Applied Mathematics & Information Sciences
An International Journal

http://dx.doi.org/10.18576/amis/170602

Authentication Solutions in Industrial Internet of Things: A Survey

*Noura S. Aldossary and Rachid Zagrouba**

SAUDI ARAMCO Cybersecurity Chair, College of Computer Science and Information Technology, Imam Abdulrahman Bin Faisal University, P.O. Box 1982, Dammam 31441, Saudi Arabia

Received: 1 Dec. 2022, Revised: 11 Feb. 2023, Accepted: 15 Feb. 2023
Published online: 1 Nov. 2023

Abstract: With the rapid growth of industry 4.0, the Industrial Internet of Things (IIoT) is considered to be a promising solution for converting normal operations to 'smart' operations in industrial sectors and systems. The well-known characteristics of IIoT has greatly improved the productivity and quality of many industrial sectors. IIoT allows the connectivity of many industrial smart devices such as, sensors, actuators and gateways. The connectivity feature makes this critical environment vulnerable to various cybersecurity attacks. Subsequently, maintaining the security of IIoT sys-tems remains a challenge to ensure their success. In particular, authenticating the connected IIoT devices is a must to ensure that they can be trusted and prevent any malicious attempts. Hence, the objective of this survey is to overview, discuss and analyze the different solutions related to de-vice authentication in the domain of IIoT. Also, we analyze the IIoT environment in terms of characteristics, architecture and security requirements. Similarly, we highlight the role of (machine-to-machine) M2M communication in IIoT. We further contribute to this survey by outlining several open issues that must be considered when designing authentication schemes for IIoT. Fi-nally, we highlight a number of research directions and open challenges.

Keywords: IIoT; M2M Communication; Authentication, Industry 4.0, Cybersecurity

1 Introduction

The expansion and use of the Internet of Things (IoT) in modern life have given humanity a more sophisticated existence. An IoT system is comprised of a huge collection of interconnected smart nodes that gather and exchange information about their surrounding environment without human intervention. Examples of these smart devices are sensors, actuators and smart meters[1]. The Statistica report estimates that there will be around 75 billion connected devices worldwide in 2025 [2]. IoT can be found in every domain of our daily lives, such as health, agriculture and transportation. One well-known domain that utilizes' IoT technology is the industrial domain.

An extension of IoT is the Industrial Internet of Things (IIoT). It includes similar features of IoT like inter-connectivity and saving human effort. However, it varies in its utilization, the IIoT is deployed for industrial reasons such as the manufacturing domain, product optimization and other management systems, whereas IoT systems are primarily used for consumer services like fitness trackers and smart phones. IIoT depends on machine-to-machine (M2M) communication between devices, as it plays a major role in active monitoring and control. The benefits of utilizing IIoT include high flexibility and low maintenance costs while offering new services to manufacturers.

On the other hand, the adoption of IIoT introduces severe security risks. Such risks arise due to the missing or lack of essential security features. For instance, successful attacks targeting availability or operational safety in industries can be catastrophic. The 2015 Ukraine power utility attack is a prominent example[3]. In fact, depending on the targeted facility, outages might impact not only a single business but also customers, suppliers, or even a nation's vital infrastructure. Hence, security is a major requirement in IIoT environment.

Among the many security needs for IIoT, authentication is of particular importance. In an IIoT system, authentication is primarily used to manage the identification of communicating devices validate their identities. Hence, authentication between communicating entities in M2M setup is crucial as it countermeasures various cybersecurity risks[4]. Due to the resource

* Corresponding author e-mail: rmzagrouba@iau.edu.sa

© 2023 NSP
Natural Sciences Publishing Cor.

constrained nature of IIoT, it is important to adopt a lightweight authentication mechanism. So, this paper provides a thorough overview of authentication solutions in IIoT.

2 Background

2.1 IIoT

The industrial internet of things, or IIoT, is an environment where industrial smart nodes are connected through communication software and operate collaboratively to achieve a complex industrial task all without human intervention. Another definition of IIoT is, a system that is comprised of interconnected industrial smart nodes, cyber-physical assets and optional edge or cloud computing technologies[5]. These industrial smart devices can collect, monitor, exchange and analyze huge amounts of real time data within the industrial environment and act upon the generated information to enhance the overall production value. This value includes but not limited to; enhancing productivity, reducing consumption of energy and enhancing product quality.

As the popularity of IIoT increased, the benefits they introduced to manufacturing plants aided in the development of industry 4.0. To be specific, Industry 4.0 at a manufacturing plant operates on one basic principle: to combine numerous machines, companies and facilities, to develop a unified chain. This unified chain can benefit from optimizing and automizing operations. However, in order to take advantage of the various opportunities that are present in IIoT and industry 4.0, companies must make major changes in every aspect of their business. The first pre-request in order to adopt such technologies is to transform the business to function seamlessly in a digital world[6].

IIoT will potentially make a paradigm shift in the entire industry. To illustrate, a German manufacturing company, which was involved in Industrial Internet Consortium (IIC) is currently tracking the position of expensive power tools so that these tools can be configured remotely with the right parameters. On a wider scale, in the oil and gas industry, pipeline monitoring and early detection of leaks can prevent hazardous incidents from occurring. IIoT

2.1.1 Industry 4.0

In 2011, the industry 4.0 or “industrie 4.0” was proposed in the context of advancing the German economy[7]. There are several key technological enablers which drive industry 4.0, namely; IIoT, big data, artificial intelligence, robotics and machine learning. This revolution would result in a highly autonomous and dynamic production network with the goal of increasing industrial efficiency and transparency. The computerization of industrial processes is going to be met through the utilization of cyber-physical systems (CPS); thus, allowing the interconnected entities to behave as smart devices and autonomously achieve a common goal[8].

2.1.2 IIoT characteristics

Primarily, based on the relationship between IoT and IIoT, characteristics present in IoT are no different than those present in IIoT. Main characteristics can be identified as follows[9]:

- **Heterogeneity:** IoT devices use diverse set of protocols, different architectural designs and a wide range of specifications. Mostly, they can communicate with different devices and platforms through networks. However, the heterogeneous nature of these devices caused an absence of common security features[10].
- **Resource limitations:** IoT devices have limited computational, communicational and storage capabilities. Therefore, in order to increase system efficiency, algorithms should be designed to be simple and lightweight.
- **Connectivity:** connectivity is a default characteristic of IoT which allows both accessibility and compatibility. Accessibility is achieved by entering the network, whereas compatibility contributes towards the common capability to consume and produce data.
- **Real-time processing:** IoT systems produce huge amounts of data, effectively processing these data is essential to provide efficient systems.
- **Scalability:** is a system’s capacity to adapt to changing circumstances and meet future demands. which entails expanding the network to accommodate the growing number of hardware devices and software units on the network, as well as vertical scalability, which has to do with the capacity to improve the performance of current software or hardware by utilizing more resources[11].

2.1.3 IIoT architecture

There is no fixed standards in the establishment of IoT infrastructure; indeed it is based on the application or domain used. Primarily, the three-layer hierarchial architecture is utilized to start a basic communication among devices in IIoT. The three layers are namely; perception, network and application layer. The additional support layer is mainly used for the exchange of information and implementation of data control procedures.

© 2023 NSP
Natural Sciences Publishing Cor.

The five-layer architecture is comprised of an extra business layer intended to manage the whole system[1]. As demonstrated in figure 1, the first layer contains physical components, the second layer contains communication nodes, the support layer includes storage units, and the fourth layer is the interactive layer. Below is a detailed description of each layer[12].

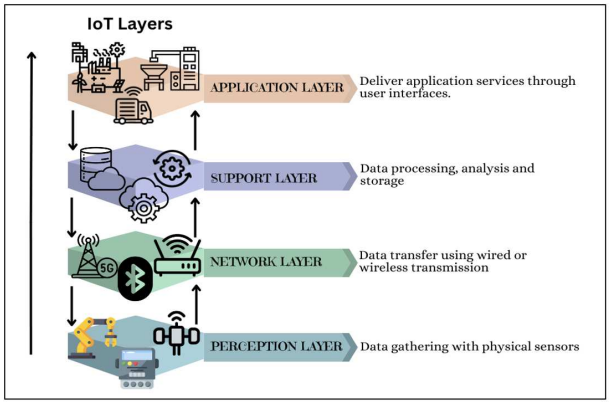

Fig. 1: Architecture of IIoT.

–**Perception layer:** also referred to as the physical layer. Its main responsibility is to sense and collect data about the surrounding IIoT environment. This is done with the help of different technologies such as Radio frequency identification (RFID), GPS and wireless sensor networks (WSN). However, this layer is very sensitive, which makes it vulnerable to malicious attacks. Also, this layer suffers from limitations in terms of computation and energy, which affects the efficiency of the entire system.

–**Network layer:** also referred to as transmission layer. It is responsible for connecting network devices, smart things and networks to each other. It carries the information collected through sensors to the support layer. Either a wired or wireless trans-mission method, such as 3G, 5G, WiFi, ZigBee, and Bluetooth, can be used. The main challenge in this layer is maintaining a high-reliability link for secure communication between devices.

–**Support layer:** also referred to as middle ware layer. To increase the three-layer architecture security and protect against threats, an additional support has been proposed to eliminate any unnecessary information and extracts the useful information. Which contributes to enhancing the overall system performance. Also, it implements big data processing modules and cloud computing. Thus, making it vulnerable to security issues related to the cloud.

–**Application layer:** also referred to as the service layer. It depends on the data gathered by the perception layer and the communication established by the network layer. It acts as an intermediary between the end user and the connected device. Application layer may advance, dependent on software, with minor or no change to other layers. Thus, securing this layer is challenging as software modifications introduce new weaknesses.

In 2017, the Industrial Internet Consortium (IIC) introduced a working IIoT frame-work; it is referred to as Industrial Internet Reference Architecture (IIR). It is used as an architectural standard for most IIoT systems. As demonstrated in figure 2, The architecture is comprised of three principal tiers[13]:

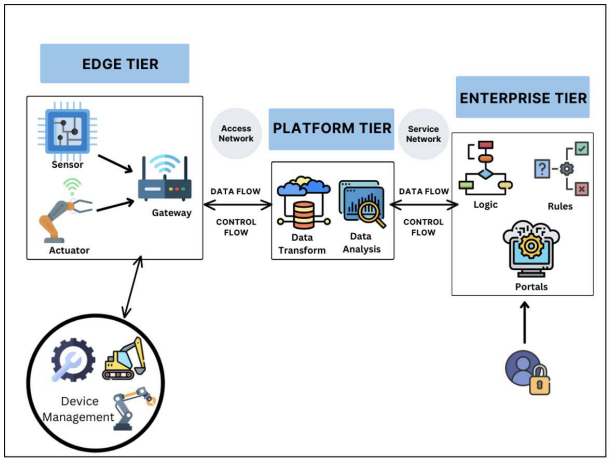

Fig. 2: Three-layered IIR Architecture.

–**Edge tier:** it is responsible for collecting data from edge nodes and forwards it to the information domain.

–Platform tier: it is responsible for analyzing the data coming from the Edge layer to upper layers.

–**Enterprise tier:** it is responsible for hosting particular applications (e.g. end-user interfaces) among others. Also, it creates control commands to be forwarded to the Platform and Edge layers.

2.1.4 IIoT security requirements

As an essential step towards having a secured and trusted IIoT system, we have to outline and discuss the major security goals for IIoT operation which are the following[14]:

–**Access control:** only a suitable access control mechanism will enable IIoT nodes to communicate securely. This is accomplished through authentication and authorization as well as some data policies.

© 2023 NSP
Natural Sciences Publishing Cor.

–**Authentication:** the initial step in securing any system is to authenticate legitimate identities and build a trust-based communication among the sharing environment. Verifying the identity of IIoT devices is crucial to prevent unauthorized access to the system.
–**Authorization:** the process of permitting legitimate nodes access to different re-sources based on rules or conditions.

Confidentiality, Integrity and Availability (CIA triad) are the three foundational principles of information security[15].

–**Confidentiality:** ensuring that IIoT nodes are protected from unauthorized disclosure and access. Usually, maintaining this property is done by converting data into unreadable format with the help of cryptographic algorithms.
–**Integrity:** ensuring that data transferred between IIoT nodes is accurate and has not been misused or tampered with.
–**Availability:** ensures that resources are always accessible and available. In IIoT, disruption in production and threats to safety measures can be done through many denial-of-service (DoS) attack techniques.

2.2 Machine-to-machine (M2M) communication

Machine-to-machine communication (M2M), also referred to as Machine-type-communication, implies communications between a huge number of cooperating nodes that exchange sensed data and make decisions with minimal to no human interference. Currently, there are 5 billion M2M nodes have been connected to wireless networks, and according to estimates from Cisco and Ericson, that number will increase up to 500 billion by the end of the decade[16].

2.2.1 M2M architecture

From a functional perspective, the general architecture of M2M communication consists of three fundamental interconnected domains which are the following[17]:

–**M2M domain:** it contains a set of devices that are utilized for running the M2M applications. A variety of these devices are equipped with built-in sensors to detect changes, while other devices only consist of storage capabilities. M2M devices are able to exchange the senses, the connectivity between these devices is achieved through a small area network (e.g. ZigBee, WiFi, Bluetooth) for forwarding and receiving data to or from the network domain.

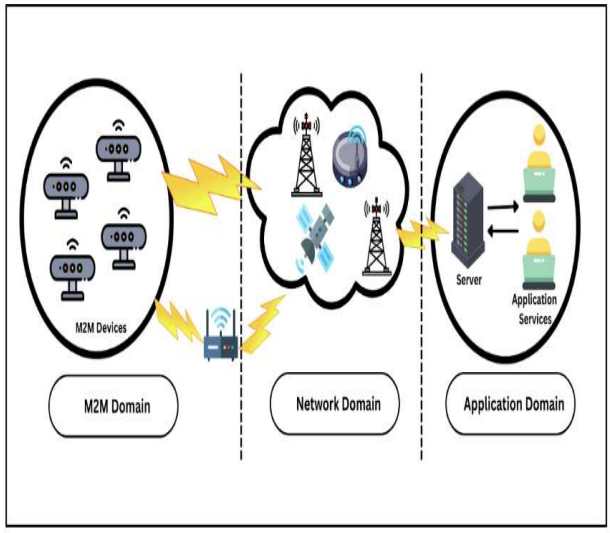

Fig. 3: M2M Communication Architecture.

–**Network domain:** it contains an array of heterogeneous network devices allowing the M2M domain and application domain to communicate. The access technology utilized by this domain includes, but not limited to, WLAN, Ethernet, UTRAN and 3G.
–**Application domain:** it contains the remote servers which are responsible for storing the data collected by the M2M devices or other network nodes. The data is then made available to authorized users through an application. These applications in turn allow remote monitoring, remote sensing and remote control of data.

2.2.2 M2M in IIoT

Multiple industrial processes are interconnected using intelligent devices thanks to IIoT and M2M connections. This setup produces and compiles valuable industrial data. These concepts are brought to the industry via the Industrial Internet Consortium and Industry 4.0, which also concentrate on integrating various production processes with cutting-edge internet-based analytical and computational capabilities. For example, Avent SmartEdge is an IIoT gateway that connects smart devices to the cloud. Using a completely customized online interface from any place with access to the internet, one may check the connected devices' status and manage them[18].

3 Literature review

Authentication Using Cryptography in IIoT Environment.

© 2023 NSP
Natural Sciences Publishing Cor.

• Symmetric-based approaches

Currently, cryptography is a fundamental fragment of authentication, and many cryptography approaches provide a good opportunity to enhance the security of IIoT. Symmetric-based authentications commonly uses hash functions and Exclusive OR (XOR) operations, which are considered efficient for resource constrained IIoT devices[19]. Several approaches utilize hash and XOR operations for authentication. Authors in[20], proposed a simple machine-to-machine authentication protocol based on XOR and hash operations for IIoT environment. The proposed solution is comprised of two main steps; a) registration step, where the smart sensor register itself to the Authentication Server (AS) and secure pre-shared keys created by the AS are sent to each router, b) authentication step, where the sensor authenticates itself to the router achieving mutual authentication. Although their proposed protocol is suitable for the constrained nature of IIoT environment, many weaknesses have been identified in the protocol[21]. Authors in [22], inspired by [20], introduced a Lightweight Authentication and Key Distribution (LAKD) protocol for resource-constrained IIoT devices. The protocol is designed for M2M communication based on four simple operations namely; XOR, Hash function, and addition, and subtraction. There are mainly two phases in the proposed protocol, which are registration and authentication. The sensor and gateway exchange secret values during the registration phase in order to prove their identities during the authentication phase. In the authentication phase, the sensor and gateway recognize each other to build confidence in each other's identities and generate a session key. Also, only four messages are needed to be exchanged between entities to achieve successful mutual authentication and key distribution mechanism. The LAKD protocol provides better security as compared to [16]. However, it is still computationally limited due to the additional hash operation in the sensor node.

Similarly, in [23], authors proposed an efficient authentication mechanism for establishing secure communication between IIoT devices. The proposed scheme uses lightweight operations (e.g. Hash and XOR) to perform authentication between the smart sensor and the router. The two phases comprised of registration and authentication achieve mutual authentication by establishing a secure communication between the two entities. However, there are several limitations regarding authentication of sensor and router in their proposed scheme. Authors in [24], introduces SLAP, a secure and lightweight authentication protocol for M2M communication. They utilized symmetric cryptographic operations, which are XOR and Hash operations, for developing the proposed authentication scheme.

Also, the two phased authentication scheme produces a shared secret key after just two cycles of interaction and achieves mutual authentication without the need of any human interference. Yet, the scheme suffers from potential key escrow problem, which can be fixed by regulating the centralized authority used for the registration phase through government entities and enforcing strict laws. In [25], a single-factor lightweight authentication protocol (SF-LAP) for machine-to-machine communication in IIoT systems is introduces. The protocol offers a secure method for conversation by using XOR an Hash operation, this guarantees that the communication between sensor and controller is secured. Also, it protects the connection using a time stamp technique and a secure pre-shared key.

Finally, to verify the security of the proposed protocol, Burrows Abadi Needham (BAN) and Gong, Nedham and Yahalom (GNY) logics were used. The formal verification is conducted using AVISPA tool to ensure the suggested protocol is secure. Authors in [26], proposed a PUF-based efficient authentication and session establishment protocol (PEASE) for M2M communication in IIoT. Only lightweight XOR and hash operations are used for authentication. The proposed solution does not demand any clock synchronization between devices, and it overcomes the scenario where the authentication step must utilize a fuzzy extractor of high computational complexity resulting from PUF noise. This is achieved by not reusing the similar challenge in the authentication phase. It comprises of two message exchanges, which ensures security and availability while maintaining lightweight capability.

The protocol is comprised of four phases namely; registration, initialization, authentication and device log-out phases. In the registration phase, both the device and supervisor exchange secrets, if no exception is encountered, this step is performed only once in the entire lifecycle of the device. Then, in the initialization phase, the device and supervisor (e.g. gateway) will authenticate one another and share a key for secure communication during the session. Finally, in the device log-out phase, the supervisor will receive a log-out request from the device, records the event, and delete the matching data entry from the device table. The CPN tools have been used for security modeling and verification. In [27], authors proposed an authentication protocol for IIoT devices in WSN networks. In their protocol, only XOR, hash, and symmetric operations have been used for the authentication process. In addition, they introduce PUFs and bloom filters to store and search challenge/response pairs. The proposed protocol functions are based on several steps. First, the cloud server has wireless sensors and gateways registered and stored. Then, pre-authentication is conducted between gateway and cloud server and the connection is maintained by the gateway. Lastly, the identity information (challenge) is sent to the gateway by the sensor device. The gateway in turn requests for the response value from the cloud server in equivalent challenge/response sets. The gateway authenticates itself to the sensor using the response value. Figure 2 demonstrates the protocol communication flow.

© 2023 NSP
Natural Sciences Publishing Cor.

• Asymmetric-based approaches

Authors in [28], proposed privacy preserving scheme to ensure authenticity in heterogeneous IIoT systems. They developed a novel authentication scheme over a multicryptosystem (ASMC), equivalent to two distinct scenarios, respectively, neigh-boring nodes utilizing the same cryptographic approach and the mixture of diverse cryptosystem nodes. The ASMC scheme supports various cryptographic systems such as RSA, ECC, DL and lattice-based. Also, privacy was achieved by using ring signature design to construct the proposed scheme. Moreover, the proposed scheme considers cloud data centers for authenticity and privacy of IIoT devices. Authors assumed that public and private keys in addition to different system parameters had been stored in the devices prior to their deployment. After their successful deployment, the devices will gather the data and transfer it to the cloud data centers. Yet, their scheme is based on different public key cryptographic approaches, which is not efficient for IIoT environment. In addition, random oracle model was used to ensure the unforgetability and privacy features of the suggested model. Authors in [29], proposed a cross-domain device authentication scheme for 5G IIoT. The scheme is comprised of two coupled components to achieve both authentication and privacy during initial access. Firstly, device authentication is achieved by implementing probabilistic preamble coding to randomize, hash and encrypt preamble values and distribute them across different layers. This approach will easily expose the preamble information to eavesdroppers. Therefore, to tackle this issue, they developed a privacy preserving protocol by randomly encrypting preamble sequence after coding and prior to transmission at every IIoT device. The one- dimensional quantum walk is utilized by the protocol to enhance the privacy level in the authentication system. However, no security analysis has been made to measure the protocol's security against well-known attacks.

Authentication using blockchain in IIoT environment.

Many works have utilized blockchain technology for authentication in the IIoT environment. The proposed privacy preserving authentication protocol in [30], utilizes blockchain technology in combination with multifactor authentication for cross-domain IIoT systems. They used physically unclonable functions (PUFs) to develop a multifactor key derivation mechanism, which avoids the likelihood loss of factor attack as well as ensuring several components at the server side are secured. Also, in order to gather derived keys for IIoT nodes, leveraged on-chain dynamic accumulator. This allows the blockchain to only store the accumulator of each domain, eliminating the need of directly registering a huge amount of device keys, thus resulting in a major reduction in storage overhead. Also, incorporating the on-chain accumulator with cross-domain device authentication will satisfy privacy preservation requirements. The formal security analysis has been carried out using BAN logic and a proof-of-concept prototype has been conducted to evaluate the performance. In [31], the authors introduced Authenblue, a block-chain-based authentication protocol for sensors, nodes and coordinators in IIoT domain. The proposed protocol intends to improve the authentication procedure in BCTrust protocol by improving the method of collecting unique identifiers (UI). In the inception step, the values of the UI switched from being fixed values, MAC addresses, to be generated values. Such enhancement is essential for the key management process. Also, the proposed protocol is intended to be implemented in Zigbee-based WSN environment. The authors simulated several components of the protocol by using NS3 tool to demonstrate its performance. The proposed solution in[32], utilize Blockchain technology to authenticate devices in cross-domain IIoT. The efficient blockchain-assisted secure device authentication mechanism (BASA) constructs trust between untrusted entities rather than placing trust in a third-party. It adopts the consortium blockchain as a trusted platform to share domain specific information. Also, identity-based signature (IBS) is utilized throughout the authentication process. In case of privacy compromising, the public key of an entity can be revoked easily because of the flexibility of the identity management method. Also, according to the design, entities can be authenticated anonymously by those in a different domain. The security and efficiency of BASA has been evaluated to during the performance analysis. Also, authors in[33], introduced a distributed ledger-based authentication architecture. The proposed architecture combines Secure Multi-Party Computation (SMPC) and Distributed Ledger Technology to identify malicious attacks and sensors in the IIoT environment. The decentralized architecture of the pro-posed architecture ensures authenticity and integrity of the IIoT nodes utilizing private blockchain and master nodes administering the rules set by the administrator. The overall objective is to provide a plug-and-play layer of security above the existing IIoT.

Authenticating using other technologies in IIoT environment.

Authors in [34], introduced a lightweight fingerprint-based device authentication scheme for the industrial domain. Ultra-wide band (UWB) signals are utilized while performing the authentication process. The authentication scheme is comprised of sensor to monitor industrial processes, anchors to capture the wireless signal's fingerprint, as well as a lightweight architecture for authenticating devices. As shown in figure 1, the actual physical location of the industrial node is represented as the fingerprint, this fingerprint can be approximately estimated using time difference of arrival (TDOA) technique. Based on the fingerprint, a trusted zone is built and utilized by the authentication scheme for authenticating all wireless packets. At last, a simulation

© 2023 NSP
Natural Sciences Publishing Cor.

of the experiments has been done to show the competence of the proposed scheme. However, no formal/informal security analysis has been made to evaluate the security of the proposed scheme against state-of-the-art attacks. The proposed scheme in [35], adopted Merkle hash tree approach to conduct multiple entries after a single authentication and group signature technology to ensure anonymous authentication between IIoT devices and servers. Also, the one-authentication-multiple-access paradigm has been utilized to allow each valid device to access the server several times after one authentication. their scheme is comprised of IIoT devices, servers and a gateway. IIoT devices are equipped with PUFs to create their own private keys. In addition, servers provide services to authorized devices. Similarly, the responsibility of the gateway is to issue certificates for the IIoT devices. Whenever an IIoT device asks to enter a group administered by a particular gateway, the gateway needs to create a group certificate for that device as well as add the device's identity to the identity list. Although they obtained results that have demonstrated the efficiency in communication and authentication time. Yet, the scalability and security of the proposed scheme remain a concern.

sectionComparison and analysis

Although solutions related to device authentication in IIoT are still in its initial stage, the discussed works demonstrated the ability of different approaches to overcome the challenges present in the IIoT environment. Mainly, all reviewed papers considered M2M communications in IIoT systems. Table 1 shows a comparison between works that address machine to machine authentication in IIoT. The comparison is done based on the following metrics: Approach, O&G, attack, security feature, lightweight, delay, overhead, scalability and cost.

In IIoT environment, several approaches can be utilized to perform authentication between smart devices. It is noticeable that most works [10,12,14–16,22, 24] adopted symmetric cryptographic approaches for authentication in IIoT. Works in [20,22–25] used simple XOR and Hash operations only, while works in [26,27] utilized additional hardware namely; physical unclonable functions (PUFs). PUFs are considered a type of lightweight and cost-effective hardware with embedded security primitives[36]. They exploit the unique characteristics of the device which is known as hardware fingerprinting technology. Also, they are well known with their uniqueness and unpredictability features. Also, it has recently been adopted by many IIoT schemes for secure key storage and agreement[37,38]. In addition, asymmetric cryptographic approaches, also referred to as public key techniques, recently gained attention [28,29].

Also, works in [17,18,19,20] utilized Blockchain technology for authentication in IIoT. Blockchain is a distributed database which is commonly shared among all nodes in the network. The utilization of blockchain technology in the domain of cryptocurrencies (e.g. Bitcoin) has become prominent for its role in maintaining a private and decentralized ledger of transactions. As a result of utilizing blockchain, different entities can be verified without the dependency on a third party for authentication. When information is added to a public ledger, it cannot be changed[39]. Hence, combining Blockchain technology and IIoT has multiple advantages such as decentralization, identity anonymity and removal of third-part verification.

In addition, characteristics of Ultra Wide Band (UWB) signals [34] are used for authentication in IIoT. Although they proposed a well-designed scheme, Non-line-of-Sight (NLOS) transmission still remains an obstacle for communication between tags and anchors. Other technologies like Markle hash tree and group signature [35] have been used as well. Moving further with network overhead, authors of all reviewed papers have done performance analysis of their schemes. They performed comparisons of their proposed schemes with similar solutions in terms of computation and communication complexity as well as energy consumption. The authors concluded that the proposed schemes resulted in better performance as compared to other solutions. the most commonly used performance features based on the literature are communication, computation and memory. It is noticed that reference [27] standout the rest with 0.0224ms in terms of low computational cost. However, the scheme achieved high communication cost with a result of 2688 bits due to the utilization of continuous authentication[40]. Furthermore, the lowest communication cost and memory consumption is achieved in reference [20] with 1024 bits and 768 bits respectively. It is noticed that references [25,28,29,31,35] did not perform any comprehensive evaluation based on the metrics listed in table 1. It is important to note that all proposed works [20,22–25,27–35] excluding [26] show that there is a lack of scalability in their solutions, this limitation reduces the availability of the proposed schemes.

Regarding security validation tools, there is a wide range of tools and techniques for validating the security aspects of authentication protocols. Works in [10,12,24,17,14,15] used The Automated Validation of Security Applications and Protocols (AVISPA) which is commonly used for such intention. It depends on a modular, expressive and formal language to analyze protocol security features automatically. In addition, Burrows–Abadi– Needham (BAN), which is a comprised of a collection of rules to test protocols against predefined security features[41], has been utilized by works in [10,14,15,23]. Also, authors in [22] used Colored Petri Net (CPN) tool to analyze the security performance of their scheme. It is used to simulate and analyze colored Petri Nets[42]. In addition, To simulate the hash function and display all feasible hash values, Random Oracle Model (ROM) has been used by [23]. The ROM be queried for the hash value by all entities, whether they are valid or not. It provides strong security validation for

© 2023 NSP
Natural Sciences Publishing Cor.

Table 1: Evaluation comparison of IIoT device authentication schemes.

Ref	Year of Pub.	Approach	O&G	Lightweight	Network overhead			Scalability	Cost	Security validation	Limitation
					Communication	Computation	Memory				
[26]	2022	Symmetric Cryptographic Operations, PUF	No	Yes	1536 bits	0.39 ms	-	High	Low	Informal, CPN tools	Does not consider Peer-to-peer (P2P) communication
[25]	2022	Symmetric Cryptographic Operations	No	Yes	-	-	-	Low	Low	Informal, AVISPA, BAN and GYN logic	Limited scalability
[29]	2022	Quantum Cryptography	No	No	-	-	-	Low	High	Informal	High complexity of operations
[35]	2022	Group signature, Merkle hash tree	No	No	1408 bits	0.0068 ms	-	Low	Low	Informal, ROM, BAN logic	Limited scalability
[27]	2022	Symmetric Cryptographic Operations, PUF, Bloom filters	No	No	High 2688 bits	0.0224 ms	-	Low	High	Informal, AVISPA	High network overhead
[24]	2022	Symmetric Cryptographic Operations	No	Yes	Low 1184 bits	0.277 ms	-	Low	Low	Informal, AVISPA	Key escrow problem
[30]	2022	Blockchain	No	No	-	2577.28 ms	-	Low	High	AVISPA	High network overhead
[28]	2022	Asymmetric Multi-Cryptosystem	No	No	-	-	-	Low	Low	Informal	High network overhead
[31]	2020	Blockchain	No	Yes	-	-	-	Low	High	-	No security analysis against attacks
[23]	2020	Symmetric Cryptographic Operations	No	Yes	1024 bits	0.0657 ms	896 bits	Low	Low	AVISPA, BAN logic	Authentication is limited between sensor and router
[32]	2020	Blockchain	No	No	1536 bytes	362.629 ms	-	Low	High	Informal	High network overhead, high latency
[33]	2020	Blockchain	No	No	-	6464 ms	-	Low	High	Informal	High network overhead
[22]	2020	Symmetric Cryptographic Operations	No	Yes	1536 bits	0.296 ms	-	Low	Low	Informal, AVISPA, BAN logic	Vulnerable to to desynchronization attack
[34]	2019	UWB	No	Yes	-	-	-	Low	Low	-	No security analysis of proposed scheme
[20]	2017	Symmetric Cryptographic Operations	No	Yes	1024 bits	0.0548ms	768 bits	Low	Low	Informal	Low security

© 2023 NSP
Natural Sciences Publishing Cor.

cryptographic-based schemes. It is observed that, Refs. [18, 21] did not conducted any security analysis for their proposed schemes.

Moving towards IIoT authentication attacks, Table 2 demonstrates the various attacks against which the discussed protocols for IIoT are resistant. Only the protocols that the authors' formal and informal security analyses were performed on are listed in the table, along with highlighting the attacks that their suggested solutions are resistant to. A list of attacks is included in the table, along with an annotation indicating if the tested protocol is resistant to each attack. We only include the commonly discussed attacks. The attacks that appeared once (e.g. physical attacks) are included under the others column. The (✓) mark shows that the authors have illustrated the immunity of their proposed scheme to an attack. The (-) mark shows that the protocol has not been validated to be exposed to attack.

We observed that reply attacks, man-in-the-middle (MITM) attacks and impersonation attacks were the most frequently tested attacks in IIoT environment. This indicates that they are considered to be amongst the dangerous attacks targeting IIoT environments. Besides, an imposter can merge different approaches when conducting an attack. An imposter can intercept and sniff traffic then re-transmit it to assure the recipient to take specific actions. The attack outcome depends mainly on the imposter's skills, knowledge, and weakness of the targeted environment. Confidential information loss is among the most catastrophic results of an impostor. The use of timestamps for messages and one-time session keys when during communication are countermeasures against this sort of impostor behavior.

Table 3 summarizes the security features of the discussed protocols. Additionally, we only listed the protocols in this table for which the authors conducted formal and informal security analysis, emphasizing the security features that their schemes offer. Also, the (✓) indicates that the proposed protocol fulfills the security features. The (-) indicates that the proposed protocol did not provide any information about the assurance of ownership. The analysis demonstrated that anonymity, mutual authentication and session key agreement are the most desirable security features.

General table / for all criteria (cost, strengths, weaknesses, scalability, overhead approach, year of publication).

4 Gap analysis

The number of IIoT devices and their integrated applications are increasing rapidly. These nodes are inter-connected with full autonomy and with no human intervention. In the IIoT domain, authentication is an essential requirement which substantially defines the success or failure of securing these inter-connected systems. Based on the conducted survey study, there are several appealing authentication solutions for M2M setups in IIoT that have been introduced. However, there are some of these works that still have limitations in terms of security and design.

There are several related works that have security issues, design flaws and considerably high overhead. Authors in [21] identified that the work proposed by [20] lacks resistance to impersonation, tampering and reply attacks. Also, the protocol in [22] is said to outperform [20] in terms of security strength and design architecture. But, it does not explicitly explain how synchronization is maintained between sensor and gateway, hence it is not able to avoid desynchronization attacks. Furthermore, works in [30–33] utilized blockchain to defeat the problem of over-centralization. However, this significantly increases the computational overhead of the proposed protocols. Similarly, [28,29] used quantum cryptographic solutions to strengthen the security of their proposed schemes. Nevertheless, this affects the performance pertaining to high levels of computational and communication costs, which makes such approaches not fit for the resource-constrained nature of IIoT environment.

In addition, as per the definition of protocol scalability described in [43], the proposed protocols in [20,22–25] lack scalability. That means the M2M communication between sensors and gateways possess a many-to-one relationship; due to the utilization of pseudonyms, the gateway does not attain a direct identity index, and cannot verify which device the message originated from, therefor it fails to discover the related calculation parameters; the succeeding calculations must traverse the whole client table and thoroughly perform the authentication process one by one. This limitation makes the performance analysis insignificant because of the unidentified cost of exhaustive search.

To address the above limitations, we will propose a solution based on biometrics to address the existing gaps in recent schemes in order to become more lightweight, reduce the computational efforts and ensure scalability to be more suitable for the domain of IIoT.

5 Finding

To sum up the reviewed schemes, authentication is a vital process for communication in IIoT environments. The process is comprised of confirming the identity of communication entities. During the authentication process, one or more features may be utilized. Adding additional features will only increase the safety of the entire process. Besides, the use of passwords alone for authentication may result in weak security. An imposter can crack or intercept passwords. Thus, a better approach is to utilize biometrics to avoid impersonation or spoofing attacks.

Authentication is exposed to frauds and deceptive users. Imposters can carry out attacks to steal confidential

© 2023 NSP
Natural Sciences Publishing Cor.

Table 2: Comparison of authentication attacks in IIoT

Reference	Reply	MITM	Tracking	Offline identity guessing	Desynchronization	Eavesdropping	Impersonation	Modification	Injection	DoS	Known Session-specific Temporary Information	Key Disclosure	Compromised	Others
[20]	✓	✓	-	-	-	-	✓	✓	-	-	-	-	-	-
[22]	✓	✓	✓	✓	✓	-	✓	-	✓	✓	✓	✓	-	-
[23]	✓	✓	-	-	-	✓	✓	-	-	-	-	✓	-	-
[24]	✓	✓	✓	-	-	-	✓	✓	-	-	-	-	✓	-
[25]	✓	✓	✓	-	✓	✓	✓	✓	-	-	-	-	✓	-
[28]	-	-	-	-	-	-	-	-	-	-	-	-	-	✓
[29]	-	-	-	-	-	✓	-	-	-	-	-	-	-	✓
[26]	✓	✓	-	-	✓	-	-	-	-	✓	✓	✓	-	✓
[27]	-	✓	-	-	✓	-	-	✓	-	-	-	-	-	✓
[35]	-	-	-	-	-	✓	✓	-	-	-	-	-	-	✓
[30]	✓	-	-	-	✓	-	✓	-	-	-	-	-	-	✓

Table 3: Comparison of security features in IIoT

Reference	Privacy	Authenticity	Anonymity	Integrity	Unlikeability	Mutual Authentication	Forward Secrecy	Backward Secrecy	Confidentiality	Session Key Agreement
[20]	-	✓	-	-	-	✓	-	-	✓	✓
[22]	-	✓	-	✓	-	✓	✓	✓	✓	✓
[23]	-	✓	✓	-	✓	✓	-	-	-	✓
[24]	-	✓	✓	-	✓	✓	-	-	-	✓
[28]	✓	✓	✓	✓	-	-	-	-	-	-
[26]	-	✓	✓	-	✓	✓	✓	✓	✓	✓
[27]	-	✓	✓	-	✓	✓	✓	✓	-	-
[35]		✓	✓	-	-	-	-	-	-	-
[30]	✓	✓	✓	-	-	✓	✓	-	-	-
[32]	✓	✓	✓	-	-	✓	✓	-	-	✓

user or device information, disrupt the operation of different system elements, or cause an entire malfunction to the system. As mentioned earlier, the utmost serious attacks are reply attacks, impersonation attacks and MITM attacks as they may lead to loss of user or device data as well as compromising important security features. Similarly, desynchronization attack can be as dangerous as the previously mentioned attacks, this is because in IIoT environments, proper synchronization of data is essential for the whole system's function.

The use of session keys is a crucial part for securing communication, which are mainly used to encrypt it. To safeguard the communication against MITM or reply attacks, it is worth utilizing one time session keys, and utilizing timestamps for messages. As a result, the system can unmistakably determine whether the processed message was generated by a genuine network node or whether it was intercepted and retransmitted by an imposter.

Along with the security features, we should also consider scalability issues of protocols in IIoT environment.

© 2023 NSP
Natural Sciences Publishing Cor.

Devices used in IIoT are usually limited in terms of computing power. Thus, the calculations executed on IIoT devices while the device is running mustn't consume its energy. Therefore, it is worthwhile to use lightweight cryptographic algorithms when developing authentication protocols. Besides, this will guarantee an appropriate level of security without draining system resources. In contrast, data storage should be managed by centralized units, which have larger amounts hardware and computational resources than individual devices.

6 Conclusion

With the rising requirement of automation in various fields, IIoT have become an exceptional technology. This technology has fueled the transformation of the industrial sector to Smart Industry 4.0. As part of this transformation, various security concerns evolved. One major concern is related to authentication between IIoT devices. Therefore, this paper introduces a thorough analysis of authentication schemes for M2M communication in IIoT, as a result, a list of research directions and open challenges are outlined. In addition, security requirements and characteristics of IIoT have been discussed as well. After investigating the recent solutions in security schemes for IIoT, we highlight further research directions in this area.

Firstly, when designing protocols for IIoT, security is an important aspect to consider. An appropriate level of security should be provided during M2M communication as the techniques of bypassing security are becoming more sophisticated. Hence, research objectives in security protocols for the domain of IIoT should concentrate on technologies and solutions that offer better security. Also, security includes crucial components which are identity authentication and verification. These procedures should be carried out while considering at least two factors. Only utilizing passwords for authentication does not offer a high enough level of security. A good solution that is worth adopting is utilizing biometric techniques throughout these two procedures.

The second aspect to security in IIoT environment is performance. IIoT devices carry critical data and require high reliability of systems. The network overhead during communication between IIoT devices should be as low as possible. This will enable the devices to collaborate effectively and efficiently with no delays. Also, performing calculations in clouds or fog can contribute to achieve efficient bandwidth utilization and minimal transmission delays.

Lastly, scalability is a crucial aspect to give thought to. As IIoT is a key enabler for industry 4.0, it has become huge and highly distributed. Solutions for authentication must align with these advancements by enabling scalable approaches. Adding IIoT entities as needed without compromising the system's performance is referred to as a scalable approach.

After reviewing the present state-of-knowledge in the domain of protocols for IIoT environment, we draw ourselves future research objectives. In our next work, we will concentrate on designing and creating a secure device communication scheme to be employed in IIoT. We will include biometric features to distribute the session key and successfully achieve device authentication. Also, we will take security features into account while designing the scheme to maintain safety. We will also incorporate time stamps and one-time verification credentials to safeguard the environment from potential attacks.

Acknowledgement

We would like to thank SAUDI ARAMCO Cybersecurity Chair for funding this project.

References

[1] Sethi P, Sarangi SR. Internet of Things: Architectures, Protocols, and Applications. Journal of Electrical and Computer Engi-neering 2017;2017. https://doi.org/10.1155/2017/9324035.

[2] Global natural gas consumption 2021 — Statista n.d. https://www.statista.com/statistics/282717/global-natural-gas-consumption/ (accessed February 15, 2023).

[3] Whitehead DE, Owens K, Gammel D, Smith J. Ukraine cyber-induced power outage: Analysis and practical mitigation strategies. 70th Annual Conference for Protective Relay Engineers, CPRE 2017, Institute of Electrical and Electronics Engi-neers Inc.; 2017. https://doi.org/10.1109/CPRE.2017.8090056.

[4] Sukumaran RP, Benedict S. Authentication and Cryptography solutions for Industrial IoT-A Study. 6th International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud), I-SMAC 2022 - Proceedings 2022:76–81. https://doi.org/10.1109/I-SMAC55078.2022.9987278.

[5] Alabadi M, Habbal A, Wei X. Industrial Internet of Things: Requirements, Architecture, Challenges, and Future Research Di-rections. IEEE Access 2022;10:66374–400. https://doi.org/10.1109/ACCESS.2022.3185049.

[6] Gilchrist Alasdair. Industry 4.0: the industrial internet of things. Apress; 2016.

[7] Zhou K, Liu T, Zhou L. Industry 4.0: Towards future industrial opportunities and challenges. 2015 12th International Con-ference on Fuzzy Systems and Knowledge Discovery, FSKD 2015, Institute of Electrical and Electronics Engineers Inc.; 2016, p. 2147–52. https://doi.org/10.1109/FSKD.2015.7382284.

[8] Alladi T, Chamola V, Parizi RM, Choo KKR. Blockchain Applications for Industry 4.0 and Industrial IoT: A Review. IEEE Access 2019;7:176935–51. https://doi.org/10.1109/ACCESS.2019.2956748.

[9] Sisinni E, Saifullah A, Han S, Jennehag U, Gidlund M. Industrial internet of things: Challenges, opportunities, and directions. IEEE Trans Industr Inform 2018;14:4724–34. https://doi.org/10.1109/TII.2018.2852491.

© 2023 NSP
Natural Sciences Publishing Cor.

[10] ICT Platform Society, Han'guk Kwahak Kisul Chŏngbo Yŏn'guwŏn, Institution of Creative Research Professionals, Institute of Electrical and Electronics Engineers. Changwon Section, Institute of Electrical and Electronics Engineers. 2017 Interna-tional Conference on Platform Technology and Service (PlatCon-17): proceedings: 13-15 February 2017, Busan, Korea. n.d.

[11] Ottolini D, Zyrianoff I, Kamienski C. Interoperability and Scalability Trade-offs in Open IoT Platforms. Proceedings - IEEE Consumer Communications and Networking Conference, CCNC, Institute of Electrical and Electronics Engineers Inc.; 2022. https://doi.org/10.1109/CCNC49033.2022.9700622.

[12] Qiu T, Chi J, Zhou X, Ning Z, Atiquzzaman M, Wu DO. Edge Computing in Industrial Internet of Things: Architecture, Ad-vances and Challenges. IEEE Communications Surveys and Tutorials 2020;22:2462–88. https://doi.org/10.1109/COMST.2020.3009103.

[13] Burhan M, Rehman RA, Khan B, Kim BS. IoT elements, layered architectures and security issues: A comprehensive survey. Sensors (Switzerland) 2018;18:1–37. https://doi.org/10.3390/s18092796.

[14] Khan MA, Salah K. IoT security: Review, blockchain solutions, and open challenges. Future Generation Computer Systems 2018;82:395–411. https://doi.org/10.1016/j.future.2017.11.022.

[15] Fink GA, Zarzhitsky Di V., Carroll TE, Farquhar ED. Security and privacy grand challenges for the Internet of Things. 2015 International Conference on Collaboration Technologies and Systems, CTS 2015 2015:27–34. https://doi.org/10.1109/CTS.2015.7210391.

[16] Here's how we can build the future internet — WIRED UK n.d. https://www.wired.co.uk/article/bc/heres-how-we-can-build-the-future-internet (accessed June 5, 2023).

[17] El-Kader SMA, Hussein H. Fundamental and Supportive Technologies for 5G Mobile Networks. vol. i. 2019. https://doi.org/10.4018/978-1-7998-1152-7.

[18] Avnet Industrial IoT Gateway - Powered by Raspberry Pi - Documents - Product Pages - element14 Community n.d. $https://community.element14.com/products/devtools/product-pages/w/documents/23055/avnet-industrial-iot-gateway-powered-by-raspberry-pi?ICID=I-CT-LP-TC-000017-IIOT_M2M_COMMUNICATIONS-AVNET_IOT_GATEWAY-MAR21-WF2402973$ (accessed June 5, 2023).

[19] Nandy T, Idris MYI Bin, Md Noor R, Mat Kiah ML, Lun LS, Annuar Juma'At NB, et al. Review on Security of Internet of Things Authentication Mechanism. IEEE Access 2019;7:151054–89. https://doi.org/10.1109/ACCESS.2019.2947723.

[20] Esfahani A, Mantas G, Matischek R, Saghezchi FB, Rodriguez J, Bicaku A, et al. A Lightweight Authentication Mechanism for M2M Communications in Industrial IoT Environment. IEEE Internet Things J 2019;6:288–96. https://doi.org/10.1109/JIOT.2017.2737630.

[21] Aghili SF, Mala H. Breaking a Lightweight M2M Authentication Protocol for Communications in IIoT Environment. n.d.

[22] Lara E, Aguilar L, Sanchez MA, García JA. Lightweight authentication protocol for M2M communications of re-source-constrained devices in industrial internet of things. Sensors (Switzerland) 2020;20. https://doi.org/10.3390/s20020501.

[23] Baruah B, Dhal S. An Efficient Authentication Scheme for Secure Communication between Industrial IoT Devices; An Effi-cient Authentication Scheme for Secure Communication between Industrial IoT Devices. 2020.

[24] Panda S, Mondal S, Kumar N. SLAP: A Secure and Lightweight Authentication Protocol for machine-to-machine communi-cation in industry 4.0. Computers and Electrical Engineering 2022;98. https://doi.org/10.1016/j.compeleceng.2021.107669.

[25] Shahzad K, Alam M, Javaid N, Waheed A, Chaudhry SA, Mansoor N, et al. SF-LAP: Secure M2M Communication in IIoT with a Single-Factor Lightweight Authentication Protocol. J Sens 2022;2022. https://doi.org/10.1155/2022/1309402.

[26] Gong X, Feng T, Albettar M. PEASE: A PUF-Based Efficient Authentication and Session Establishment Protocol for Ma-chine-to-Machine Communication in Industrial IoT. Electronics (Switzerland) 2022;11. https://doi.org/10.3390/electronics11233920.

[27] Yi F, Zhang L, Xu L, Yang S, Lu Y, Zhao D. WSNEAP: An Efficient Authentication Protocol for IIoT-Oriented Wireless Sensor Networks. Sensors 2022;22. https://doi.org/10.3390/s22197413.

[28] Tan Z, Jiao J, Yu M. A Privacy Preserving Authentication Scheme for Heterogeneous Industrial Internet of Things. Security and Communication Networks 2022;2022. https://doi.org/10.1155/2022/9919089.

[29] Xu D, Yu K, Ritcey JA. Cross-Layer Device Authentication With Quantum Encryption for 5G Enabled IIoT in Industry 4.0. IEEE Trans Industr Inform 2022;18:6368–78. https://doi.org/10.1109/TII.2021.3130163.

[30] Zhang Y, Li B, Wu J, Liu B, Chen R, Chang J. Efficient and Privacy-Preserving Blockchain-Based Multifactor Device Authentication Protocol for Cross-Domain IIoT. IEEE Internet Things J 2022;9:22501–15. https://doi.org/10.1109/JIOT.2022.3176192.

[31] Zagrouba R, AlAbdullatif A, AlAjaji K, Al-Serhani N, Alhaidari F, Almuhaideb A, et al. Authenblue: A new authentication protocol for the industrial internet of things. Computers, Materials and Continua 2021;67:1103–19. https://doi.org/10.32604/cmc.2021.014035.

[32] Shen M, Liu H, Zhu L, Xu K, Yu H, Du X, et al. Blockchain-Assisted Secure Device Authentication for Cross-Domain Industrial IoT. IEEE Journal on Selected Areas in Communications 2020;38:942–54. https://doi.org/10.1109/JSAC.2020.2980916.

[33] Lupascu C, Lupascu A, Bica I. DLT based authentication framework for industrial IoT devices. Sensors (Switzerland) 2020;20. https://doi.org/10.3390/s20092621.

[34] Gao S, Ding Y, Lu Y, Han L, Chen C, Yu X, et al. A Lightweight Fingerprint-based Device Authentication Architecture for Wireless Industrial Automation Networks. n.d.

[35] Zhang Q, Wu J, Zhong H, He D, Cui J. Efficient Anonymous Authentication Based on Physically Unclonable Function in Industrial Internet of Things. IEEE Transactions on Information Forensics and Security 2023;18:233–47. https://doi.org/10.1109/TIFS.2022.3218432.

© 2023 NSP
Natural Sciences Publishing Cor.

[36] Maes R, Verbauwhede I. Physically unclonable functions: A study on the state of the art and future research directions. Information Security and Cryptography, vol. 0, Springer International Publishing; 2010, p. 3–37. $https://doi.org/10.1007/978-3-642-14452-3_1$.

[37] Braeken A. PUF based authentication protocol for IoT. Symmetry (Basel) 2018;10. https://doi.org/10.3390/sym10080352.

[38] Idriss TA, Idriss HA, Bayoumi MA. A Lightweight PUF-Based Authentication Protocol Using Secret Pattern Recognition for Constrained IoT Devices. IEEE Access 2021;9:80546–58. https://doi.org/10.1109/ACCESS.2021.3084903.

[39] Sukumaran RP, Benedict S. Authentication and Cryptography solutions for Industrial IoT-A Study. 6th International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud), I-SMAC 2022 - Proceedings 2022:76–81. https://doi.org/10.1109/I-SMAC55078.2022.9987278.

[40] Al-Naji FH, Zagrouba R. A survey on continuous authentication methods in Internet of Things environment. Comput Commun 2020;163:109–33. https://doi.org/10.1016/j.comcom.2020.09.006.

[41] Burrows M, Abadi M, Needham R. rHp0jz-Burrows90 1999;8:1–19.

[42] Luo F, Feng T, Zheng L. Formal Security Evaluation and Improvement of Wireless HART Protocol in Industrial Wireless Network. Security and Communication Networks 2021;2021. https://doi.org/10.1155/2021/8090547.

[43] Braeken A. Public key versus symmetric key cryptography in client–server authentication protocols. Int J Inf Secur 2022;21:103–14. https://doi.org/10.1007/s10207-021-00543-w.

Noura Aldossary is a master student in the field of Information Security at Imam Abdulrahman Bin Faisal University (Dammam, KSA). She received her bachelor's degree in computer science in June 2020 from Imam Abdulrahman Bin Faisal University.

Rachid Zagrouba is an assistant professor from September 2015 at Imam Abdulrahman Bin Faisal University (Dammam, KSA). He received his Ph.D. in Computer Science in December 2007 form University of Rennes 1 (France). He was involved in several French-funded and IST FP6/7 European projects. He is the Ph.D. Co-Supervisor of several Ph.D. students and Supervisors of several Master students in the area of computer networking, wireless Sensor Networks, Wireless Network Security, and IoT security.

© 2023 NSP
Natural Sciences Publishing Cor.