. Through the cloud, the user has access to information. The system prototype model consists of the following devices.

- ***WSN-IIoT network:*** Sensor nodes are installed on machines in the industry. The sensor nodes receive control signals from the operator (e.g., turn on/off the machine), collect data from machines (e.g., production count, machine temperature, pressure, etc.) and wirelessly relay it to the gateway using low-power modules such as Zigbee (IEEE 802.15.4) and Z-Wave (a.k.a, ZW0500).
- ***Gateway***: Typically, a gateway is stationary and powered by the mains. The gateway serves as an intermediary between the smart IoT sensor node, the cloud, and the CA. It supports the IEEE 802.3 and IEEE 802.11 standards for data transmission via the Internet. The gateway authenticates the IIoT network's nodes before transferring their data to the cloud and vice versa.
- ***Certification authority:*** The certification authority (e.g., Symantec, GeoTrust, and others) builds a database of the network's nodes and uses it to undertake mutual authentication before giving certificates to nodes. Each sensor node receives a unique implicit certificate from the CA, which they must use to create public and private keys.

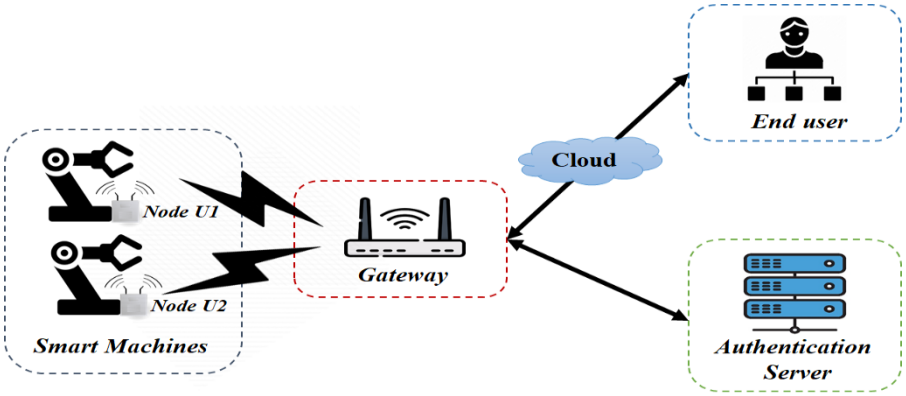

Fig. 2. An IIoT system model based on a mutual authentication key exchange method

The Dolev-Yao adversary model recommended in [41, 50] has been used in the suggested approach. According to the threat model, the adversary can uncover the industrial network's flaws, which can then be exploited to exploit the industries' potential resources. Consider an IIoT-enabled smart automobile manufacturing business [51], where sensor nodes are used to monitor and control robotic arm activities, manage logistics, and identify raw material requirements at the warehouse, among other things. According to the Dolev-Yao adversary model, robotic industrial machines (nodes), logistics and warehouse network devices (gateway), and other IIoT devices are under threat. In the IIoT, an adversary can listen to all conversations between industrial nodes, gateways, and CA.

An adversary can collect, modify, and replay network signals to gain privileged access to industrial robotic arms (e.g., welding, painting, transportation, and assembling), among other things. In addition, an adversary can pose as a legal industrial node to steal data from RFID tags. Physical capture of smart industry devices (nodes and gateways) is not conceivable because they are secured with physical locks and monitored by surveillance cameras. The adversary may attempt to change the lifetime of the expired authenticator to gain unauthorized access to the

industrial network and introduce malware into the industry's computerized production units. Furthermore, the attacker can intercept data sent between network entities to obtain security parameters that can be used to generate future secret keys, activate driverless cars, and so on.

The adversary can create and inject new messages through the network to perform a DoS attack that prevents control orders from being sent to industrial machinery (e.g., warehouse storage sequencing error). To summarize, the opponent can obstruct the smooth and secure operation of production units, warehouses, and logistics, among other things. Financial and reputational harm, company interruption, and lower efficiency are all possible outcomes of hostile attacks.

6. PROPOSED METHODOLOGY

Multi-variable identifications (M-VIDs), which cannot be easily associated with the ID or tracked, must be assigned to defend against attacks related to identification. To satisfy these needs, this technique switches the fixed ID identification out for the regularly changing M-VID identifiers. Before sending the range to the UE, the serving network (SN) assigns a range of M-VID IDs to the User (D). The SN then starts the ID relocation process and gives the user two M-VID values, S and L, which stand for the range's start and length M-VID values. S stands for the range's start point, and L for the range's length. It is up to the network operator to specify the length K. The user reads the allocated range D as follows: The largest M-VID in D is (S+L), whereas the smallest M-VID in D is S. The SN then randomly produces a new M-VID value between S and S+L whenever it needs to identify the user and adds it in the identification message that will be sent to the user. The user equipment also knows that the M-VID utilized for identification should remain between S+L and S.

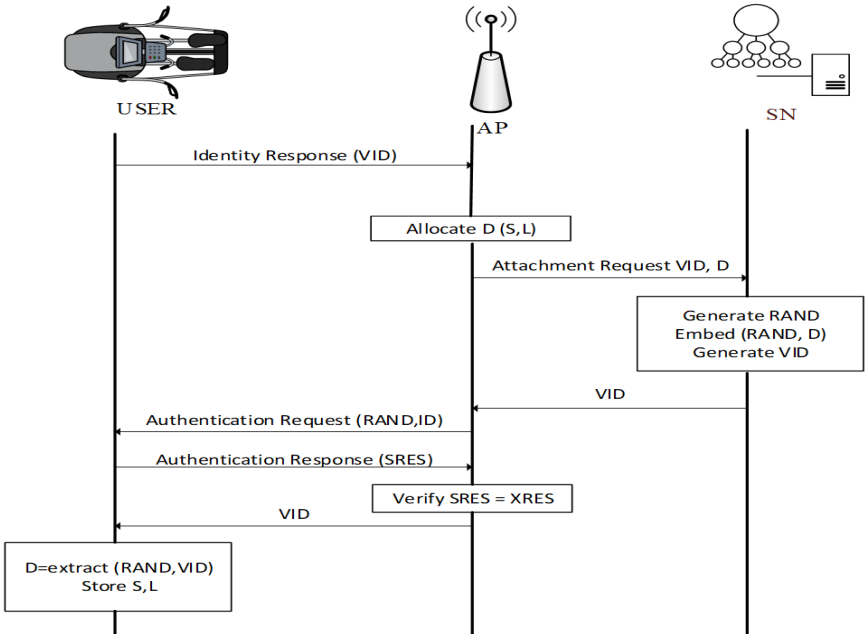

Fig. 3. The essential steps of sending and assigning of ID range to the user.

The SN incorporates the newly created M-VID value among S+L and S into the identification message that will be sent to the user. When the SN wants to identify the user, this occurs. The user checks the incoming M-VID to see if it falls between S+L and L or not. If the received M-VID falls within the proper range, the user may respond and begin the service request procedure; if not, the user discards the message requesting identification. Fig. 3 depicts the allocation procedure and the user receiving the M-VIDs range.

To implement the proposed solution some modifications must be executed in SN and user. As illustrated in the following subsections, we provide our proposed algorithms for both SN and user end.

6.1 The Proposed Algorithm in SN

The proposed solution suggested values for all identifiers as shown in Table 2. A table called P-table contains M-VIDs for all users within its service region that have been added to the SN storage. One user's M-VIDs are stored in a tuple of P-tables, which include the fields VID, S, T, V, and V. The start and length M-VID values in the user-assigned range are denoted by S and L, respectively. The T represents the M-VID value that was most recently used to identify the user, whereas the V represents the M-VID value that the user most recently used to submit a service request. The SN furthermore maintains a list of M-VID ranges known as VID-pool. The VID-pool is a table with columns S, L, and STATUS, as illustrated in Table 2. M-VID ranges' start and length M-TMSI values are stored in variables S and L, respectively. The STATUS next to each range indicates whether or not the range is available for use. When STATUS is set to 0, it means that the relevant range is available for use. The associated STATUS will be 1 for the given range.

Table 2. M-VID values in the proposed solution

a- VID Pool

S	*L*	*STATUS*
S_1	L_1	*1*
…	…	…
Si	L_i	1
…	…	…
S_K	L_K	0
…	…	…
Sn	*Ln*	0

b- P-table

VID	*S*	*L*	*T*	*V*
VID_1	S_1	L_1	T_1	V_1
…	…	…	…	…
…	…	…	…	…
VIDi	*Si*	*Li*	*Ti*	*Vi*
…	…	…	…	…
…	…	…	…	…
VID_K	S_K	L_K	T_K	V_K

The proposed scheme can be described using two phases: Setup and Manage M-TMSIs.

A. Setup Phase (The Initial Allocation)

The initial M-VIDs range allocation to users within the SN's service region is carried out during the setup phase. Only the initial execution of the Setup phase is performed, and it must be successful before the management phase is launched. The following are the main steps in the Setup phase:

- VID-pool information initialization using M-VIDs: The SN executes the Initialize-Pool algorithm to initialize the M-VID-pool with the M-VID range bounds.
- Give the users access to the M-VID ranges: Within its service area, the SN executes the Allocate Range algorithm for each user.
- Provide the M-VID ranges to the users: The SN provides the bounds of the M-VID ranges assigned to the concerned users.

B. Manage Phase (Monitor and Control)

As depicted in Algorithm 1, the manage phase entails continuing actions and processes that include monitoring the M-VID-related service requests made by the user, the SN, and other SNs, and appropriately modifying the M-VID data at the SN. Through several methods for M-TMSI range allocation, re-allocation, and

de-allocation during the Manage phase, the SN manages the M-VID identities and preserves the consistency of the contents of the P-table and the M-VID-pool.

• M-VID range Allocation: The SN allocates a new M-VID range D to the user after successful authentication runs.

• M-VID range Re-Allocation: After a successful run of the Tracking Area Update (TAU) procedure, the SN determines whether to replace the M-VID range that is currently allocated to the user or to keep it. If the range currently allocated to the user will cause an M-VID collision, the SN replaces it with a new range.

• M-VID range De-Allocation: The SN de-allocates the M-VID range allocated to a user after a successful request.

• M-VID Validation: When a user sends a request including an M-VID identifier to the SN, the latter verifies that the request is initiated by a genuine user using the Validate Request algorithm.

6.2 The Proposed Algorithm for User

The suggested scheme needs the user to be expanded to store the following four values: S_{User}, L_{User}, T_{User}, and V_{User}. The bounds of the M-VID range provided by the SN are stored in the S_{User} and L_{User}. The M-VID identities that the user most recently sent and received are kept in the T_{User} and the V_{User} respectively. Modifications about VID relocation, identification, and service request processes should also be made to the user's functionality.

The user confirms that the embedded M-VID value within the identification message is within the appropriate range (VID is between S_{User} and S_{User} +L_{User}) and is distinct from the M-VID that was last delivered or received by the user after receiving an identification message request from the SN (T_{User} or V_{User}). If so, the user replies by submitting a service request and updating its T_{User} to the newly arriving VID identity. If not, the message request is ignored. Algorithm 2 shows the M-VID validation process.

Algorithm 1: The Manage phase algorithm

```
Input: The VID or ID identifiers of the user involved in the request and service request code
1:  while true do
2:    if request ='An Attachment' then
3:        call Allocate-Range (VID)
4:        call VID-Relocation-Procedure
5:  end if
6:    if request ='Tracking Area Update TAU' then
7:         call ReAllocate-Range (VID)
8:         call ID-Relocation-Procedure
9:    end if
10:    if request ='Request from the SN to forget about the User" then
11:          call DeAllocate-Range (VID)
12:    end if
13:    if request ='Identification the User' then
14:          call Identification-User (VID)
15:    end if
16:   if timer ='0' then
17:    for each User whose timer is expired do
18:                call ReAllocate-Range (VID)
19:               call ID-Relocation-Procedure
20:           end for
21:    end if
22:    if request ='Radio Resource Channel request with ID identifier' then
23:                call Validate-Request (ID)
24:   if Auth = true then
25:                     process the request
```

26: *else*
27: *discard the request*
28: *end if*
29: *end if*
30: *end while*

Algorithm 2: Identifying message validation algorithm

Input: identifying message including the ID (VID) received from serving network
1: if ($S_{User} \leq VID \leq S_{User} + L_{User}$)
2: if ($VID \neq T_{User}$ & $VID \neq V_{User}$)
3: update $V_{User} = VID$
4: initiate a service request
5: else
6: discard the request
7: end if
8: else
9: discard the request
10: end if

If a user certifies that it was the intended recipient of the identification message sent by the SN, the user starts a service request. To start a service request, the user first creates a new M-VID value at random (VIDUser), inserts it into the message to the SN, and changes VIDUser to TUser. Algorithm 3 describes the stages involved in a service request.

Algorithm 3: Service Request Algorithm

1: create a random fresh M_U *such that:*
2: $S_U \leq M_U \leq (S_U + L_U)$,
3: $M_U \neq T_U$, *and*
4: $M_U \neq V_U$
5: update $T_U = M_U$
6: initiate service request

7. ANALYSIS AND DISCUSSION

In the current IIoT architecture, a user is given an ID identifier to be able to be identified specifically throughout the identification process. The user's ID is always included in the identifying request message and sent to the user whenever the providing network wants to identify an idle user. The issue is that the allocated ID is kept for a long enough time for an attacker to connect it to the permanent identification ID of the user and use it to attach identifying communications to that user.

As a result, the current identification process is not secure against user link-ability attacks. The properties of ID identifiers and the ID allocation mechanism are recommended to be improved, adding security performance and protecting against link-ability attacks. Each time a user is identified, a random VID identification is used, which ensures that an observer cannot connect the identifying request to the same user.

7.1 The Key Features

In our proposed approach, the user is only required to perform a minimal amount of computation, with the serving network bearing the rest of the burden. We assert that the overhead is little since the SN has limitless computing capacity. We additionally assert that the user's calculation overhead is minimal. The delay time in SN and the user comparing by utilizing ID rose slightly due to the VID changing in every identification and random access. It nonetheless outperformed encryption techniques like ENC-ID. The VID enhanced the characteristics of ID identifiers by replacing it with the VIDs which added a high level of user privacy in IIoT networks. A new random VID is generated and consumed whenever a user is requested to be identified to the SN. This guarantees

that an observer cannot link the VIDs to a certain user, and hence prevents against tracking the user. As the VID changes in every request, the delay time increases slightly in the network and the user compared by using ID. However, it was better than an encryption method like ENC-ID. The delay time on SN and user by using the ID, VID, and ENC-ID.

Figures 4 and 5 display the delay time on SN and user utilizing the ID, VID, and ENC-ID. The identification process takes a little longer when M-VIDs are used than the normal technique because the identification (ID) is sent in clear text. While the identifying process takes longer with the encryption method. Because encryption methods require algorithms to encrypt and decrypt the ID with every identification operation, there was a greater time delay or overhead. Encryption and decryption tasks will take longer to complete in user and SN. In addition to that, each identifying procedure requires more time for the generation of encryption keys.

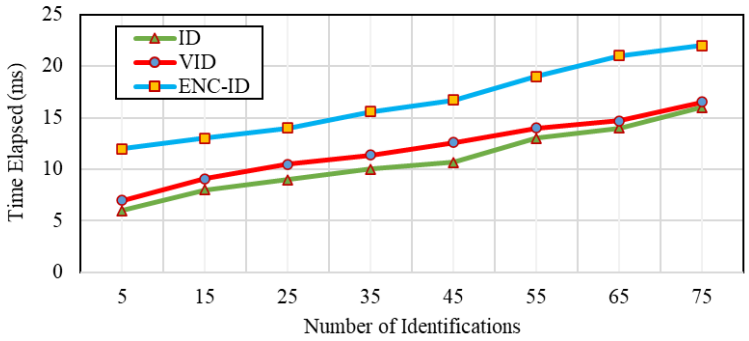

Fig. 4: User identification overhead on SN.

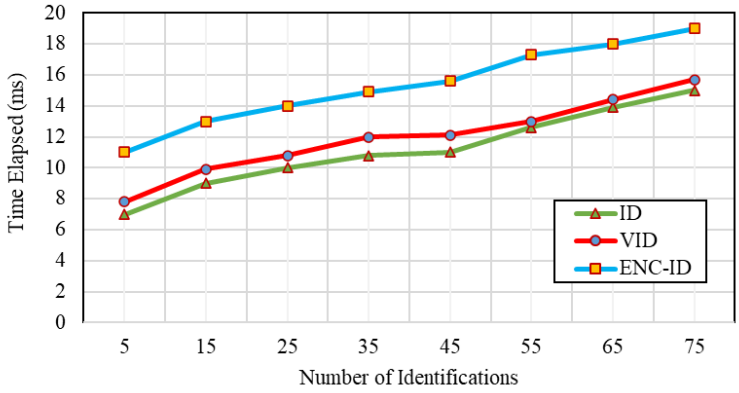

Fig. 5: User identification overhead on User.

Considering the features of system impact and Compatibility with IoT architecture, the proposed solution gives a minimal system impact, which is transparent to the intermediary networks because it does not call for modifications to the messages or the messaging infrastructure. Due to the minimum changes, it requires of the network parties, the solution can easily be compatible with the current IIoT architecture.

7.2 Security Analysis

The security of the solution is examined in this part in terms of unlinkability, anonymity, and untraceability.

A. *User Unlink-ability*

Linkability is the potential for connecting different user identities. By making IIoT networks unlinkable, the proposed technique eliminates user linkability and defends users against tracking attacks. Instead of being given a permanent ID that can be traced and associated with a specific user, the user is given a series of temporary identities, or VIDs. As seen in Fig. 6, a new random VID is generated and used each time a user requests to be

recognized by the network. This ensures that a viewer cannot connect the VIDs to a specific user, preventing the viewer from tracking the user.

B. User Anonymity

The suggested system offers a high level of confidence in preserving user identification. Since the ID is only accessible by the NS and the user and no other party on the network is aware of it, an attacker cannot know it. The ID is also never utilized or communicated. Because the NS changes the VID before being sent to the user, there is no way for an attacker to determine the VID given to a specific user. Until a user uses their VID for identification, the attacker is not made aware of their VID. It is important to note that the attacker cannot benefit from knowing a specific VID. The approach used by the suggested scheme about VID selection grants a user the right to protect their user anonymity and hinders attackers from doing so. The user can only use a VID once, therefore as soon as the network successfully identifies them, they are given a brand-new VID that is distinct from the one they were previously using. The brand-new VID given to the user is chosen randomly and has nothing to do with the VID that they utilized most recently. VIDs allocated to a specific user appear to an attacker to be random bit streams that cannot be connected to a specific user. As a result, the attacker is unable to identify the target user, and Fig. 6 illustrates the provision of the highest level of identity anonymity.

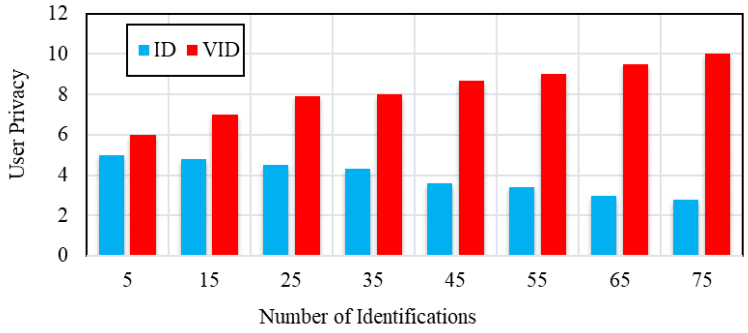

Fig. 6: User privacy comparison between ID and VID.

C. User Un-traceability

Traceability is the ability to track previous identity requests and responses coming from the same subscriber. The proposed method improves the properties of the pseudonyms and the methods for allocating them, which prevents user traceability and defends users from tracking attacks (TIDs). This makes it challenging for an observer to distinguish between identification requests and responses sent to the same user because the pseudonyms exchanged in the network appear random and unrelated from the observer's point of view. As a result, the user's untraceability is provided and the observer is unable to recognize the user's previous identification requests and responses.

8. CONCLUSION

The issue of safeguarding the privacy of the identifying procedure in the IIoT network is addressed in this study with a practical solution. Through a secure identification technique that enables a user to be uniquely identified by the network while remaining anonymous within the network, the identifying procedure privacy is maintained, preventing adversaries from being able to monitor and identify the user. The benefit of the solution is that it is simple to integrate into the existing architecture and is compatible with current IIoT technology standards. With minimum changes at both the network and the user level, low computing overhead on the part of the network, and negligible calculation overhead on the part of the user, the proposed method protects the identifying procedure privacy in IIoT and ensures user un-traceability and unlink-ability.

REFERENCES

[1]. Peter, O., Pradhan, A., & Mbohwa, C. Industrial internet of things (IIoT): opportunities, challenges, and requirements in manufacturing businesses in emerging economies. Procedia Computer Science, (2023), 217, 856-865, https://doi.org/10.1016/j.procs.2022.12.282

[2]. Kumar, R., Rani, S., & Awadh, M. A. Exploring the application sphere of the internet of things in industry 4.0: a review, bibliometric and content analysis. Sensors, (2022), 22(11), 4276, https://doi.org/10.3390/s22114276.

[3]. Garrido, G. M., Sedlmeir, J., Uludağ, Ö., Alaoui, I. S., Luckow, A., & Matthes, F. Revealing the landscape of privacy-enhancing technologies in the context of data markets for the IoT: A systematic literature review. Journal of Network and Computer Applications, (2022), 207, 103465, https://doi.org/10.1016/j.jnca.2022.103465

[4]. Ali, A., Al-Rimy, B. A. S., Alsubaei, F. S., Almazroi, A. A., & Almazroi, A. A. HealthLock: Blockchain-Based Privacy Preservation Using Homomorphic Encryption in Internet of Things Healthcare Applications. Sensors, (2023), 23(15), 6762, https://doi.org/10.3390/s23156762

[5]. Rizi, M. H. P., & Seno, S. A. H. A systematic review of technologies and solutions to improve security and privacy protection of citizens in the smart city. Internet of Things, (2022), 20, 100584, https://doi.org/10.1016/j.iot.2022.100584

[6]. Kamdjou, H. M., Baudry, D., Havard, V., & Ouchani, S. Resource-Constrained eXtended Reality Operated with Digital Twin in Industrial Internet of Things. IEEE Open Journal of the Communications Society, (2024), https://doi.org/10.1109/OJCOMS.2024.3356508

[7]. Kamarudin, N. H., Suhaimi, N. H. S., Nor Rashid, F. A., Khalid, M. N. A., & Mohd Ali, F. Exploring Authentication Paradigms in the Internet of Things: A Comprehensive Scoping Review. Symmetry, (2024), 16(2), 171, https://doi.org/10.3390/sym16020171

[8]. Mengistu, T. M., Kim, T., & Lin, J. W. A Survey on Heterogeneity Taxonomy, Security and Privacy Preservation in the Integration of IoT, Wireless Sensor Networks and Federated Learning. Sensors, (2024), 24(3), 968, https://doi.org/10.3390/s24030968

[9.] Alotaibi, B. A survey on industrial Internet of Things security: Requirements, attacks, AI-based solutions, and edge computing opportunities. Sensors, (2023), 23(17), 7470, https://doi.org/10.3390/s23177470

[10]. Mohsan, S. A. H., & Li, Y. A Contemporary Survey on 6G Wireless Networks: Potentials, Recent Advances, Technical Challenges and Future Trends. arXiv preprint arXiv:2306.08265, (2023), https://doi.org/10.48550/arXiv.2306.08265

[11]. Yazici, İ., Shayea, I., & Din, J. A survey of applications of artificial intelligence and machine learning in future mobile networks-enabled systems. Engineering Science and Technology, an International Journal, (2023), 44, 101455, https://doi.org/10.1016/j.jestch.2023.101455

[12]. Huda Mahmood, Nurul, et al. "Six Key Enablers for Machine Type Communication in 6G." arXiv e-prints (2019): arXiv-1903, https://doi.org/10.48550/arXiv.1903.05406

[13]. Hasan, M. K., et al. "Inter-cell interference coordination in LTE-A HetNets: A survey on self organizing approaches." 2013 International Conference on Computing, Electrical and Electronic Engineering (ICCEEE). IEEE, 2013, https://doi.org/10.1109/ICCEEE.2013.6633932

[14]. Saeed, M. M. A., Saeed, R. A., & Ahmed, Z. E. (2024). Data Security and Privacy in the Age of AI and Digital Twins. In Digital Twin Technology and AI Implementations in Future-Focused Businesses (pp. 99-124). IGI Global, https://doi.org/10.4018/979-8-3693-1818-8.ch008

[15]. Saeed, Mamoon M., et al. "A novel variable pseudonym scheme for preserving privacy user location in 5G networks." Security and Communication Networks 2022 (2022), https://doi.org/10.1155/2022/7487600

[16]. Hasan, Mohammad Kamrul, et al. "Evolution of industry and blockchain era: monitoring price hike and corruption using BIoT for smart government and industry 4.0." IEEE Transactions on Industrial Informatics 18.12 (2022): 9153-9161, https://doi.org/10.1109/TII.2022.3164066

[17]. Strinati, Emilio Calvanese, et al. "6G: The next frontier: From holographic messaging to artificial intelligence using subterahertz and visible light communication." IEEE Vehicular Technology Magazine 14.3 (2019): 42-50, https://doi.org/10.1109/MVT.2019.2921162
[18]. Tariq, Faisal, et al. "A speculative study on 6G." IEEE Wireless Communications 27.4 (2020): 118-125, DOI: 10.1109/MWC.001.1900488
[19]. Van Der Zwaag, Klaas Minne, et al. "A manchester-ook visible light communication system for patient monitoring in intensive care units." IEEE Access 9 (2021): 104217-104226, https://doi.org/10.1109/ACCESS.2021.3099462
[20]. Saeed, Mamoon M., et al. "A comprehensive review on the users' identity privacy for 5G networks." IET Communications 16.5 (2022): 384-399, https://doi.org/10.1049/cmu2.12327
[21]. Saeed, Mamoon M., et al. "Task Reverse Offloading with Deep Reinforcement Learning in Multi-Access Edge Computing." 2023 9th International Conference on Computer and Communication Engineering (ICCCE). IEEE, 2023, https://doi.org/10.1109/ICCCE58854.2023.10246081
[22]. Ahmed, Zeinab E., et al. "Mobility Management Enhancement in Smart Cities using Software Defined Networks." Scientific African (2023): e01932, https://doi.org/10.1016/j.sciaf.2023.e01932
[23]. Amanlou, Sanaz, Mohammad Kamrul Hasan, and Khairul Azmi Abu Bakar. "Lightweight and secure authentication scheme for IoT network based on publish–subscribe fog computing model." Computer Networks 199 (2021): 108465, https://doi.org/10.1016/j.comnet.2021.108465
[24] Huda Mahmood, Nurul, et al. "Six Key Enablers for Machine Type Communication in 6G." arXiv e-prints (2019): arXiv-1903, https://doi.org/10.48550/arXiv.1903.05406
[25]. Saeed, Mamoon M., et al. "Attacks Detection in 6G Wireless Networks using Machine Learning." 2023 9th International Conference on Computer and Communication Engineering (ICCCE). IEEE, 2023, https://doi.org/10.1109/ICCCE58854.2023.10246078
[26]. Saeed, Mamoon M., et al. "Green Machine Learning Approach for QoS Improvement in Cellular Communications." 2022 IEEE 2nd International Maghreb Meeting of the Conference on Sciences and Techniques of Automatic Control and Computer Engineering (MI-STA). IEEE, 2022, https://doi.org/10.1109/MI-STA54861.2022.9837585
[27]. Saeed, Mamoon M., et al. "Anomaly Detection in 6G Networks Using Machine Learning Methods." Electronics 12.15 (2023): 3300, https://doi.org/10.3390/electronics12153300
[28]. Muthana, Abdulrahman A., and Mamoon M. Saeed. "Analysis of user identity privacy in LTE and proposed solution." International Journal of Computer Network and Information Security 9.1 (2017): 54, https://doi.org/.5815/ijcnis.2017.01.07
[29]. Saeed, Mamoon M., Rashid A. Saeed, and Elsadig Saeid. "Preserving privacy of paging procedure in 5th G using identity-division multiplexing." 2019 First International Conference of Intelligent Computing and Engineering (ICOICE). IEEE, 2019, https://doi.org/10.1109/ICOICE48418.2019.9035167
[30]. Saeed, Mamoon M., et al. "Preserving Privacy of User Identity Based on Pseudonym Variable in 5G." Computers, Materials & Continua 70.3 (2022), https://doi.org/10.32604/cmc.2022.017338
[31]. Wang, Qixu, et al. "PCP: A privacy-preserving content-based publish–subscribe scheme with differential privacy in fog computing." IEEE Access 5 (2017): 17962-17974, https://doi.org/10.1109/ACCESS.2017.2748956
[32]. Bonawitz, Keith, et al. "Towards federated learning at scale: System design." Proceedings of machine learning and systems 1 (2019): 374-388, https://doi.org/10.48550/arXiv.1902.01046
[33]. Niknam, Solmaz, Harpreet S. Dhillon, and Jeffrey H. Reed. "Federated learning for wireless communications: Motivation, opportunities, and challenges." IEEE Communications Magazine 58.6 (2020): 46-51, https://doi.org/10.1109/MCOM.001.1900461

[34]. Ylianttila, Mika, et al. "6G white paper: Research challenges for trust, security and privacy." arXiv preprint arXiv:2004.11665 (2020), https://doi.org/10.48550/arXiv.2004.116

[35]. Das, Ashok Kumar, et al. "Biometrics-based privacy-preserving user authentication scheme for cloud-based industrial Internet of Things deployment." IEEE Internet of Things Journal 5.6 (2018): 4900-4913, https://doi.org/10.1109/JIOT.2018.2877690

[36]. Saeed, R. A., Saeed, M. M., Ahmed, Z. E., & Hashim, A. H. (2024). Enhancing Medical Services Through Machine Learning and UAV Technology: Applications and Benefits. In Applications of Machine Learning in UAV Networks (pp. 307-343). IGI Global https://doi.org/10.4018/979-8-3693-0578-2.ch012

[37]. Li, Xiong, et al. "A robust and energy efficient authentication protocol for industrial internet of things." IEEE Internet of Things Journal 5.3 (2017): 1606-1615, https://doi.org/10.1109/JIOT.2017.2787800

[38]. Esfahani, Alireza, et al. "A lightweight authentication mechanism for M2M communications in industrial IoT environment." IEEE Internet of Things Journal 6.1 (2017): 288-296, https://doi.org/10.1109/JIOT.2017.2737630

[39]. Xiong Li, et al. "A robust ECC-based provable secure authentication protocol with privacy preserving for industrial Internet of Things." IEEE Transactions on Industrial Informatics 14.8 (2017): 3599-3609, https://doi.org/10.1109/TII.2017.2773666

[40]. Paliwal, Swapnil. "Hash-based conditional privacy preserving authentication and key exchange protocol suitable for industrial internet of things." IEEE Access 7 (2019): 136073-136093, https://doi.org/10.1109/ACCESS.2019.2941701

[41]. Chang, Chin-Chen, and Hai-Duong Le. "A provably secure, efficient, and flexible authentication scheme for ad hoc wireless sensor networks." IEEE Transactions on wireless communications 15.1 (2015): 357-366, https://doi.org/10.1109/TWC.2015.2473165

[42]. Gope, Prosanta, et al. "Lightweight and physically secure anonymous mutual authentication protocol for real-time data access in industrial wireless sensor networks." IEEE transactions on industrial informatics 15.9 (2019): 4957-4968, https://doi.org/10.1109/TII.2019.2895030

[43]. Sun, Yuanyuan, et al. "When machine learning meets privacy in 6G: A survey." IEEE Communications Surveys & Tutorials 22.4 (2020): 2694-2724, https://doi.org/10.1109/COMST.2020.3011561

[44]. Shakiba-Herfeh, Mahdi, Arsenia Chorti, and H. Vincent Poor. "Physical layer security: Authentication, integrity, and confidentiality." Physical layer security (2021): 129-150, https://doi.org/10.1007/978-3-030-55366-1_6

[45]. Ahmed, Mohammed Imtyaz, and Govindaraj Kannan. "Secure and lightweight privacy preserving Internet of things integration for remote patient monitoring." Journal of King Saud University-Computer and Information Sciences 34.9 (2022): 6895-6908, https://doi.org/10.1016/j.jksuci.2021.07.016

[46]. Chiu, Wei-Yang, Weizhi Meng, and Chunpeng Ge. "NoSneaky: A Blockchain-Based Execution Integrity Protection Scheme in Industry 4.0." IEEE Transactions on Industrial Informatics (2022), https://doi.org/10.1109/TII.2022.3215606

[47]. Luo, Xi, et al. "A lightweight privacy-preserving communication protocol for heterogeneous IoT environment." IEEE Access 8 (2020): 67192-67204, https://doi.org/10.1109/ACCESS.2020.2978525

[48]. Almaiah, Mohammed Amin, et al. "A lightweight hybrid deep learning privacy preserving model for FC-based industrial internet of medical things." Sensors 22.6 (2022): 2112, https://doi.org/10.3390/s22062112

[49]. Osorio, Diana Pamela Moya, et al. "Towards 6G-enabled internet of vehicles: Security and privacy." IEEE Open Journal of the Communications Society 3 (2022): 82-105, https://doi.org/10.1109/OJCOMS.2022.3143098

[50]. Wang, Ding, Wenting Li, and Ping Wang. "Measuring two-factor authentication schemes for real-time data access in industrial wireless sensor networks." IEEE Transactions on Industrial Informatics 14.9 (2018): 4081-4092, https://doi.org/10.1109/TII.2018.2834351

[51]. Sooriakumaran, Prasanna, et al. "A multinational, multi-institutional study comparing positive surgical margin rates among 22 393 open, laparoscopic, and robot-assisted radical prostatectomy patients." European urology 66.3 (2014): 450-456, https://doi.org/10.1016/j.eururo.2013.11.018