PUF-Based Authentication and Key Agreement Protocols for IoT, WSNs, and Smart Grids: A Comprehensive Survey

Priyanka Mall, Ruhul Amin, *Senior Member, IEEE*, Ashok Kumar Das, *Senior Member, IEEE*, Mark T. Leung, and Kim-Kwang Raymond Choo, *Senior Member, IEEE*

***Abstract*—Physically unclonable function (PUF) is a physical unit fabricated inside a sensor and generally considered as an assurance anchor of resource inhibited device. Essentially, the function is based on the cryptographic approach, where a key is created and utilized such that it cannot be cloned. More specifically, it is an arbitrary function, which maps inherent properties of the hardware devices to a unique bit stream of information. Authentication and key agreement (AKA) protocols are widely used in electronic commerce, electronic stock trading, and many secured business transaction platforms, because they allow the communicating devices to mutually authenticate each other while exchanging authenticated session key (or secret key) that can be used subsequently to establish a secured communication channel. Yet, these protocols are also vulnerable to a broad range of security outbreaks. In light of these notions and practical applications, this article is intended to: 1) provide an overview of AKA protocols, PUF plus the combined PUF-based AKA; 2) systematically and taxonomically examine and discuss with pros and cons of AKA applications to the fast growing areas of Internet of Things, wireless sensor networks, and smart grids based on a meticulous survey of the existing literature; 3) summarize the challenges to deployment and potential security risks of the underlying technologies and possible remedies or mitigation strategies; and 4) to conduct and report a comparative performance and security analysis with respect to the three focused areas.**

***Index Terms*—Authentication and key agreement (AKA), physically unclonable function (PUF), smart grid, wireless sensor networks (WSNs).**

I. Introduction

A NODE in the sensor network, commonly referred as a sensor node, has the capacities to perform assembling and processing of sensitive data as well as to communicate with other adjoining nodes in the network. Typically, a sensor node consists of five major components: 1) a controller; 2) a transceiver; 3) a sensor; 4) an external memory; and 5) a power source. To be specific, a controller in a sensor node completes certain tasks, processes data, and controls the node's component functionality. Microcontroller is a type of controller widely used in sensor nodes because of its inexpensiveness and elasticity in connecting to other devices. Also, it has the advantage of low power consumption. A transceiver has the features of functioning as both transmitter and receiver. However, a major disadvantage of transceiver is its lack of unique identifiers. There are four operational states of a transceiver: 1) transmit; 2) receive; 3) idle; and 4) sleep. In the new generation of transceivers, static machines are built-in for automating operations/functions.

The authentication and key agreement (AKA) protocol is a security protocol used for one-time password generation. This protocol is a process that is based on the challenge–response pair (CRP) and utilizes symmetric cryptography, providing user identity privacy. The AKA protocol embraces various features, such as flexibility in credentials, Denial of Service (DoS) resistance, and efficiency, and it is commonly found in universal mobile telecommunication systems (UMTSs), code-division multiple access (CDMA), etc., [120], [121]. Moreover, AKA allows the communicating devices to mutually authenticate each others while exchanging authenticated session key (or secret key) and establishing secured communication channels. Because of these desirable properties, the protocol is widely used in electronic commerce, electronic stock trading, and many other secured business transaction platforms.

In this article, we focus on three application domains of physically unclonable function (PUF)-based AKA protocols, namely: Internet of Things (IoT), wireless sensor networks (WSNs), and Smart Grid.

IoT has been viewed by many as a pervasive new-age technology in the near future. IoT arrangement involves of a unique identifier allocated to a single device. Communication amongst these devices befalls on both the Internet and the local networks without direct human interference. Generally, an IoT device consists of wireless sensors, actuators, and computer devices. These units are synchronized and operated through Internet enabling data transfer. IoT devices are usually

Manuscript received December 7, 2021; accepted January 7, 2022. Date of publication January 11, 2022; date of current version May 23, 2022. *(Corresponding author: Kim-Kwang Raymond Choo.)*

Priyanka Mall is with the Department of Electronics and Communication Engineering, IIIT Naya Raipur, Chattisgarh 892002, India (e-mail: priyanka16101@iiitnr.edu.in).

Ruhul Amin is with the Department of Computer Science & Engineering, IIIT Naya Raipur, Chattisgarh 892002, India (e-mail: amin_ruhul@live.com).

Ashok Kumar Das is with the Center for Security, Theory and Algorithmic Research, International Institute of Information Technology Hyderabad, Hyderabad 500 032, India (e-mail: ashok.das@iiit.ac.in).

Mark T. Leung is with the Department of Management Science and Statistics, The University of Texas at San Antonio, San Antonio, TX 78249 USA (e-mail: mark.leung@utsa.edu).

Kim-Kwang Raymond Choo is with the Department of Information Systems and Cyber Security, The University of Texas at San Antonio, San Antonio, TX 78249 USA (e-mail: raymond.choo@fulbrightmail.org).

Digital Object Identifier 10.1109/JIOT.2022.3142084

defined by a number of specifications or parameters, such as power, energy, lifetime, and cost, among other; however, security and privacy are one of most crucial yet technologically challenging areas. This is because many IoT devices are not properly safeguarded and/or easily accessible. There have been many security primitives proposed or in existence for the Internet but they are not suitable enough for the IoTs. In general, two basic premises for IoT security protocols that the devices should be invulnerable to the attacks such as the side-channel attack and that they should be resistant to unnecessary human interference. It follows that confidentiality, sender/receiver authenticity, and integrity of the communication messages should be maintained during transfer of data among these devices.

WSNs have been employed in fields, such as military surveillance, air pollution monitoring, pressure measurement, healthcare, and many other environmental and urban applications. There are a number of underlying characteristics, such as low data transmission and power consumption, limited battery energy, and inexpensive.

In smart grid, "the grid" usually denotes to the electric grid, transmission lines network, transformers, and other units that send electricity to the factories, public facilities, houses, or other entities from the power plant. Here, we extend the electric grid's nature to its capacity. What makes the grid smart is the technology used for the purpose of establishing a two-way communication amongst the utility and its customers, and also the sensing along with the transmission lines. The associated smart grid characteristics include efficient electricity transmission, faster refurbishment of electricity after power turbulences, enhanced incorporation of customer–owner power generation systems, reduced cost of management and operations for services, thereby reduced costs of power for running the system, reduced uttermost demand, thereby lowered electricity consumption and charges, increased large-scale renewable energy system integration and adoption, and enhanced security features.

In this article, we present an outline of AKA protocols and those that utilize PUF, and discuss their applications in fast growing areas of IoT, WSNs, and smart grids. Based on our review, we summarize several challenges and research opportunities associated with the deployment of PUF-based AKA protocols. We also conduct and report a comparative performance and security analysis with respect to the three focused areas.

In the next section, we present the relevant background materials on AKA protocols (Section II) and PUFs (Section III). In Sections IV–VI, we review and summarize the existing approaches in IoT, WSN, and smart grid context, respectively. In Section VII, we describe the setup used in the evaluation of various cryptographic primitives. In Section VIII, we present a comparative summary of the performance and security of the protocols examined in this article, followed by the conclusion in Section IX.

II. Authentication and Key Agreement Protocol

While the steps may differ between AKA protocols, there are a number of fundamental steps required to ensure secure communication. Generally, the AKA protocol is a security protocol used for one-time password generation. This protocol is a process based on the CRP and utilizes symmetric cryptography, providing user identity privacy. Authentication allows one to determine whether the communicating parties are who they claim to be and are authorized to access the resources. Establishment is concerned with the cryptographic keys used to protect the communication by ensuring data confidentiality and integrity. There are various phases associated with both AKA.

1) *Registration and Enrolment Phase:* In this particular phase, the initiation of the application occurs where other operations (e.g., verification of the user's identity information) are performed. During registration, the entities and the parties involved register themselves using their personal information (e.g., business registration number or legal name and national registration number, such as social security number) during this phase, and the information used for the registration may be recorded, based on the regulatory requirements.
2) *Entity Authentication Phase:* This phase deals with the authentication and record keeping of the entities and the parties involved.
3) *Key Exchange Phase:* In the key exchange phase, two or more parties communicate securely by first exchanging the secret key used to encrypt and decrypt messages, also called as encryption key exchange. The phase ensures the secure establishment of a secret key between two or more parties, even in the presence of an eavesdropper.
4) *Password Authentication Phase:* In this phase, two or more entities compute the cryptographic key based on the knowledge of their own password.
5) *Credential Management Phase:* The phase deals with the creation, issuing, preprocessing, activation, and storage of the credentials. Other functionalities, such as record keeping, and credential renewal, replacement, and revocation are also supported in this phase.
6) *Dynamic Node Addition Phase:* This phase allows one to add new nodes dynamically, in order to scale up the network/system.
7) *Mobile or Smart Card Revocation Phase:* The smart card should be revoked and reissued in the event that the smart card is misplaced or stolen, or when the key is compromised. This phase helps to protect the user's information from smart card loss or other related attacks. The revocation and reissuance require additional communication rounds (and consequently computational overheads).

Now, we will briefly review the general security requirements of AKA protocols.

In PUF modeling attacks, an adversary collects a subset of all CRPs of PUF and tries to derive a numerical model from the CRP data retrieved, in order to predict *PUF's* response to the random challenges with a higher precision [116]. Several methods, such as linear programming, algebraic techniques, and *ML* techniques, are being used to facilitate such an attack. Generally, strong PUFs are (surprisingly) more prone to modeling attacks, which affects its unpredictability and physical unclonability, particularly if the predictive model has been

derived by the adversary [117]. An arbiter PUF (APUF) is one strong PUF, which involves parallel-staged multiplexer (MUX) chains, where the challenges are given to the selection inputs of the *MUX* chains and the responses are generated by exploiting the delay difference between two paths. A particular selection input is provided to the *MUXes* of the same stage, which helps in determining whether the signal is transmitted in parallel or across. The arbiter *PUF's* functionality can be signified by an additive linear delay model where the delay is obtained by adding the propagation delay from every particular stage, which can be mathematically expressed as follows:

$$\Delta * = \vec{\omega}^T \vec{\Phi}.$$

In the above equation, $\vec{\omega}$ is a feature vector that denotes the propagation delay of each *MUX* in the APUF, and $\vec{\Phi}$ is an n-bit challenge Ch function

$$\vec{\Phi}(\vec{Ch}) = \left(\vec{\Phi}_1(\vec{Ch}), \vec{\Phi}_2(\vec{Ch}), \vec{\Phi}_3(\vec{Ch}), \ldots, \vec{\Phi}_n(\vec{Ch}), 1\right)^T.$$

In the above equation, $\vec{\Phi}_b(\vec{Ch}) = \Pi_{a=b}{}^n(1 - Ch_a), b = 1, 2, 3, \ldots, m$.

Shi *et al.* [118] presented two approximation modeling attacks—1) logical approximation and 2) global approximation. The main difference between the two models lies on the mapping of relationship between the input and output of MUX. Specifically, logical approximation uses linear functions in conjunction with basic logical operators (e.g., AND, OR, and NOT) whereas global approximation adopts the sinc(x) function along with filtering characteristics. Both logical and global approximation models are considered strong PUFs. The logical approximation should be considered when the PUF structure is a composition of logical gates. In logical approximation, the PUF structure is decomposed into basic logical gate formation using the *AND, OR*, and *NOT* operators. Henceforth, the logical gate function is approximated and *PUF's* input parameters are substituted by the approximated functions. Then, all approximation functions are aggregated on the basis of the wiring of individual logical gate and, thereby, the global approximation function for the PUF is obtained. Global approximation should be considered when the logical structure is complex and cannot be further decomposed into basic logical gates. In this case, the features of the mapping relationship between the input and output of the PUF structures are extracted and analyzed. A mathematical function with similar characteristics is obtained and then the mapping relationship is approximated. Subsequently, the mathematical functions are transformed and combined into the global approximation function. As a result, a model is built and trained.

1) *PUF Modeling Attack:* It is mandatory to achieve at least the number ($N_{\min}$) of direct CRPs from the (PUF) for the purpose of modeling a linear (PUF) with a given level of accuracy. $N_{\min}$ is a parameter determined by the type of (PUF) as well as the learning strategy. Here, $N_{\min}$ is the minimum number of CRPs required to model an N-stage delay-based linear (PUF) with a misclassification rate ϵ. The value of $N_{\min}$ is given as

$$N_{\min} = O\left(\frac{N}{\epsilon}\right).$$

Under this scheme, the attacker is required to correctly assume the key indices for the discovery of L_{sub} CRPs. Here, ind_1 is a number between 0 and $L-1$ (where L is the length of the original response string from which we acquire the substring), and ind_2 is a number between 0 to $L_{PW}-1$ (where L_{PW} is the substring length that has been padded). The attacker will encounter $L \times L_{PW}$ choices if the indices are to be randomly guessed. Theoretically, the attacker can construct a (PUF) model for every choice (M_{iter}) by training it on the set of L_{sub} CRPs with the help of machine learning methods. However, the number of hypothetical (PUF) as for building an accurate model will rise exponentially, because the attacker has to obtain $N_{\min}$ correct CRPs. With the condition $L_{\text{sub}} > N_{\min}$, the attacker will be able to breach the system with $O(L \times L_{PW})$ attempts. Nevertheless, if $L_{\text{sub}} < N_{\min}$, then the attacker is required to initiate $N_{\min}/L_{\text{sub}}$ number of rounds of authentication so as to get at least $N_{\min}$ CRPs. Therefore, $N_{\min}$ must be increased for a fixed ϵ with N to improve security while managing strong performance. This also requires a structural alteration to delay-based PUFs.

2) *Impersonation Attack:* Over a public/open channel in the course of the execution of the protocol, there can be eavesdropping from the attacker's side. This could lead to the modification of the message or even retransmission of the message to the user to impersonate itself as a valid user. During the execution, the attacker may trap the login message. The attacker then generate another valid message, which will be validated. To do so, the attacker has to compute valid credentials. However, the attacker cannot guess the user identity, password, and the secret key because they have high entropy property. It is then impossible for the attacker to predict the trapped message in a particular polynomial time. Even if an adversary impersonates the user, he/she will not be able to login into the mobile device. The mobile device requires password, which is actually not used since it is stored in the network [116], [119].
3) *Logical Attacks:* These are attacks where the users are lured to connect with nearby free fake *Wi-Fi* networks. This type of attacks may lead to leakage of sensitive information and data exploitation. For the logical attack, usually a fake-free *Wi-Fi* or a rogue access point (AP) is being set up. However, in this protocol, we do not store any sensitive information in the memory. If the device maintains a table of data, such as the sensor node identity and the challenges for the (PUF)-based device, then the risk of logical attacks is mitigated.
4) *Session Key Security Attack:* Using the responses and the random number generated with IDs of the communicating nodes and the devices, a common key is produced. The common key helps to secure communication. Because of the (PUF) circuitry, the response

evaluated cannot be duplicated, leaving practically no chance for the duplicity of the (PUF) circuit [119]. Thus, the common key between the nodes is crucial to resisting any external attacks.

5) *Stolen Device:* Typically, only an authenticated user with a trusted device is allowed to access the network. Suppose the mobile device is stolen or lost. An adversary, *AD*, may seek to impersonate like the authenticated or trusted user in order to gain access to the network. However, *AD* has to login to the system where he or she will be asked to provide the password, which is known only by the authenticated user of the device. Also, *AD* is required to provide the *ID*. Thus, if *AD* cannot satisfy all requirements needed to login to the system, the impersonation of a trusted user cannot be established. On the other hand, in the event that *AD* gets all information stored in the device via a side-channel attack, any kind of changes like this will correspondingly change the *PUF's* behavior, rendering the malicious plan of no use. It is because PUF will not be able to produce the same response for a particular challenge if its behavior is changed. Furthermore, password is often implemented in the form of a one-way noninvertible hash function. Given that AD cannot extract the password even he/she has acquired the parameters computed using the authenticated user's password. In summary, a stolen mobile device should not pose the risk of information leakage, [116].
6) *Insider Attack:* Normally, we simply assume that a so-called secured server/system is safe and authenticated and, thereby, can be fully trusted. Also, it is often assumed that the chance of leakage of any kind of information is negligible. In reality, a system can get hacked because of the insider attack. This generates concern for the security and privacy of user information to address this issue, and the password used in the protocol should not be used or stored as it is. Instead, password of the user P_{di} in the protocol is given to and stored in the server in the form of U_{pdi} where $U_{pdi} = h(Pd_i \| R_{ui})$ and the term R_{ui} is a random number. Moreover, it will be difficult for any adversary to extract the password P_{di} because the one-way hash function in PUF is noninvertible [116].

III. Physically Unclonable Function

Being a random function, PUF maps basic properties of the hardware entity to a unique bit stream of information. PUF uses CRP to facilitate authentication. The use of PUF in the sensor, for example, enables only the authenticated person to access the respective data because PUF will generate a unique response each time. A PUF response alters between PUF instance(s), even for the same challenge. In PUF-based authentication, it is expected to maximize the reliability of the response and the complexity of the model so as to increase the differentiating ability of the PUF instance and, thus, to prevent the attacks from the adversary. However, the response generation is related to varying operating conditions, such as temperature and voltage.

TABLE I
Comparison of the Evaluation Metrics of Multiple PUFs

EVALUATION METRICS	SRAM	OPTICAL PUF	MEMRISTORS	CNT PUF
ENTROPY	LOW	MEDIUM	HIGH	HIGH
REPRODUCIBILITY	YES	YES	YES	YES
RECONFIGURABLE	NO	YES	LIMITED	LIMITED
CRP	LINEAR	EXPONENTIAL	LINEAR	LINEAR
COST	HIGH	HIGH	HIGH	HIGH
ENERGY CONSUMPTION	HIGH	LOW	LOW	
VOLATILE/ NON-VOLATILE	VOLATILE	NON-VOLATILE	NON-VOLATILE	NON-VOLATILE
NATURE OF PUF	WEK	STRONG	STRONG	STRONG

TABLE II
PUF Properties: A Comparative Summary

Properties	Optical PUF	Arbiter PUF	RO PUF	SRAM PUF	Butterfly PUF
Evaluatable	✓	✓	✓	✓	✓
Unique	✓	✓	✓	✓	✓
Physically Unclonable	✓	✓	✓	✓	✓
Unpredictable	✓	Conditional	Conditional	✓	✓
Reproducible	✓	✓	✓	✓	✓
One-way	Untested	×		×	×
Tamper Evident	✓	Untested	Untested	Untested	Untested
Mathematically Unclonable	✓	×	×	×	×
Randomness	Explicit	Implicit	Implicit	Implicit	Implicit
Modeling	Difficult	p=3.55%0 q=5000 q-observed queries & p-prediction error	p=3.55% q=5000 q-observed queries & p-prediction error		

A. Properties

Random functions such as PUF are required to meet the following properties: 1) no two challenges should produce identical response; 2) PUF should satisfy the uniqueness property, that is, no two PUF devices can be the same because, during the manufacturing of the PUF devices, some fabrications are done so that the uniqueness of PUF is maintained; 3) the property of the unpredictability should also be satisfied by the PUF; 4) reliability property should also be met by the PUF; 5) the CRPs should be arbitrary and generated in a brief amount of time; 6) modeling of the PUF should be impossible from a certain set of CRPs; 7) low attack multiplicity (i.e., a CRP pair extracted at a certain point of time cannot be extracted at another time instance by attacker) should be fulfilled by the PUF; and 8) in order to maximize the security, PUF devices are required to meet the strict avalanche condition (SAC). Tables I and II show the comparisons of multiple PUFs across different evaluation metrics and properties, respectively, [122].

B. Types

One key application of PUF is in security, that is, to mitigate invasive and semiinvasive attacks. Generally, PUFs are being classified with respect to the fabrication method and security strength. Based on the fabrication method, there exists two types of PUFs, namely, silicon PUFs and nonsilicon PUFs. The former (i.e., silicon PUFs) is edged with supplementary ICs and is engineered on the same die as a part of the circuit.

In silicon PUFs, the discrepancies during the manufacturing are apprehended in the form of challenge and the difference in the circuit characteristics is formed as a exceptional response for a respective challenge. Nonsilicon PUFs, fabricated on the silicon system, require special assembly practices, which are not the generic complementary metal oxide semiconductor (CMOS) production technology fragment. The response produced from the challenge set in the case of nonsilicon PUFs is attained from arbitrary physical difference in the physical arrangement instead of ICs.

C. Security

For a PUF instance, say, given PUF_{Ad} when a challenge C and an n-bit string are provided, then the decisional uniqueness problem can help decide whether PUF_i is the n-bit string $X = PUF_i(C)$ or an arbitrary n-bit string. In the decisional exclusivity problem, the problem of producing a PUF instance PUF_i with the help of PUF_{Ad} is difficult. For the probabilistic polynomial time algorithm, say P, there is a negligible function $G()$ where $| P_b(P(C, PUF_{Ad}, X) = 1) - P_b(P(C, PUF_{Ad}, PUF_i(C)) = 1) | \leq G(n)$.

Suppose we use two challenges, C_1 and C_2, and two n-bit strings, X_1 and X_2. Then, the two-decisional uniqueness problems can help decide whether $X_1 = PUF_i(C_1)$ and $X_2 = PUF_i(C_2)$ for a particular PUF instance PUF_i or two arbitrary n-bit strings. For the two-decisional uniqueness problem, there exists an insignificant function $G()$ for all probabilistic polynomial time algorithm Q such that $| P_b(Q(C_1, C_2, PUF_{Ad}, X_1, X_2) = 1) - P_b(Q(C_1, C_2, PUF_{Ad}, PUF_i(C_1), PUF_i(C_2)) = 1) | \leq G(n)$.

There are three security strength levels, ranging from strong PUFs to weak PUFs to controlled PUFs. The main motives behind these types of PUFs are the number of challenges and response's accessibility from outside. Strong PUFs provision a large number of CRPs. Through complex input–output relations and an exponentially increasing number of CRPs, protections are provided to the CRPs of the PUFs as the CRPs are accessible to the outside. Strong PUFs are often used for device authentication purposes and activates in certain MHz range such that even a short period of snooping can gather many CRPs. Hence, strong PUFs are susceptible to multiple attacks. Controlled PUFs have a strong and solid PUF in the core part with control logic protection. In the controlled PUFs, CRPs are difficult to access directly since the challenges of the PUFs are preadministered before passing to the strong PUF and the responses are also preprocessed before getting out of the strong PUF. The preprocessing of the CRPs evidently progresses the security of the measured PUFs. The algorithm is also incorporated to the same chip of which the PUF is fabricated, through which only the controlled PUF is accessible. Both the PUF and the algorithm are completely intimate. The definite outputs of the PUF are not directly accessible to the outsiders and the outputs that are accessible to the outsiders are actually the outputs processed from the algorithms. The third type is weak PUFs. They have few and fixed challenges and the responses from these challenges are never made public anyway. Weak PUFs are primarily used for deriving a secret key in the cryptographic algorithms and are slightly vulnerable to modeling attacks. The architectures of different types of PUFs are shown in Figs. 1 and 2.

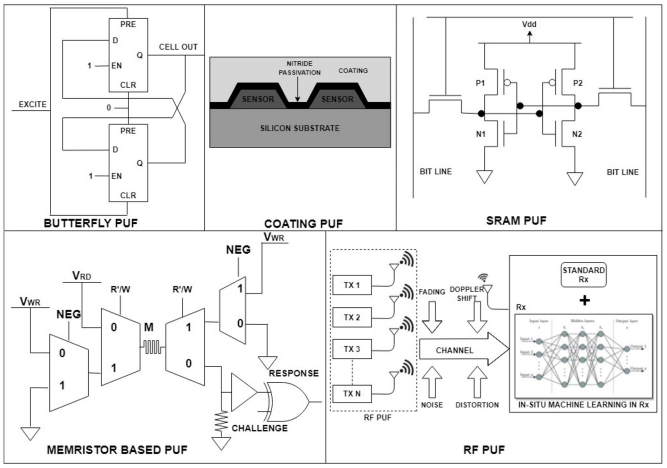

Fig. 1. Circuit architectural diagrams for different PUFs–part i.

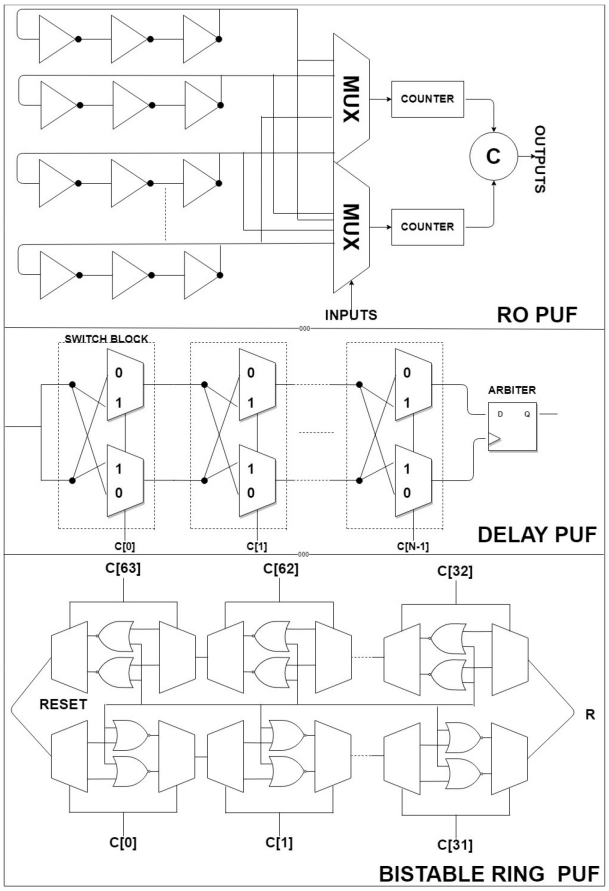

Fig. 2. Circuit architectural diagrams for different PUFs–part ii.

1) *Ring Oscillator PUF:* The RO frequencies are taken in a counter and are subsequently transformed into binary outputs via a simple comparison method. PUF-based RO uses the uncontrollable process delay variations of the digital components as a randomness source. The RO's frequency relies on the gate and the routing delay, which is separately determined during the manufacturing

process in an uncontrollable manner. The ring oscillator's output frequencies fluctuate and hence, this factor is used for the formation of the binary response.

2) *Arbiter-Based PUF:* Arbiter-based PUF is a kind of delay-based PUF that familiarizes race condition between two digital paths. Both paths end in an arbiter element of a chip and the chip determines the faster of the two paths and, subsequently and correspondingly, gives binary values as the output. The arbiter-based PUF also generates outputs with very low unpredictability, which is further improved by the XOR Arbiter PUF. An arbiter-based PUF exploits the intrinsic timing alterations of the two symmetrically designed paths to a single bit response at the output. The circuit consists of multiple connected stages along with an arbiter at the chain's end where each stage has two outputs and three inputs with a single bit of the challenge and the two outputs from the previous stage [123].
3) *SRAM PUF:* The static random-access memory (SRAM) PUF uses the randomness of the SRAM cells after the cells are powered up. SRAM PUF can be connected effortlessly to the standard digital circuitry straight, which is rooted on the same chip. They can also be easily arrayed in cryptographic implementation in the form of a hardware block. The SRAM cells have their own chosen states that result from the differences in the threshold voltages every time they are powered. The SRAM output produces a unique and arbitrary pattern of 0 and 1 s like the chip's thumbprint and is unique to a certain SRAM. SRAM PUFs are used as a high security requirement in defence, military systems, and financial transactions [124].
4) *Butterfly PUF (BPUF):* The BPUF is a procedure that targets to emulate the behavior of an SRAM PUF. The BPUF is a cross-coupled bistable circuit that can be made unstable before it settles to one of the two possible stable states. The structure of the BPUF has two latches whose outputs are cross-coupled. In summary, a BPUF consists of two cross-coupled latches and conducts exploitation of random assignment of an unstable state to a stable state. This is done by presetting one latch while putting the other in clear mode via an excite signal.
5) *Optical PUF:* An optical PUF comprises of a transparent element, which has been doped with the light scattering particles where the process of placing of these particles is uncontrollable and the laser-particle interaction is also intricate. Hence, it is very hard for any outsider or attacker to clone the PUF for the purpose of generating the same pattern. The core section of the design of the system consists of an optical token that comprises an optical microstructure. The optical PUF possesses multiple advantages, such as low cost per piece, high complexity of the outputs generated, and resilience against the modeling attacks and physical cloning attacks. However, the setup of the optical PUF is quite laborious because of the size of setup and mechanical positioning.
6) *Delay PUF:* The delay-based PUF circuit consists of extraction and assessment of the random delay and exploits the arbitary disparities in the delays of the wires and the silicon gates. The two path transitions are measured and compared to determine the one reaching the end first. Depending on the transistor that comes first, an arbiter, which is generally executed as a latch, produces 0 or 1. A delay loop-based PUF is a ring oscillator with logic. There are four types of delay-based PUF: a) arbiter-based PUF; b) XOR-based arbiter PUF; c) lightweight secure PUF; and d) feedforward PUF. A delay-based PUF also exploits the built-in delay features of the physical components that varies from chip to chip.
7) *Glitch-Based PUF:* Glitch-based PUF is a new delay-based PUF of which the glitch waveforms arise at the output of the random logic. The glitches are used in the form of information source generation that eventually performs nonlinearly from the delay variation amongst the gates and each gate's pulse propagation characteristic. Glitch-based PUF mainly comprises of control registers, data registers, glitch generator, sampling circuit, and two types of delay circuits [126].
8) *Bistable Ring PUF:* The *BR-PUF* is built upon the concept of a ring consisting of a uniform number of inverters with two probable stable states. Exponentially, large sum of CRPs can be produced from *BR-PUF* by the duplication of the inverters and the addition of the MUXs between the stages [125].
9) *Coating PUF:* On the top of an IC, i.e., integrated circuit, a coating PUF can be constructed as a network of metal wires in the form of a comb. A dense material exists between the comb spaces, which is also doped with particles that are dielectric. The exclusive randomness is made into use by obtaining an exclusive device identifier. The coating PUF or also known as the Opaque PUF on the top of the IC protects the circuits below from any alterations from attackers including reverse engineering. The coating PUF also offers strong protection against physical attacks and tampering of evidence. In such event, the responses of the PUF change substantially after its attack with a FIB.
10) *RF PUF:* This PUF needs no additional hardware at the transmitter and can be used individually with multifactor authentication of security characteristics as a physical layer security feature. RF-PUF is suitable for real-time authentication of the wireless nodes with the use of vital process variation on the RF properties [127].
11) *CRP Reconfigurable PUF:* Without changes to the main PUF structure, the CRP can be made reconfigurable by the addition of circuits to the design. This feature is achieved through multiple ways: a) preprocessing the challenge bits. Rather than providing the challenge bits directly to the PUF, the bits are given to the newly added circuit, i.e., either linear feedback shift registers (LFSRs) or hash functions, whose yield is then further given to the PUF in the form of a challenge bit; b) preprocessing of the response bits. Rather than directly considering the yield of the PUF, it is first given to the recently added

circuitry, which is mostly the hash function, whose output is further considered as the PUF response; and c) addition of an extra reconfigurable components for preprocessing the PUF's output, which is also known as output recombination.

12) *Memristor-Based PUF:* Memristor-based PUF is compatible with CMOS fabrication standards where a memristor, also known as resistive-RAM (RRAM), has a two terminal unreceptive electric section to provide easy tamper detection and to guarantee security for the PUF's response. A memristive device consists of several distinct resistance states where they can switch its states. The resistance variations in the device depends on the voltage/current that are applied previously across/through the device. A memristor is a combination of both memory and resistor.
13) *Diode-Based PUF:* The crossbar arrays nearly possess discrete advantages and are absolutely the most attractive option for PUF design. The crossbar arrays have advantages, such as a consistent structure, small energy consumption, and simple execution. In this, the input voltage for writing purpose is generally higher than that for reading.
14) *CNT-Based PUF:* The carbon nanotube field-effect transistor (CNTFET)-based PUF focuses on improved consistency, low energy consumption, and power consumption. CNT is used in the channel in the CNTFET transistors. The common discrepancies in the CNT are chirality, doping concentration, growth density, misalignment, and diameter.

D. Applications

PUFs provide solutions to applications, such as random number generators (RNGs), radio-frequency identification (RFID) tags, and device authentication. PUFs, partly due to their associated randomness property, are used in devices for the purpose of low-cost authentication.

1) *System Identification:* For anti-counterfeiting technologies, PUFs are used for identification determination because of its unclonability and unpredictability property. The responses that are generated from the PUF devices can be used straight for the identification. The PUF's CRPs are stored in the database along with the physical system's identity that are embedded in the PUF device. During the identification process, the verifier selects an arbitrary CRP from the stored CRPs. After evaluation, if the response generated is same as the response stored in the database for a specific challenge, then the identification procedure is done successfully or else it has failed. The CRPs are also used only once for every PUF so as to prevent the replay attack and should be eliminated after the identification. The unique identification is actually possible if the response generated from the PUF devices has enough entropy with respect to the size of the population [2]. The determination of the false-acceptance-rate (FAR) and the false-rejection-rate (FRR) is done on the basis of the inter and intradistance histogram overlapping. The FAR and the FRR sum should be minimized and also the threshold should be established at the intersection of both the histograms to achieve the optimal state.

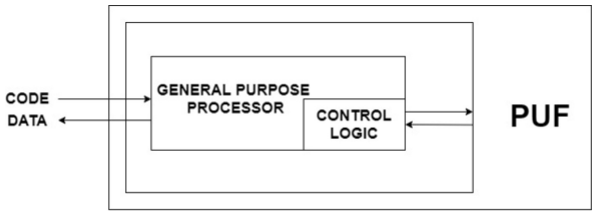

Fig. 3. Schematic framework of anonymous computation and software licensing.

2) *Secret Key Generation:* There are intrinsic properties of the PUFs in the integrated circuits, which can be used for the storage and secret key generation. The secret key is generated from the intrinsic arbitrariness, which are familiarized by the unavoidable variability in the manufacturing process. There is actually no requirement of explicit key programming. As a result, this simplifies the key distribution and does not need conventional nonvolatile key memory. PUFs also facilitate with improved security. The keys are not used directly because the PUF responses are generally noisy and have limited entropy amount. There is actually need of uniformly random and perfectly reliable keys for the cryptographic algorithms. An algorithm, known as the two-phase algorithm, solves the issue of secret key extraction from the nearby secrets in the information theory. In this algorithm, there are two phases: a) the initial generation phase and b) the reproduction phase. In the initial generation phase, the PUF is enquired and a secret key is produced by the algorithm along with additional information known as the helper data, which can be publicly communicated to the device by the verifier. Both the secret key and the helper data are stowed in a secured database by the verifier instead of storing them in the device. While in the reproduction phase, the verifier provides the helper data to the process or to the algorithm where it is used for the extraction of the equivalent key from the PUF. Hence, the device encompassing the PUF and the verifier can establish a shared secret key [2].
3) *Anonymous Computation and Software Licensing:* Anonymity makes the unlawful IP core vendor (CV) hard to pretend as a legal system developer (SD) [4]. Fig. 3 schematically illustrates how anonymous computation and software licensing work under this framework.
4) *Hardware Entangled Cryptography:* In existing cryptographic primitives, secret key generations from PUFs are raised and addressed in the application scenarios. However, it can also fully integrate the PUF in the primitive itself, which is termed as hardware entangled cryptographic primitives [2]. Hardware entangled cryptographic primitives are keyless since a secret key is not stored in either volatile or nonvolatile memory. This

offers security against attackers specifically targeting either type of memory.

5) *Random Number Generator:* RNG depends on the unpredictability feature of the small number metastable challenges because all *SPUF* challenges are based on the hidden and unknown timing differences that are inherent in the chip manufacturing. PUF-based RNG is inexpensive and is an important alternative for the expensive and complicated hardware RNG [1].
6) *Device Authentication:* PUFs are used for the authentication of the individual ICs with no use of expensive cryptographic primitives. The PUF output is unique as well as unpredictable. PUFs have an exponential number of CRPs from which the response is unique for respective IC and for respective challenge. Typically for device authentication, several steps are taken: a) after the PUF is manufactured, the server accesses the PUF and generates CRP table where the pairs are warehoused in the internal secret storage; b) the PUF is then given to the client and the client submits a request to the server for authentication; c) the server then selects the known CRP and submits the challenge to the client; d) the client runs the challenge on the PUF and then sends the response to the server; and e) the server then finally checks whether the response received is correct or not and whether particular CRP is marked as utilized [3].

IV. PUF User Authentication and Key Agreement for IoT Settings

Authentication and validation are key areas in IoT deployment. Braeken [5] proposed an efficient method of authentication between two IoT devices with the use of PUFs along with a common cluster node. The CRPs are not stored explicitly. Hence, in the event that an attacker is successful to attain access to the database, the stored data of associated CRPs cannot be tied to (or as operational input for) any learning algorithm type and security is maintained. This proposed scheme draws on only the elliptical curve multiplication together with additions rather than using the intensive pairing operations as an alternative scheme. Based on a completely different conceptual foundation, Bian *et al.* [6] proposed a new biometric authentication scheme in which ideas of PUF and fuzzy extractor are adopted. The inherent security features of user's fingerprint biometrics and PUFs are used to design an innovative user AKA protocol, *Bio-AKA*, for the security characteristics. The proposed scheme employed the fuzzy extractor to defend the privacy and to reinforce the biometric data security and thereby, improve the robustness of the scheme. Akhundov *et al.* [7] demonstrated the design, development, and evaluation of the *SRAM-PUF* technology and elliptic curve cryptography (ECC)-based application-specific secure communication architecture. This article acquaints with the elliptical curve Diffie–Hellman (ECDH) public-key-based cryptographic protocol, which exploits the properties of PUF and derives keys as the root-of-trust for silicon authentication. The design of the modular hardware architecture is proposed by the authors for support of the protocol. In turn, the proposed protocol validates the solution by prototyping and verifying of the protocol variant on the *Xilinx Zynq-7000 APSoC* device for analysis of practicality and feasibility of the proposed scheme.

There are also recent developments from the perspective of IoT in security of power. Bansal *et al.* [8] proposed an authentication protocol for vehicle-to-grid (V2G) devices based on PUF. The electrical energy stockpiled in the EV batteries functions as a power source for the grid and supplementary energy-efficient EVs. Their proposed protocol addresses these issues at the same time via the use of PUFs to acquire a two-step mutual authentication (MA) amongst an EV and the grid server. Fang *et al.* [9] demonstrated a general IoT system architecture to handle an array of heterogeneous IoT devices. Based on the trust relationships among different entities in the IoT system, various trust models are proposed and examined. Using a least trust compulsory model, an efficient and flexible authentication scheme is developed with explicit consideration of heterogeneous IoT devices in the system. This scheme provides security and privacy.

In the IoT world of V2G, Boke *et al.* [10] drew attention toward the negotiations done in the areas of security, resources, and flexibility to bait customers with low prices, and smaller and advance designs of IoT devices and their significance. This article conferred the degree of security in every layer of IoT stack. During the encryption of the data, the near-field communication (NFC) protocol that operates on physical-data link layer and IPv6 over low-power wireless personal area networks (6LoWPAN), which is a network layer protocol, lacks the proper key management. In cryptographic algorithms, key management as well as key generation and storage are important integral parts of encrypting data. The authors of the paper also discussed various types and methods of key generation techniques that provided solution to a variety of situations and environments. An exemplifying application is management of the level of necessary security and the availability of resources for strengthening communication protocols. V2G devices are small in size, cheap, and resource constrained. These make the devices prone to multiple attacks. As a result, there is an increase in the need for a secured, lightweight, and vehicle owner privacy protection protocols for V2G. Bansal *et al.* [11] attempted to provide a solution for the EVs and charging stations security issue by proposing a secure PUF-based authentication called the SUKA protocol for V2G systems where PUF is used for two-step mutual authentication. PUF is essentially lightweight, secured, and privacy preserving.

Wang *et al.* [12] proposed as an entropy pump used to enhance the entropy. The PUF-based entropy pump is further used in a password improvement application for implanted IoT devices. Because of the strict timing and device requirement of power, existing cryptographic solutions may not be completely relevant to or suitable for IoT devices. To address the concern, PUF represents and can be adopted as a capable hardware primitive because of its lesser hardware cost and energy efficiency. The authors of the paper established that the proposed outline demonstrates an overall 48% substantial improvement on the human-generated passwords' entropy. The design is verified on the *Nexys 4 DDR FPGA* board,

which has low hardware overhead and subsequently guarantees the feasibility for IoT applications. On another front, Barbareschi *et al.* [13] overcame the issues generated by the traditional cryptography-based security solutions due to relatively small computing resources of the involved nodes. This article proposed a mutual authentication scheme, which relies on the PUF's adoption, special integrated circuits, unclonability, uniqueness, and tamper-evident characteristics. The proposed scheme addresses this deficiency and is resilient toward these attacks.

Amongst the latest developments in IoT security assurance, Liu *et al.* [14] proposed design ensures secured transmission of data and bidirectional authentication of the identities among IoT devices and terminals. The design yields low communication costs with additional benefits of being lightweight and flexibility in key updates. The terminal authentication during the key agreement is maintained by the protocol and the design boosts the business system's security over the smart grid. On the other hand, the study by Jiang *et al.* [15] acquaints with PUF in the AKA protocol to ensure the security of system even if the sensors and user devices are compromised. In their scheme, PUF eradicates any secret information storage in the user devices or vehicle sensors when PUF is used as a hardware fingerprint generator. The user device cannot be accessed by an arbiter user if the PUF is used collectively with the password. The proposed protocol offers anonymity and desynchronization resilience by means of public-key cryptography. This protocol is independent from the influence of the known attacks and can achieve predictable security properties with elaborated security analysis. Furthermore, Byun [16] proposed a PUF-based multifactor authenticated key exchange (PUF-MAKE). The user possesses the multifactor authenticators. While the server preserves the PUF outputs for authentication, the user securely holds a PUF-embedded device. Technically, the proposed PUF-MAKE protocol is secured and requires three communication flows. This article explained the PUF-MAKE protocol in a comprehensive manner.

Further IoT security improvement can be found in recent studies. Barbareschi *et al.* [17] proposed a mutual authentication scheme based on PUF. The scheme permits fog nodes and resource-controlled IoT devices to mutually demonstrate their respective individualities. The adoption of a cloud automated framework permits the scheme to be offered in the form of as-a-service, and eases setup on fog nodes. Liang *et al.* [18] used a lightweight security encryption primitive like PUF for protection of low-cost device and information security because such devices are vulnerable to multiple attacks. Therefore, PUF is used as a countermeasure in the design of devices during the manufacturing process. In this article, a two-stage multiple-choice arbiter (TSMCA)-based PUF (TSMCA PUF) in the RFID system is proposed, specifically tailoring for the low cost and interconnected IoT devices security issues of the RFID technology in IoT. The TSMCA PUF focuses on the double PUF-based bidirectional RFID identity authentication protocol design. This allows the bidirectional authentication between a server and a tag for the IC authentication to work in the low-cost RFID systems using the exclusive-OR (XOR) and the character padding operations for the response generation. The proposed protocol is resilient against multiple attacks.

Moreover, Melki *et al.* [19] proposed a lightweight secured multifactor device authentication scheme for IoT devices based on two ideas—1) configurable physical unclonable functions within the IoT devices and 2) channel-based constraints. The proposed scheme used some simple cryptographic operations, such as bitwise XOR operation and one-way hash function. In their protocol, the random channel characteristics are used to provide high robustness against various attacks and also maintain low complexity. The scheme curtails minimum computation and communication overheads. Under a different approach, Garg *et al.* [20] presented a robust lightweight and provably secured AKA scheme for IoT. The authors used the lightweight operations, such as elliptical curve cryptography, physical unclonable function, hash function, concatenation, and XOR operations. Design of the protocol supports mutual authentication among the IoT nodes and the server. The scheme is resilient against numerous security attacks, such as DoS attacks, replay attacks, spoofing, and more. For the health sector, Suganthi *et al.* [21] proposed an end-to-end mutual authentication protocol for security and privacy protection of the patient that balances the security and performance needed in the healthcare environment. The protocol uses PDA or smartphone as a gateway node for continuous monitoring of the patient. The scheme also ensures that the patient has authenticated sensor nodes. The proposed protocol is proven to be efficient.

Chatterjee *et al.* [22] developed a protocol by combining the concepts of the identity-based encryption, i.e., IBE, PUF, and Key-ed Hash function. The protocol's security is formally proven under the session key security and framework of the universal composability. In a follow-up work, Braeken [23] proposed an alternative scheme that universally solved the issues existing in the scheme of PUF-based protocol presented by Chatterjee *et al.* for IoT. The Chatterjee *et al.* protocol had issues like the security attacks. The new follow-up scheme provides a secure key agreement and a communication phase amongst the two IoT devices. The proposed scheme also offers authentication based on identity and repudiation with the use of the elliptical curve multiplication along with additions rather than using the intensive pairing operations.

Chatterjee *et al.* [24] proposed an idea for the advancement of the Handshake Protocol in the SSL/TSL layer for the authentication of client–server pair and secret key share. It substitutes the RSA/DSA certificate exchange with the projected PUF-based scheme. The modules are implemented in *OpenSSL* for the validation purpose.

In the sector more related to consumer-oriented IoT, Rahim *et al.* [25] demarcated the block chain and sensor-based PUF authentication mechanism grouping for the purpose of resolving the real-time nonrepudiable access to IoT devices in a smart home. This is done by the exploitation of a mining less consensus mechanism for the establishment of immutable pledge to transactions, including commands, status alerts, and actions of the users and IoT devices. Das *et al.* [26] presented a novel lightweight authentication scheme, which is suitable for

the wearable device. It allows the users for mutually authenticating their devices with mobile terminal like the android or the *iOS* device and for creation of session key between the devices in order to secure communication between the wearable device and the mobile terminal. The authors also presented a security analysis of the proposed scheme using the popular Real-Or-Random model. They used the automated validation of Internet security protocols and applications (AVISPA), a common formal security verification tool, in the analysis. It should be note that the proposed scheme uses only the hash function and the XOR operations for the resource-limited wearable devices. The proposed protocol has shown low computation and low communication costs, with better security and functionality features.

Additionally, for the applications to smart devices, Xie *et al.* [27] demonstrated a lightweight privacy-preserving two-factor authentication scheme for IoT devices. In their scheme, PUF is used as an authentication factor. The IoT device can anonymously and easily communicate with the server, which is located at the data and control unit. The proposed scheme is robust, efficient, and resistant against attacks. Also, Das *et al.* [28] proposed a biometric-based privacy preserving user authentication (BP2UA) scheme for the cloud-based IoT deployment. BP2UA has strong authentication between the users and smart devices by the key agreement among the smart devices and the gateway. The real-or-random model is used by the BP2UA for security analysis of the scheme. The *BP2UA's* practical demonstration is done by the *NS2* simulation. It was found that the scheme is robust and has low communication and computation overheads. Then, Aman and Sikdar [29] addressed certain problems that the previous related works were having and attempted to ensure hardware security. The authors presented hybrid protocols for attestation, which use PUF, to provide attestation and mutual authentication for IoT devices and the verifier. One proposed protocol is for attestation for a single device whereas another is for attestation of multiple identical IoT devices. Within them, PUFs are used in the protocol to generate secrets and deliver the mutual authentication. The scheme is resilience against physical and cloning attacks.

Even more for IoT security and authentication, Chatterjee *et al.* [30] developed a lightweight identity-based cryptosystem appropriate for IoT secured authentication and message exchange among the devices. The scheme employs PUF for the public identity generation for each device. The identity is then used as a public key in each device for message encryption. The protocols implementation also involves low hardware and software overheads. Rostami *et al.* [31] developed a mechanism for the operation of a prover device and a verifier device. The objective is to properly verify the authentication of the prover device by the verifier device. Data string is generated by the prover device by means of submitting a challenge to PUF and then achieving the response string. From the produced response string, a substring is selected, which is then injected into the data string. Additionally, random bits are injected into the bit positions of the data string that has not been allotted to the selected substring. Based on the challenge, the verifier further generates a projected response string by evaluating a computational model of the PUF. A search process is performed by the verifier for the purpose of identifying the designated substring within the data string using the estimated response string. In this manner, the verifier can determine whether or not the prover device is trustworthy on the basis of the degree of similarity between the identified substring and its corresponding substring of the estimated response string.

Moreover, Aman *et al.* [32] introduced a mutual authentication protocol for the IoT devices. The scheme is efficient and resilience against attacks, such as the physical attack and cloning attack. PUF is used in the proposed scheme in order to provide protection to the physically unguarded devices and to avoid storing information in the devices. Under this proposed protocol, storage and communication costs as well as the computational complexity are very low.

There have been recent works taken into account of lightweightness and authentication concurrently in IoT. Huth *et al.* [33] proposed a provably secured and lightweight authentication protocol. It attempts to simultaneously resolve the privacy and lightweightness issues with the use of both PUF and channel-based key agreement (CBKA). Previous studies addressed or resolved either the issue of privacy or lightweightness independently. The proposed scheme uses CBKA with amended definition and provides solution to the flaw in the PUF-based authentication protocol when an outsider-chosen perturbation security cannot be definite. Another recent development can be found in [34]. It proposed to embed a PUF-based authentication key exchange (AKE) and broadcast authentication (BA) protocols in RFID to simultaneously address the lightweight and authentication issues. The protocol is memory leakage resilient. Idriss *et al.* [35] implemented strong delay-based PUF to perform an accurate evaluation to integrate the area footprints of different PUFs. Factoring and examination of the PUF implementation cost shows that some of the enhanced PUF designs actually turned out to have poorer efficiency compared to their simpler counterparts.

There have been an abundance of advancement in authentication associated with IoT devices. Qureshi and Munir [36] proposed the PUF-IPA, which is a strict PUF-based identity preserving protocol for IoT device authentication. The protocol provides resilience against security attacks, such as the brute force attack, replay attack, and more. The PUF's response accuracy is improved from 89% to 98% using this proposed protocol. The protocol also preserves the identities of the devices and implements strong and controlled logic. Ayub *et al.* [37] proposed an identity-based three-party authentication and key exchange protocol that utilizes PUF to protect stored confidential information. The authors also introduced an efficient protocol based on a fuzzy extractor. The protocol is resilient toward security attacks and has low computation and communication overheads. Moreover, De Smet *et al.* [38] presented a mutual authentication scheme based on PUF for a fog architecture. It is resistant to security attacks, information attack, and others. Symmetric key encryption and decryption operations are used in the proposed protocol with good

performance. Gope *et al.* [39] proposed an anonymous novel authentication scheme using PUF for RFID-empowered UAV applications. Security and performance analysis of the protocol showed that the protocol is secured and efficient. Likewise, Chikouche *et al.* [40] proposed a privacy-preserving authentication protocol based on ECC. The authors proposed an enhanced code-based authentication protocol for IoT. The protocol is resilient to various security attacks, replay attacks, desynchronization attacks, and so forth. The performance analysis of the proposed protocol showed that the protocol is efficient and reliable. Lo and Yohan [41] proposed an authentication protocol that is lightweight, robust, and based on bluetooth low energy (BLE). The authentication protocol generates a secured unique session key. Li *et al.* [42] proposed a three-factor anonymous authentication scheme for WSNs in the IoT environment. The proposed protocol is computationally efficient and has more security features than peers. Challa *et al.* [43] introduced a new signature-based authentication key establishment scheme for the IoT environment. The proposed protocol is tested using the Burrows-Abadi-Needham logic and the AVISPA tool for informal security analysis. It is implemented using the widely accepted NS2 simulator. Zhou *et al.* [44] demonstrated an efficient authentication scheme for IoT. It is implemented in conjunction with the cloud servers using lightweight cryptographic modules like the one-way hash function and the XOR operation. The formal verification of the protocol is done via Proverif, which guarantees the security robustness of the proposed scheme. Gope *et al.* [34] developed a lightweight PUF-based privacy-preserving authentication protocol for the RFID system. The proposed protocol, which is secured and efficient, is effective for the RFID tags with efficient security features. Li *et al.* [45] proposed a certificateless public-key cryptography (CL-PKC) under the concepts of elliptic curve and PUF-based end-to-end mutual authentication and key exchange protocol for the IoT. The proposed protocol is secured against attacks and provides forward secrecy. The protocol also achieves the design goals of the three handshakes with no real participation of the server. Aman *et al.* [46] proposed protocols for the data provenance with authentication and privacy preserving in IoT systems. It is operated in an environment where one protocol is for the IoT device connected directly to the wireless gateway whereas another protocol for the IoT device connected indirectly to the wireless gateway via multiple hops of other IoT devices. The PUF-based protocols are efficient in terms of computational complexity and energy requirements. Barbareschi *et al.* [47] presented the physical hardware-enabled mutual authentication protocol (PHEMP) that attains mutual authentication in one-to-many communication phase using the PUF technology, which helps the communicating bodies to achieve synchronization. The proposed protocol is robust and resilient toward security attacks. It is implemented on FPGA belonging to the Xilinx Zynq-7000.

For practical authentication applications to secured business transactions via IoT devices, for example, Frikken *et al.* [48] used PUF in their scheme for the improvement of the protocol's resistance to several attacks. In particular, the user uses the bank-issued PUF and password. The protocol is secured and contains high security features. These include no user being able to get the authentication without his/her own device, the device not being able to be cloned, and the user not being able to be impersonated even the details of the authentication record and personal information are obtained by an attacker. The authors also added a protective mechanism to the scheme.

Section IV outlines recent PUF-based AKA research and proposed protocols in the IoT area. The section briefly describes the mechanics of these protocols and the implementation methods in various settings, including health, telecommunication, and more. Their strengths and weaknesses are discussed and possible remedies are suggested. Table III summarizes the descriptions of PUF works among IoT-related research papers examined in this survey and Fig. 4 delineates the categorization of the research works for IoT on the basis of cryptographic operations and the entities present in the architectures.

TABLE III
DESCRIPTION OF THE IOT-RELATED RESEARCH PAPERS

Protocols	Description
Haji *et al.* [8]	*SRAM-PUF* and *ECC*-based communication architecture verified on *Xilinx Zynq-7000 APSoC*
Boke *et al.* [11]	Various methods of key generation techniques and advance *IoT* devices designs
Bansal *et al.* [12]	*EVs* and charging stations security using *SUKA* protocol
Wang *et al.* [13]	Innovative *PUF* application as an entropy pump verified on *Nexys 4 DDR FPGA* board
Barbareschi *et al.* [14]	*PUF*-based mutual authentication scheme *CE* system devices
Liu *et al.* [15]	Protected data transmission and authentication for *IoT* devices
Jiang *et al.* [16]	*PUF*-based *AKA* protocol
Byun *et al.* [17]	textitPUF-MAKE protocol
Barbareschi *et al.* [18]	*PUF*-based Mutual authentication scheme for fog and textitIoT devices
Liang *et al.* [19]	*TSMCA*-based *PUF* in *RFID* system
Melki *et al.* [20]	Lightweight secure multi-factor device authentication scheme for IoT devices
Garg *et al.* [21]	Robust lightweight and provably secure *AKA* scheme for *IoT*
Suganthi *et al.* [22]	End to end mutual authentication protocol for privacy protection in healthcare
Braeken *et al.* [24]	Efficient identity-based *AKA* protocol for *IoT* devices using *PUF*
Rahim *et al.* [26]	Block-chain and sensor-based *PUF* authentication for smart home *IoT* devices
Das *et al.* [27]	Novel lightweight authentication scheme suitable for wearable device
Xie *et al.* [28]	*PUF*-based Lightweight authentication for *IoT* devices
Kumar *et al.* [29]	*BP2UA* scheme for the cloud-based *IIoT*
Aman *et al.* [30]	*PUF*-based hybrid protocol for mutual authentication of *IIoT* devices and verifier
Chatterjee *et al.* [31]	Lightweight Identity-based cryptosystem for *IoT* devices using *PUF*
Rostami *et al.* [32]	Verification operation of authentication of prover by verifier device using *PUF*
Chua *et al.* [33]	Mutual authentication protocol for the *IoT* devices
Idriss *et al.* [36]	Strong delay-based *PUFs* evaluation for *IoT* devices
Qureshi *et al.* [37]	*PUF-IPA* protocol
Ayub *et al.* [38]	Identity-based three party *AKA* protocol using *PUF*
Ruben *et al.* [39]	Mutual authentication scheme based on *PUF* for a fog architecture
Chikouche *et al.* [41]	Privacy preserving authentication protocol based on *ECC* for IoT
Lo *et al.* [42]	Light-weight and robust authentication protocol based on *(BLE)*
Frikken *et al.* [49]	*PUF*-based protocol for increasing of protocol's resistance to attacks

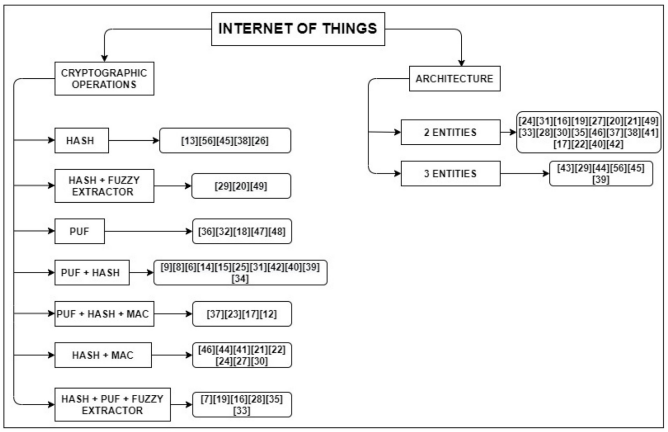

Fig. 4. IoT categorization.

V. PUF User Authentication and Key Agreement for WSNs

In the previous section, we focus on PUF-based AKA research and security enhancement for IoT. In the current section, we shift the focus to the domain of WSN and relevant areas. Gope *et al.* [49] proposed a lightweight and privacy-preserving mutual authentication protocol for users. Only the users with trusted device is granted the authority to access the industrial WSN (IWSN). The protocol uses lightweight cryptographic primitives, such as PUF, bitwise exclusive operations, and one-way cryptographic hash function, and creates for the sensor nodes physical layer security. In IWSN, a crucial requirement is a user's ability to directly access the real-time information from selected sensor nodes. It follows that the scheme should still provide security when these nodes are compromised. According to the study, the proposed scheme is demonstrated to be secured and efficient for resource-constrained sensing devices in IWSN. On the other hand, it is difficult to obtain confidentiality and mutual authentication in the WBAN because of a variety of attributes, such as reliability, energy efficiency, and the hardware constraints. Thus, an adversary is able to attain information. This deficiency raises the need of an efficient mutual authentication along with the confidentiality so as to provide anonymity and untraceability of data sharing among sensor nodes. Like [49] and [50] proposed a lightweight privacy-preserving mutual user authentication scheme in that authenticated users and devices are given the authority to access the IWSN. It is claimed that the proposed protocol embraces efficiency and security. The scheme should still be secured even any sensor node(s) is (are) captured by the attacker. The lightweight cryptographic primitives, such as the one-way cryptographic hash function, PUF, and bitwise exclusive operations (XOR), are used in the scheme. The proposed scheme is secured and efficient for the resource-controlled sensing devices in IWSN. Kumar *et al.* [51] developed a PUF-based protocol tailored for the characteristics and deployment of IWSN. It is resilient toward malicious security acts, including user device loss, denial of service attack, and more. Formal security analysis of the proposed protocol is done using the random oracle model and formal verification of security is done by the ProVerif tool. Alzahrani *et al.* [52] created an improved AKA scheme for wireless body area networks (WBAN). The proposed scheme employs BAN logic for security analysis and the ProVerif as an automated simulation tool. This article also examined Xu *et al.*'s protocol and discussed its vulnerabilities.

While there exist a number of studies targeting authentication between sensors and the control unit (CU), most of them fail to examine the mutual authentication issue in depth. Among the few, Xie *et al.* [53] proposed a PUF-based lightweight mutual authentication mechanism for body area network (BAN) sensors. As mentioned earlier, BAN is typically resource constrained, which makes the adoption of PUF more appealing. Here, the control unit is used as the midpoint and network sensors can establish secured communication in a manner that the authenticity of data exchange is maintained. Sensors are not required for encryption and thus, ease the burden on the restricted resources in BAN nodes. The design comes with low overheads and is able to protect the network from various forms of vulnerability.

Gope and Hwang [54] proposed an AKA protocol for unattended and hostile deployment in WSN. The PUF-based protocol allows anonymous user authentication with cost-efficiency in both communication and computation. These features make the proposed protocol appealing to be adopted in the often resource-constrained WSN. Turknovic *et al.* [55] developed a scheme in which a remote user using a lightweight AKA protocol can exchange session key with sensor node in order to facilitate mutual authentication between the communicating nodes. It should be noted that the user is not able to access the gateway nodes under this design. Specifically, the authors proposed the use of PUF for the AKA mechanism in heterogeneous *ad hoc WSNs*. The design tackles the WSN's resource-constrained architecture and uses simple hash and XOR operations in relevant computation. The protocol provides features, such as password protection, free password choice, and dynamic node addition, in addition to some high-end security features, including insider attacks, resistance to impersonation, and smart card breach. For WMSN, Wu *et al.* [56] constructed a new authentication protocol based on a novelty concept and compared its performance with those of other contemporary counterparts. The analysis found out the proposed scheme is efficient and resistant to various forms of attacks. The proposed scheme is formally verified by the Proveif.

The PUF technology has been pervasively applied to WSN security in healthcare. For example, He *et al.* [57] presented a robust anonymous authentication scheme for networks deployed in the health care sector, especially for the wireless medical sensor network (WMSN). In summary, the scheme consists of four phases—1) registration; 2) login; 3) authentication; and 4) password change. The proposed scheme is resilient against a variety of security loopholes, such as privileged insider, offline password guessing, stolen smart card, and replay attacks. It is found to be efficient and incurs low overheads. Khan and Kumari [58] proposed a secured protocol for user authentication in healthcare services through WMSNs. The design embraces mutual authentication as well as session AKA among different devices within the network. The scheme

provides major security features to protect against password guessing, insider, user impersonation, sensor node impersonation, and multilogged-in attacks. Srinivas *et al.* [59] presented a lightweight PUF-based scheme for security enhancement of AKA. The proposed scheme is tailored for the healthcare applications in the WMSN environment. The protocol is found to be computationally efficient and performed well in security analysis. Salam and Khan [60] developed a cross-layer protocol for AKA for healthcare applications running on WSN. The PUF-based protocol meets the requirements specific to heterogeneous BAN. Through cooperation and adaptability, it can be implemented over most existing WSN or wireless infrastructures with high network reliability and energy efficiency. The protocol also improves reliability throughput, packet delivery ratio (PDR), and energy consumption for mobile networks using conventional BAN protocols.

Not only in the healthcare sector but also the PUF-based AKA technology can be found in a handful of commercial applications. Kompara *et al.* [61] discussed the weaknesses in the untraceability provision and proposed a novelty AKA scheme with application in smart grid. This article analyzed existing mutual authentication designs for the two-hop WBANs along with the anonymous and untraceable key establishments. The proposed scheme addresses these two issues and is further shown to be efficient. The informal analysis tool Scyther and AVISPA are used to perform security analysis of the protocol and subsequently validated with the use of BAN logic. This article also stipulated that there exist multiple cryptographic protocols designs for secured communication over smart grid systems; however, the current protocols generally does not support conditional anonymity feature and elastic key management. Wang *et al.* [62] discussed a blockchain-based AKA protocol for smart grid systems utilizing edge computing. Via blockchain, the protocol is able to synthesize efficient conditional anonymity and key management deprived of any complex cryptographic primitives. Security analysis demonstrates that the proposed scheme accomplishes reasonable assurance and is an ideal candidate in a smart grid deployment. Similarly, for applications in the blockchain, Patil *et al.* [63] presented a new AKA protocol utilizing PUF. Data provenance and data transparency are maintained by the proposed protocol. The study reported that it is reliable and computational and energy efficient. Zhu *et al.* [64] proposed a lightweight PUF-based mutual authentication protocol for radio-frequency identification (RFID), a widely used technology associated with the deployment of IoT. Despite its popularity, RFID exhibits a number of security and privacy issues. They pose threats not only to customers/users but also to potential losses due to cloning of tags. In light of these weaknesses, many PUF-based authentication protocols are proposed in the literature for enhancement of counterfeiting feature. Unfortunately, many schemes embrace tags with secret parameters warehoused, making them prone to physical attacks. Li *et al.* [65] proposed a PUF-based group key transfer protocol for Bluetooth. It establishes shared group key between Bluetooth master and slave devices where the slave devices does not store any secret or private parameters. In their scheme, PUF creates a mapping relationship based on the device's physical characteristics. Despite some studies illustrated otherwise, this article stipulated that this group key approach ensures security in Bluetooth broadcast messages. The proposed scheme is expected to resist attacks, including eavesdropping, tampering, replaying, and replication attack. The scheme entails higher security level with relatively minor computation, storage, and communication overheads. Similarly, Lo and Yohan [41] proposed a lightweight protocol based on PUF for generating robust AKA for BLE devices. The proposed protocol creates a unique and secured key for each session. From a different angle of application, Miao *et al.* [66] proposed an algorithm for autonomous deployment of WSN sensor nodes in the 3-D space with obstacles. Simulation results from the study suggested that the 3-D virtual force model is harnessed well and rapid during the process of the 3-D self-deployment (3DSD). Also, the nodes in the system are well distributed and defined. Naqvi *et al.* [67] focused on multifaceted applications of WSN comprising of unmanned aerial vehicles and presented an overview avenues of deployment with air-to-ground channel features. Those include drones in military surveillance and for work in disaster struck areas. Their discussions involve the use of PUF-based AKA to build resilient public safety WSN.

Aman *et al.* [68] presented a lightweight mutual authentication protocol for IoT wearable devices operating in WSN. Wearable devices are widely used but the users suffer the risk of privacy because private information is collected from the IoT devices, such as glasses and watch. The data are usually stored in remote cloud server and mobile terminal such as smartphone. They are traditionally prone to security breaches and are totally unfit for communication. The proposed protocol is robust toward different attacks but also very efficient in computation, memory, energy, and computation overheads. In another study, Wu *et al.* [69] developed, a lightweight authentication scheme for wearable devices used in conjunction of cloud server. It is designed to address a number of security concerns found in WSN-operating IoT devices. Additionally, Aman *et al.* [70] presented a PUF-based lightweight mutual authentication protocol to be used in real-time applications and IoT devices over the WSN system. Because of the specific characteristics in this environment, the design of hardware protocol must embrace not only security but also efficiency in chip usage, storage, energy, and processing capacity. The proposed protocol can be implemented in two setups—1) when an IoT device and the server communicate or 2) when two IoT devices establish a session to communicate. A security and performance analysis of the protocol indicated robustness against various attacks and high efficiency in computing, memory, energy consumption, and overheads. However, its inexpensive and simplicity nature also make it vulnerable to physical, side channel, and cloning attacks. Li *et al.* [45] proposed an end-to-end mutual authentication and key exchange scheme for IoT based on PUF. Also, Siddhartha *et al.* [71] presented a lightweight PUF-based mutual AKA protocol for authentication between IoT devices in a network environment. It is stipulated that the proposed protocol is resilient against acts, such as replay, masquerade, and MITM attacks. The study also claimed that the AKA

protocol is reliable while energy and computational efficient and reliable. Li *et al.* [42] proposed a three-factor anonymous authentication scheme for WSNs in the IoT environment. The proposed protocol is computationally efficient and has more security features.

Because of the advancement and rapidly increasing global demand of telecommunication, many research studies focus in this area. For example, Ferrag *et al.* [72] examined existing protocols, surveys, and privacy-preserving schemes related to *4G* and *5G* cellular networks. This article presented a classification taxonomy of threat models for *4G* and *5G* networks. Subsequently, the authors provided a follow-up scheme to categorize countermeasures. It involves three categories—1) cryptography methods; 2) human factors; and 3) the intrusion detection methods. The study also performed a formal security analysis on countermeasures of various authentication and privacy-preserving schemes. Li *et al.* [73] surveyed on UAV communication toward 5G/beyond 5G (B5G) wireless network. They also discussed the space-air-ground integrated networks, the 5G techniques based on the UAV platform and the research challenges in integrated network architectures. A survey study but focusing on different subject, *M87* performed a survey on the unmanned aerial vehicle communication in the 5G/beyond 5G B5G wireless networks. Space-air-ground-integrated networks are also included. In addition, this article discussed recent research works on UAV communication and the *5G* technologies/techniques. Ullah *et al.* [74] examined the benefits of *5G* and explored three cases of application—1) vehicle-to-everything (V2X) communication; 2) drones; and 3) healthcare. The authors also presented an overview of online consultation and health monitoring, remote diagnosis, and mobile robotic surgery. Meng *et al.* [75] developed a PUF-based *5G* wireless system to be used for aerial vehicles (drones). The system encompasses base station, user equipment, and unmanned aerial vehicle. The proposed scheme works in a secured manner such that the drone sends its position signals to the base station as the backhaul and the drone is also able to receive back fronthaul signal from the base station. From a different perspective, the AKA protocol suggested by Amin *et al.* [76] is used for one-time password generation. The protocol is based on CRP and symmetric cryptography, which enhance confidentiality of user identity. The PUF-based AKA captures salient features, such as flexibility in credentials, DoS resistance, and efficiency when deployed in UMTS and CDMA. Because of that the proposed protocol can be widely adopted in e-commerce and business trading/transaction platforms. The inherent AKA permits devices to mutually authenticate one another and exchange authenticated session key or secret key over the network.

Koulali *et al.* [77] focuses on beaconing period's scheduling as for of efficient means of energy consumption optimization. The authors of the article provided a learning algorithm that ensures UAV network convergence with its unique Nash equilibrium operating point where they constructed a noncooperative game and characterized the equilibrium beckoning period duration for the purpose of competing the drones.

For verification, Wazid *et al.* [78] designed a secured lightweight three-factor scheme termed the user authenticated key management protocol (UKAMP). It is specifically adapted for HIoTNs remote user authentication. UKAMP offers a number of special functionalities. Informal security analysis by the ROR model and the formal security verification using AVISPA were performed to confirm the validity. Serving a similar purpose, Byun [79] presented a new PUF-based general multifactor authentication key exchange (MAKE) based on the secured password-based AKE protocol. It claims that in the event of the authentication factors being compromised, the MAKE construction maintains secured with PUF in the device. The construction requires additional three communication flows with no public key-based primitives like signature. Yet for WSN, Das *et al.* [80] provided a new user-password AKA protocol for improved security and efficiency. Under this scheme driven by PUF, a user can authenticate his/her identity at either the base station or the cluster heads from where data are accessed. It is claimed that the proposed protocol exhibits efficiency in terms of communication and computation while being resilient to attacks, including masquerade, privileged insider, smart card breach, and DoS attacks. The inherent mechanism also supports dynamic nodes addition. Similarly, Ever [81] proposed an anonymous user AKA scheme that has improved security measures and performance, such as lowered computation and communication overheads. ECC is used in the protocol design to make it resistant to password guessing and smart card stolen attacks. The protocol was simulated by the AVISPAs for formal verification and validated further safeguard against replay, password guessing, man-in-the-middle, secret key disclosure, and impersonation attacks. Kumar *et al.* [51] used PUF, XOR, and one-way cryptographic hash operations in their AKA protocol for verification. ProVerif tool is used to conduct for formal security analysis.

Moreover, for verification through hardware devices, a security-enhanced authentication and AKA scheme is proposed in Park and Park [82]. The PUF protocol uses biometric information and functions with elliptical curve cryptosystem. This article also benchmarked with Chang *et al.*'s scheme and found that the proposed protocol is more robust to attacks (e.g., offline password guessing attack) and less likely to yield forward secrecy. Amin *et al.* [83] proposed an efficient remote mutual authentication scheme for AKA via smart card. The PUF-based protocol was tested using the AVISPA tool. It was shown that the protocol is secured against both active and passive attacks. Amin *et al.* [84] also worked with smart card. It presented a PUF-based AKA protocol (smart card) in a distributed cloud environment where the user can securely access private information from the servers. This protocol is based on both the BAN logic and is tested by the AVISPA tool. Furthermore, Byun [85] proposed a PUF-based protocol for AKE. It secures the authentication of session key between end users in WSN. The protocol is reported to be resistant to security loopholes and suitable for implementation on centralized networks. Xie *et al.* [27] proposed a novel dynamic ID-based anonymous scheme. The proposed protocol incurs low computation and bandwidth costs. Herder *et al.* [86] demonstrated the use of PUF technology for facilitating low-cost AKA and for related areas such as key generation. Both strong and weak PUFs are discussed in this article along with

their implementations and their applications. The papers also provided conceptual exposition of PUF foundation and various implementation techniques.

Additional work supporting PUF-based AKA and its functionality can also be found in the WSN-centered literature. For instance, Das *et al.* [87] designed an AKA protocol using elliptical curve cryptography. It is then verified by the AVISPAs tool. Chang and Le [88] reviewed Turkanovic *et al.*'s scheme, which is known to be vulnerable to security attacks, and proposed two AKA schemes over WSN as a remedy. The authentication scheme is reported to be efficient and results in perfect forward secrecy. Quan *et al.* [89] examined a number of user authentication protocols and proposed a secured AKA protocol based on identity cryptography for high security WSN. Jiang *et al.* [90] proposed an ECC-based untraceable two-factor authentication scheme for WSNs that satisfies the mutual authentication in BAN logic and provides additional security features. Amin *et al.* [91] proposed a two-factor user AKA scheme with RSA cryptosystem for the multiserver environment.

In the world of networking, Wang *et al.* [92] applied PUF and designed an array of mutual authentication mechanisms for sensor pairs and sensor groups in the body area network (BAN). BAN sensors can affect medical equipment's controls. Hence, their authenticity and data integrity are imperative to patient's safety assurance. However, resources in a typical BAN are limited; thus, there has been an increased focus on exploring the potential of PUF as an alternative solution. Existing protocols only concern with the authentication procedure between control unit and sensors with little focus on mutual authentication among sensor pairs and/or sensor groups. The proposed scheme in this article does not require sensors for encryption operations and thereby reduces burden on the hardware. This feature is very suitable for resource-constrained BAN. It is stipulated that the proposed probability-based scheme is resilient against multiple types of attacks such as the collusive sender impression attacks. Also, it incurs low overheads. Alzahrani *et al.* [52] proposed an AKA protocol for the wireless body area network. The PUF-based protocol uses BAN logic analysis and the ProVerif automated simulation tool for security analysis. Afghah *et al.* [93] studied the PUF deployment in SDWN, i.e., software-defined wireless networking. Typically, since the power and computation capacity for most IoT devices are insufficient and the authentication mechanism between controllers and forwarding devices in SDWN has become a critical challenge to both integrity and security of the system. Hence, a new approach to SDWN centralized management and decision making is needed to protect the network. Afghah *et al.* [93] proposed a PUF-based security protocol for the network. Their scheme incorporates digital PUFs utilizing the inherent randomness nature of the nanomaterials found in ReRAM. The study also included a performance analysis of the ReRAM-based PUF. Likewise, the efficiency of the proposed multistate machine learning technique was examined in terms of prediction of PUF's response drifts due to varying temperature and partial conditions.

Table IV concludes Section V by summarizing the WSN-related PUF-based AKA protocols. Essentially, the section

TABLE IV
DESCRIPTION OF THE WSN-RELATED PROTOCOLS

Protocols	Description
Lo *et al.* [42]	*BLE*-based Light-weight robust authentication protocol
Li *et al.* [46]	End-to-end mutual authentication and key exchange scheme for IoT
Gope *et al.* [50]	Lightweight privacy-preserving mutual user authentication protocol
Osama *et al.* [51]	Lightweight privacy-preserving mutual user authentication scheme for *IWSN*
Xie *et al.* [54]	*PUF*-based Lightweight mutual authentication mechanism for *BAN* sensors
Hwang *et al.* [55]	Authentication protocol for the *WSNs* guaranteeing security features
Wu *et al.* [57]	Authentication protocol for *WMSNs* verified via Proveif.
He *et al.* [58]	Robust anonymous authentication protocol for *WMSN*
Khan *et al.* [59]	Secure user authentication protocol for *WMSNs*
Srinivas *et al.* [60]	Lightweight authentication protocol efficient for *WMSN*
Kompara *et al.* [62]	*AKA* scheme for two-hop *WBANs*
Wang *et al.* [63]	Blockchain-based mutual *AKA* protocol for the edge-computing-based *SG* systems
Patil *et al.* [64]	Blockchain and *PUF*-based efficient privacy-preserving authentication protocol
Zhu *et al.* [65]	Lightweight *RFID* mutual authentication protocol with *PUF*
Li *et al.* [66]	*PUF*-based group key transfer protocol for Bluetooth
Aman *et al.* [69]	Lightweight efficient mutual authentication protocol using *PUF IoT* systems
Wu *et al.* [70]	Lightweight authentication scheme using cloud server for wearable devices
Aman *et al.* [71]	*PUF*-based Lightweight mutual authentication protocol for *IoT* systems
Valmiki *et al.* [72]	Lightweight mutual *AKA* protocol between *IoT* devices
Ferrag *et al.* [73]	Classification of threat models in *4G* and *5G* cellular networks
Byun *et al.* [80]	*PUF*-based *MAKE* protocol
Das *et al.* [81]	Password-based user authentication protocol for *WSNs*
Yoney *et al.* [82]	Anonymous user authentication scheme simulated *AVISPA* for formal verification
Wang *et al.* [93]	Mutual authentication mechanisms for *BAN* sensor pairs with *PUF*
Afghah *et al.* [94]	*PUF*-based novel security protocol for *SDWNs*

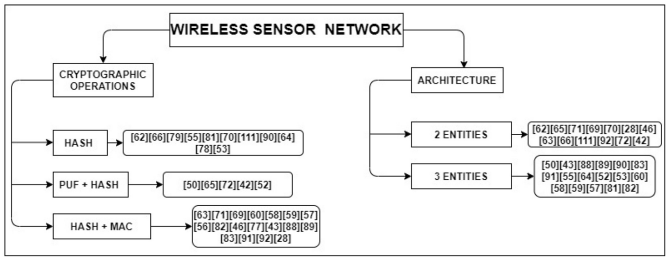

Fig. 5. WSN categorization.

overviews relevant developments in this research stream and examines possible strengths and weaknesses of proposed protocols during implementation. In addition, Fig. 5 presents the cryptographic operations and entities in a typical WSN setting.

VI. COMPARATIVE DISCUSSION ON PUF USER AUTHENTICATION AND KEY AGREEMENT IN SMART GRID

In the previous two sections, we provided comparative discussions based on the literature survey in the areas of IoT and WSN. We shift the focus of review in the current section to PUF and AKA research developments in the smart grid area.

Operating within an Internet-based smart grid environment, systems equipped with secured and efficient key exchange or AKA are of critical importance. Smart meter (SM) is a fundamental networking device linked to a power grid

TABLE V
DESCRIPTION OF THE SMART GRID-RELATED RESEARCH PAPERS

Protocols	Description
Bansal *et al.* [12]	*SUKA*) protocol for *V2G* system
Ghosal *et al.* [101]	Highlights the *KMS* significance *AMI* security in *SG*
Gope *et al.* [102]	Novel privacy-aware *AKA* scheme for smart meters
Tahavori *et al.* [103]	*PUF*-based Light-weight *AKA* and end-to-end key agreement scheme
Saeed *et al.* [104]	Novel provably secure broadcast one-way hash function based authentication protocol
Gope *et al.* [105]	*PMAKE* Scheme for *AMI* in *SG*
Reza *et al.* [106]	Security mechanism combining *ECC* and *Saalsa20* stream cipher algorithm
Bhanse *et al.* [107]	Secure authentication scheme using *VRF* for *AMI* in *SG*
Braeken *et al.* [109]	Provably secure key agreement model for smart metering communications
Malik *et al.* [110]	Demonstration of challenges and necessity for the authenticated approaches in *SG* system
Gope *et al.* [111]	Efficient authentication and privacy-preserving protocol for *EI*-based *V2G* communication
Kaveh *et al.* [112]	Privacy aware authentication protocol for *V2G* communications
Banerjee *et al.* [113]	Novel lightweight anonymous user authentication scheme for *IoT*
Das *et al.* [114]	Lightweight user *AKA*- scheme for *IoT* sensing devices in *IIoT* setting

TABLE VI
AVERAGE EXECUTION TIME USING MIRACL

Primitive	Average time on Raspberry PI 3 (in milliseconds)	Average time on server (in milliseconds)
T_h	0.309	0.024
T_{exp}	0.228	0.039
T_{ecm}	2.288	0.382
T_{eca}	0.016	0.002
T_{senc}	0.018	0.001
T_{sdec}	0.014	0.001
T_{mul}	0.011	0.004
T_{add}	0.010	0.002
T_{bp}	32.084	6.353
T_{mtp}	0.385	0.084

through communication network. Generally, SM is susceptible to physical attacks and network-based cyber-attacks because customers/users do not have proper hardware installed for protection. For the purposes of analysis and improvement of energy synchronization between customers and service providers, advance metering infrastructure (AMI) is often employed in bidirectional communications. The survey [100] focused on the key management system (KMS) (or AKA) and its significance to AMI. The review highlights key security issues associated with AMI and efforts on how key management technique can be used to safeguard the system. Challenges of the deployment of KMS are also discussed. This article outlined the differences between some outdated electric systems and smart grids.

As discussed earlier, SM is susceptible to physical attacks and network-based cyberattacks due to hardware issues. As a result, not only customer data from SM can be tampered and incorrect billing but, most importantly, demand and supply management of the power grid can be compromised and ended up in widespread outage. Hence, Gope and Sikdar [101] proposed a novel privacy-aware AKA scheme that to secure communications between SM and servers of the service provider. The PUF nature and one-way hash function of the scheme also promote additional security of the network of SMs. The design is ideal for resource-limited SM due to energy efficiency. In addition, Tahavori and Moazami [102] proposed a lightweight PUF-based AKA protocol to enhance the security of SG. The authors developed an end-to-end AKA scheme, which leads to resilience against physical, leakage, and other forms of attacks to the system. The scheme also has relatively lower computation and communication overheads. Likewise, Aghapour *et al.* [103] presented a novel provably secure broadcast protocol for AKA purpose. The concept is based on the unicast and broadcast technique and one-way hash function. The proposed scheme utilizes low storage overhead/requirement and is efficient in terms of communication and computational costs. It is stipulated that the scheme can resist against a variety of attacks.

In light of the security issues mentioned above, Gope [104] presented a PMAKE protocol designed for AMI in smart grid in order to promote the security of SM. The proposed protocol is claimed to be energy and processing efficient. On the other hand, Reza *et al.* [105] discussed a novel AKA security mechanism combining ECC and Saalsa20 stream cipher algorithm to enhance security of the network system. The development addressed and provided a remedy to energy efficiency and lightweight security issues. Specifically, the PUF-based protocol demonstrated both power and computational efficiency energy. These salient features make the proposed protocol appropriate for the adoption for SM because of reduced power consumption together with less time for encryption/decryption processes. Also, Bhanse *et al.* [106] designed a secure AKA scheme using the verified random function (VRF). The enhanced AMI is to be placed in smart grid along with PUF-based SM using the ECC security protocol. It should be pointed out that authenticity of SM data is imperative to the deployment of the smart grid network. SM communicates in a two-way fashion in that every node should be authorized and then secured for data transmission. The proposed protocol entails security and efficiency, as demonstrated by the study's performance and security analysis with the use of BAN logic. Also, related to these research works is [107], who proposed an authenticated key exchange AKE and BA protocol for the AMI in an SG setting. They proposed to install PUF in each SM and other devices to generate unique secret values. The PUF-based AKE and BA protocols are resilient to memory leakage resilient and efficient in terms of communication and computation overheads. Braeken *et al.* [108] presented a secured PUF-based AKA model for SM communications. The scheme is claimed to maintain security over the SG system and also offer higher resistance against the DoS attack.

Qasaimeh *et al.* [109] discussed the challenges and urgency for the development of AKA measures and protocols for SG. SG is commonly viewed as a likely replacement of the currently outdated power grid and is setting the trend for future in the energy sector. In terms of security, SG requires two-way communication between service provider and consumers,

TABLE VII
COMPUTATIONAL COST ANALYSIS OF IOT WITH IOT DEVICE AND SERVER AS THE ENTITIES

Protocols	IoT Device	Server	Total (ms)
Jiang *et al.* [16]	$13T_H + 2T_{PUF} + 2T_{GEN} + 2T_{SE} + 2T_{AE}$	$9T_H + 2T_{REP} + 2T_{SX} + 2T_{AD}$	1.468
Liang *et al.* [19]	$T_H + 2T_{PUF} + 2T_{XOR}$	$2T_H + 2T_{PUF} + 3T_{XOR}$	6.792
Melki *et al.* [20]	$5T_H + 5T_{XOR}$	$5T_H + 5T_{EXP} + T_F$	10.24
Garg *et al.* [21]	$4T_H + 3T_{EM}$	$8T_H + 6T_{EM}$	0.324
Braeken *et al.* [24]-P1	$5T_H + 3T_{EM} + 1T_{EA}$	$10T_H + 1T_{EM} + 2T_{EA}$	1.894
Braeken *et al.* [24]-P2	$2T_H + 1T_{EM}$	$2T_H + 3T_{EM} + 1T_{EA}$	1.626
Das *et al.* [27]	$6T_H + 3T_{XOR}$	$10T_H + 4T_{XOR}$	7.384
Xie *et al.* [28]	$FE.GEN + 5T_H + 2T_{PUF}$	$FE.REC + 2T_H$	1.028
Aman *et al.* [30]	$T_{MAC} + T_{ENC} + T_{ECC} + T_{ECCx}$	$T_{MAC} + T_{ENC} + T_{ECCx}$	0.77
Chatterjee *et al.* [31]	$4T_H + 3T_{PUF}$	$6T_H$	1.53
Chua *et al.* [33]-P1	$1T_H + 3T_{MAC} + 3T_{XOR}$	$3T_H + 3T_{MAC} + 3T_{XOR}$	5.48
Chua *et al.* [33]-P2	$5T_H + 5T_{MAC} + 7T_{XOR}$	$7T_H + 5T_{MAC} + 10T_{XOR}$	5.951
Gope *et al.* [35]-P1	$4T_H + 2T_P + RNG$	$4T_H + RNG$	1.052
Gope *et al.* [35]-P2	$5T_H + 2T_P + FE.REC + RNG$	$5T_H + FE.GEN + RNG$	1.1
Qureshi *et al.* [37]	$3T_H + 2T_P$	$T_{ENC} + 1T_{DEC}$	9.49
Ayub *et al.* [38]	$4T_H$	$4T_H$	1.96
Chikouche *et al.* [41]	$4T_H + T_{ENC}$	$5T_H + T_{DEC}$	0.218
Li *et al.* [46]	$12T_H + 14T_{em} + 4T_{ea}$	–	5.644
Frikken *et al.* [49]	$2T_H + 2T_{EXP}$	$1T_H + T_{EXP}$	4.11

Symbols: T_H- Hash Function, T_P- PUF Function, T_{GEN}- Generator Operation, T_{REP}- Reproduce Operation, T_{SE}- Symmetric Encryption, T_{AE}- Asymmetric Encryption, T_{SX}- Symmetric Decryption, T_{AD}- Asymmetric Decryption , T_{EXP}- Exponential Function , T_{XOR}- XOR Function, T_{MAC}- MAC Function, T_{ENC}- Encryption Function,T_{ECCx}- ECC Scalar point multiplication, $FE.REC$- Fuzzy Extractor Recover, RNG- Random Number Generator, $FE.GEN$- Fuzzy Extractor Generator, T_{EM}- ECC Point multiplication, T_{EA}- ECC Point addition, T_DEC- Decryption Function, $T_{e/d}$- Symmetric key encryption/decryption, T_{ECC}- ECC Function, T_{ecm}- ECC Scalar point multiplication,T_{FE}- Fuzzy Extractor, T_{GM}- Scalar Multiplication on G, T_{GA}- Scalar Addition on G, T_{MP}- Point Multiplication, T_{AP}- Point Addition.

TABLE VIII
COMPUTATIONAL COST ANALYSIS OF IOT WITH USER AND SERVER AS THE ENTITIES

Protocols	User	Server	Total (ms)
Byun *et al.* [17]	$5T_H + 2T_{ENC} + T_P$	$5T_H + 2T_{ENC}$	3.71
Suganthi *et al.* [22]	$4T_H + 2T_{ENC}$	$7T_H$	1.44
Ayub *et al.* [38]	$4T_H$	$4T_H$	1.332
Gope *et al.* [40]	$5T_H + 2T_P$	$5T_H$	2.525
Lo *et al.* [42]	$5T_H + T_P$	$4T_H + T_P$	2.501

Symbols: T_H- Hash Function, T_P- PUF Function, T_{ENC}- Encryption Operation.

TABLE IX
COMPUTATIONAL COST ANALYSIS OF IOT WITH USER, GATEWAY, AND SENSOR NODE AS THE ENTITIES

Protocols	User	Gateway	Sensor Node	Total(ms)
Kumar *et al.* [29]	$T_{FE} + 14T_H$	$9T_H$	$7T_H$	6.7
Ruben *et al.* [39]	$12T_H + 2T_P$	$12T_H + 2T_P$	$15T_H + 2T_P$	11.211
Li *et al.* [43]	$8T_H + 2T_{ECC}$	$9T_H + T_{ECC}$	$4T_H$	8.8
Challa *et al.* [44]	$5T_{ecm} + 5T_H$	$5T_{ecm} + 4T_H$	$4T_{ecm} + 3T_H$	23.16
Zhou *et al.* [45]	$10T_H$	$19T_H$	$7T_H$	5.714
Turknovic *et al.* [56]	$8T_H$	$8T_H$	$6T_H$	4.5

Symbols: T_H- Hash Function, T_P- PUF Function, T_{ECC}- ECC Function, T_{ecm}- ECC Scalar point multiplication,T_{FE}- Fuzzy Extractor.

TABLE X
COMPUTATIONAL COST ANALYSIS OF WSN WITH IOT DEVICE AND SERVER AS THE ENTITIES

Protocols	IoT Device	Server	Total (ms)
Xie *et al.* [28]	$6T_H + 3T_{EM}$	$5T_H + 3T_{EM} + 2T_{e/c}$	2.5
Li *et al.* [46]	$6T_H + 7T_{EM} + 2T_{EA}$	$6T_H + 7T_{EM} + 2T_{EA}$	5.64
Kompara *et al.* [62]	$3T_H + 4T_{XOR}$	$5T_H + 5T_{XOR}$	4.6
Zhu *et al.* [65]	$4T_H + 2T_{PUF}$	$5T_H$	0.646
Aman *et al.* [69]	$7T_H + 3T_{XOR}$	$6T_H + 4T_{XOR} + 2T_M$	1.076
Wu *et al.* [70]	$11T_H$	$7T_H$	0.43
Aman *et al.* [71]-P1	$1T_H + 2T_{MAC} + 3T_{ENC}$	$1T_H + 2T_{MAC} + 2T_{ENC}$	0.053
Aman *et al.* [71]-P2	$1T_H + 4T_{MAC} + 3T_{ENC}$	$2T_H + 4T_{MAC} + 4T_{ENC}$	0.079

Symbols: T_H- Hash Function, T_P- PUF Function, T_{XOR}- XOR Function, T_{ENC}- Encryption Function,T_{ECCx}- ECC Scalar point multiplication, T_{EM}- ECC Point multiplication, T_{EA}- ECC Point addition, T_DEC- Decryption Function, $T_{e/d}$- Symmetric key encryption/decryption.

TABLE XI
COMPUTATIONAL COSTS ANALYSIS OF WSN WITH USER AND SERVER AS THE ENTITIES

Protocols	User	Server	Total (ms)
Lo *et al.* [42]	$5T_H + T_P$	$4T_H + T_P$	2.5
Wang *et al.* [63]	$5T_H + 4T_{GM} + T_{GA}$	$6T_H + 4T_{GM} + T_{GA}$	12.38
Li *et al.* [66]	$T_H + 4T_{XOR}$	$T_H + 4T_{XOR}$	4.3
Valmiki *et al.* [72]	$4T_H + T_P$	$7T_H + 2T_P$	2.694
Islam *et al.* [92]	$6T_H + 2T_{EXP}$	$6T_H + 2T_{e/d}$	2.456
Gope *et al.* [111]	$6T_H$	$8T_H$	1.998

Symbols: T_H- Hash Function, T_P- PUF Function, T_{EXP}- Exponential Function , T_{XOR}- XOR Function, T_DEC- Decryption Function, $T_{e/d}$- Symmetric key encryption/decryption, T_{GM}- Scalar Multiplication on G, T_{GA}- Scalar Addition on G.

TABLE XII
COMPUTATIONAL COSTS ANALYSIS OF WSN WITH USER, GATEWAY, AND SENSOR NODE AS THE ENTITIES

Protocols	User	Gateway	Sensor Node	Total (ms)
Li *et al.* [43]	$8T_H + 2T_{ECC}$	$9T_H + T_{ECC}$	$4T_H$	8.5
Gope *et al.* [50]	$3T_{PUF} + 6T_H$	$9T_H$	$2T_{PUF} + 6T_H$	6.07
Kumar *et al.* [52]	$6T_H + 3T_P$	$11T_H + 2T_P$	$4T_H + 2T_P$	6.3
Alzahrani *et al.* [53]	$4T_H$	–	$6T_H$	3.09
Hwang *et al.* [55]	$8T_H$	$9T_H$	$6T_H$	4.542
Patil *et al.* [64]	$6T_H$	$4T_H$	$4T_H$	3.186
Park *et al.* [83]	$10T_H + 2T_{ecm} + 4T_{XOR}$	$16T_H + T_{XOR} + 2T_{ecm}$	$7T_{XOR} + 16T_H$	13.75
Das *et al.* [88]	$2T_{ecm} + 12T_H$	$10T_H$	$2T_{ecm} + 9T_H$	15.8
Chang *et al.* [89]-P1	$7T_H + 4T_{XOR}$	$8T_H + T_{XOR}$	$5T_H + 4T_{XOR}$	3.74
Chang *et al.* [89]-P2	$7T_H + 2T_{ecm}$	$5T_H + 2T_{ecm}$	$9T_H$	7.7
Quan *et al.* [90]	$7T_H$	$4T_H$	$5T_H$	3.8
Wei *et al.* [91]	$8T_H + 2T_{ECC}$	$9T_H + T_{ECC}$	$6T_H$	10.33

Symbols: T_H- Hash Function, T_P- PUF Function, T_{GEN}- Generator Operation, T_{REP}- Reproduce Operation, T_{EXP}- Exponential Function , T_{XOR}- XOR Function, $T_{e/d}$- Symmetric key encryption/decryption, T_{ECC}- ECC Function, T_{ecm}- ECC Scalar point multiplication,T_{FE}- Fuzzy Extractor.

TABLE XIII
COMPUTATION COST ANALYSIS OF WSN WITH USER, GATEWAY (OR BASE STATION), AND SENSOR NODE AS THE ENTITIES

Protocol	User	BS/GW	SN	Total(ms)
Wu *et al.* [57]	$10T_H$+$2T_{e/d}$	$6T_H$+$5T_{e/d}$	$5T_H$+$1T_{e/d}$	11.6
He *et al.* [58]	$4T_H$+$2T_{e/d}$	$1T_H$+$3T_{e/d}$	$1T_H$+$2T_{e/d}$	1.695
Khan *et al.* [59]	$6T_H$+$2T_{e/d}$	$9T_H$+$2T_{e/d}$	$7T_H$	4.287
Srinivas *et al.* [60]	$8T_H$+$2T_{e/d}$	$4T_H$+$1T_{e/d}$	$4T_H$+$2T_{e/d}$	3.894
Das *et al.* [81]	$11T_H$	$11T_H$	$6T_H$	5.517
Yoney *et al.* [82]	$3T_H$+$1T_{e/d}$	$3T_H$+$2T_{e/d}$	$2T_H$+$2T_{e/d}$	1.707

Symbols: T_H- Hash Function, T_P- PUF Function, $T_{e/d}$- Symmetric key encryption/decryption.

TABLE XIV
COMPUTATIONAL COST ANALYSIS OF SMART GRID WITH USER, GATEWAY, AND SENSOR NODE AS THE ENTITIES

Protocols	User	Gateway	Sensor Node	Total (ms)
Bansal *et al.* [12]	$T_P + 4T_H + 4T_{e/d}$	$3T_H + 3T_{e/d}$	$T_P + 3T_H + 3T_{e/d}$	3.275
Kaveh *et al.* [112]	$4T_H + 2T_P$	$7T_H + 2T_P$	$3T_H$	4.051
Banerjee *et al.* [113]	$17T_H + T_{FE}$	$8T_H$	$6T_H$	7.299
Das *et al.* [114]	$15T_H$	$10T_H$	$6T_H$	6.729

Symbols: T_H- Hash Function, T_P- PUF Function, $T_{e/d}$- Symmetric key encryption/decryption, T_{FE}- Fuzzy Extractor.

which is usually prone to malicious attacks. A logical remedy is thus to establish robust authentication for its communication components. The proposed scheme outlined a framework for pragmatic development and implementation of authentication procedures and AKA protocols in the SG system. Energy Internet (EI) is suggested as a new infrastructure that can be used in PUF-oriented communication within SG especially when power grids increasingly adopt open innovation supporting technology. Moreover, Gope and Sikdar [110] proposed a protocol for organizing and securing EI-based V2G communication. Under this scheme, a customer can safely access service provider's services with the help of symmetric AKA. The proposed protocol can be implemented using PUF and is resilient against attacks while efficient in computational and communication overheads. In a similar study,

TABLE XV
COMPUTATIONAL COST ANALYSIS OF SMART GRID WITH SM AND SERVICE PROVIDER AS THE ENTITIES

Protocols	Smart Meter	Service Provider	Total (ms)
Gope *et al.* [102]	$FE.REC + 5T_H + 5T_{PUF}$	$FE.GEN + 6T_H$	5.549
Tahavori *et al.* [103]	$9T_H + 2T_P + T_{GEN}$	$9T_H + T_{REP}$	6.422
Saeed *et al.* [104]	$2T_H$	$2T_H$	1.236
Gope *et al.* [105]	$FE.GEN + 6T_H + 2T_{PUF}$	$FE.REF + 6T_H$	4.538
Bhanse *et al.* [107]	$5T_H$	$5T_H$	3.09
Delavar *et al.* [108]-P1	$2T_H + 2T_P + 7T_{Exp} + 5T_{em}$	$2T_H + T_P + 7T_{Exp} + 5T_{em}$	28.60
Delavar *et al.* [108]-P2	$T_H + T_P + 2T_{Exp} + T_{em}$	$2T_H + T_{Exp} + T_{em}$	6.617
Braeken *et al.* [109]	$4T_{MP} + T_{AP} + T_S + 5T_H$	$T_{MP} + 2T_{AP} + T_S + 5T_H$	2.264

Symbols: T_H- Hash Function, T_P- PUF Function, T_{GEN}- Generator Operation, T_{REP}- Reproduce Operation, T_S- Symmetric OPeration, T_{EXP}- Exponential Function , T_{XOR}- XOR Function, T_{MAC}- MAC Function, T_{ENC}- Encryption Function, $FE.REC$- Fuzzy Extractor Recover, RNG- Random Number Generator, $FE.GEN$- Fuzzy Extractor Generator, T_{EM}- ECC Point multiplication, T_{EA}- ECC Point addition, $T_{e/d}$- Symmetric key encryption/decryption, T_{ECC}- ECC Function, T_{ecm}- ECC Scalar point multiplication,T_{FE}- Fuzzy Extractor, T_{GM}- Scalar Multiplication on G, T_{GA}- Scalar Addition on G, T_{MP}- Point Multiplication, T_{AP}- Point Addition.

TABLE XVI
COMMUNICATION COST ANALYSIS OF IOT WITH IOT DEVICE AND SERVER AS THE ENTITIES

Protocols	IoT Device	Server	Total (bits)
Jiang *et al.* [16]	640	640	1280
Liang *et al.* [19]	800	800	1600
Melki *et al.* [21]	800	480	1280
Garg *et al.* [22]	1440	2400	3840
Braeken *et al.* [24]-P1	1120	416	1536
Braeken *et al.* [24]-P2	240	240	480
Das *et al.* [27]	640	1120	1760
Xie *et al.* [28]	1280	1440	2720
Aman *et al.* [30]	1920	1600	3520
Chatterjee *et al.* [31]	1280	2240	3520
Chua *et al.* [33]-P1	1760	1600	3360
Chua *et al.* [33]-P2	1600	2080	3680
Gope *et al.* [35]-P1	576	128+nx64	-
Gope *et al.* [35]-P2	1264	1456+nx1392	-
Qureshi *et al.* [37]	800	800	1600
Ayub *et al.* [38]	960	960	1920
Gope *et al.* [40]	4160	-	-
Chikouche *et al.* [41]	1440	1440	2880
Frikken *et al.* [49]	-	-	544

TABLE XVII
COMMUNICATION COST ANALYSIS OF IOT WITH USER, GATEWAY, AND SENSOR NODES AS THE ENTITIES

Protocols	User	Gateway	Sensor Node	Total (bits)
Kumar *et al.* [29]	672	512	352	1536
Ruben *et al.* [39]	-	3840	2304	6144
Li *et al.* [43]	704	512	256	-
Challa *et al.* [44]	1536	1536	768	-
Zhou *et al.* [45]	1536	1280	3328	-
Turknovic *et al.* [56]	640	1088	280	2008

TABLE XVIII
COMMUNICATION COST ANALYSIS OF WSN WITH IOT DEVICE AND SERVER AS THE ENTITIES

Protocols	IoT Device	Server	Total (bits)
Xie *et al.* [28]	1024	1024	-
Li *et al.* [46]	-	-	2080
Kompara *et al.* [62]	960	1120	2080
Zhu *et al.* [65]	800	1120	1920
Aman *et al.* [69]	1440	800	2240
Wu *et al.* [70]	1920	1920	3840
Aman *et al.* [71]-P1	640	480	1120
Aman *et al.* [71]-P2	1600	800	2400

Kaveh *et al.* [111] presented a privacy-aware authentication protocol to assure data integrity, confidentiality, and verification. The proposed scheme incorporates PUF-based AKA for physical security of operations and communication. It is reported to be resilient toward attacks and efficient for V2G communications.

Banerjee *et al.* [112] presented a lightweight authentication scheme for IoT, which uses the cryptographic one-way hash function, PUF and XOR operations. Security analysis in the ROR model and security verification using AVISPAs demonstrated that the scheme is resistant against several attacks and has low computation and communication overheads.

TABLE XIX
COMMUNICATION COST ANALYSIS OF WSN WITH USER, GATEWAY, AND SENSOR NODES AS THE ENTITIES

Protocols	User	Gateway	Sensor Node	Total (bits)
Li *et al.* [43]	704	512	256	-
Gope *et al.* [50]	704	1280	256	2240
Kumar *et al.* [52]	704	1280	256	2240
Alzahrani *et al.* [53]	704	1280	256	2240
Patil *et al.* [64]	2080	800	1280	4160
Naqvi *et al.* [68]	704	1216	280	2200
Park *et al.* [83]	1280	2048	768	-
Das *et al.* [88]	832	512	1408	-
Chang *et al.* [89]-P1	256	256	512	-
Chang *et al.* [89]-P2	256	256	512	-
Quan *et al.* [90]	1024	1280	2816	-
Wei *et al.* [91]	1280	1024	1280	-

TABLE XX
COMMUNICATION COST ANALYSIS OF WSN WITH USER, GATEWAY (OR BASE STATION), AND SENSOR NODE AS THE ENTITIES

Protocol	Data Bits	User	BS/D/GW	SN	Total(bits)
Wu *et al.* [57]	sent	480	480	800	1760
	received	800	480	480	1760
He *et al.* [58]	sent	320	320	320	960
	received	320	320	320	960
Khan *et al.* [59]	sent	480	800	320	1600
	received	640	480	480	1600
Srinivas *et al.* [60]	sent	640	480	480	1600
	received	-	1120	480	1600
Das *et al.* [81]	sent	960	2080	-	3040
	received	1120	960	960	3040
Yoney *et al.* [82]	sent	480	320	320	1120
	received	320	480	320	1120

TABLE XXI
COMMUNICATION COST ANALYSIS OF SMART GRID WITH USER, GATEWAY, AND SENSOR NODES AS THE ENTITIES

Protocols	User	Gateway	Sensor Node	Total (bits)
Bansal *et al.* [12]	1920	1280	1440	4640
Kaveh *et al.* [112]	-	216	144	360
Banerjee *et al.* [113]	800	608	640	2014
Das *et al.* [114]	832	672	352	1856

TABLE XXII
COMMUNICATION COST ANALYSIS OF SMART GRID WITH SM AND SERVICE PROVIDER AS THE ENTITIES

Protocols	Smart Meter	Service Provider	Total (bits)
Gope *et al.* [102]	1120	1600	2720
Tahavori *et al.* [103]	-	-	1480
Saeed *et al.* [104]	400	544	944
Gope *et al.* [105]	1280	1440	2720
Bhanse *et al.* [107]	960	960	1920
Braeken *et al.* [109]	480	320	800

Industrial IoT (IIoT) has gained widespread popularity in the recent times. In IIoT, the analysis of the real-time data collected from the smart sensing devices by a remote device can be done. In IIoT, since the data are transmitted via the public channel, there are high chances for growth in the problems of the security and privacy. The smart card, password, and the personal biometrics of a legal registered user are applied in the proposed scheme for the increment in the security level of the system. The user authentication mechanism is the most effective solution in the IIoT environment for providing protection against the illegitimate access by any adversary. Srinivas *et al.* [113] proposed a new lightweight user authenticated key agreement scheme where the authorized users access the facilities from the designated IoT sensing devices mounted in IIoT setting. The fuzzy extractor is used

TABLE XXIII
SECURITY ATTACKS AND FEATURE COMPARISON OF THE AKA PROTOCOLS FOR IOT

Protocol	I1	I2	I3	I4	I5	I6	I7	I8	I9	I10	I11	I12	I13	I14	I15	I16	I17	I18	I19	I20
Haji *et al.* [8]	×	×	×	×	×	×	×	×	×	×	×	×	×	✓	×	×	×	×	×	×
Boke *et al.* [11]	✓	×	×	✓	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×
Wang *et al.* [13]	×	×	×	×	×	×	×	×	×	×	✓	×	×	×	×	×	×	×	×	×
Barbareschi *et al.* [14]	×	✓	✓	×	×	×	×	×	×	×	×	×	×	✓	×	×	×	×	×	✓
Liu *et al.* [15]	×	✓	×	×	×	×	×	×	×	×	×	×	×	✓	×	✓	×	×	×	×
Jiang *et al.* [16]	×	✓	×	×	✓	×	×	×	✓	×	×	✓	×	×	×	×	×	✓	×	×
Byun *et al.* [17]	×	✓	×	×	✓	✓	✓	✓	×	×	✓	×	×	×	×	×	✓	✓	×	×
Barbareschi *et al.* [18]	×	×	✓	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×
Liang *et al.* [19]	×	✓	✓	×	×	×	×	×	✓	×	×	×	✓	×	×	✓	×	✓	✓	×
Melki *et al.* [20]	✓	✓	✓	×	×	✓	✓	×	✓	×	×	×	×	×	×	×	×	×	×	×
Garg *et al.* [21]	✓	✓	✓	✓	✓	×	×	×	×	×	×	×	×	×	×	×	×	×	✓	✓
Suganthi *et al.* [22]	×	✓	×	×	✓	✓	×	✓	✓	×	✓	×	×	×	×	×	×	×	×	✓
Braeken *et al.* [24]	✓	✓	✓	×	✓	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×
Rahim *et al.* [26]	✓	×	×	×	×	×	×	×	×	×	×	×	×	✓	×	✓	×	×	×	×
Das *et al.* [27]	✓	✓	✓	×	✓	×	×	✓	×	×	✓	✓	×	×	×	×	×	×	×	×
Xie *et al.* [28]	×	×	×	×	✓	×	×	×	×	×	✓	✓	×	✓	×	×	×	✓	×	×
Kumar *et al.* [29]	×	×	×	×	×	×	×	×	×	×	×	×	×	✓	×	×	×	×	×	×
Aman *et al.* [30]	×	×	×	×	×	×	×	×	×	×	×	×	×	✓	✓	×	×	×	×	×
Chatterjee *et al.* [31]	×	×	×	×	×	✓	✓	×	×	×	×	×	×	✓	×	×	×	×	×	×
Rostami *et al.* [32]	✓	✓	✓	×	×	×	×	×	✓	×	×	×	✓	✓	×	×	×	×	×	×
Gope *et al.* [35]	✓	×	×	×	×	×	×	×	×	×	×	×	×	✓	×	×	×	×	×	✓
Idriss *et al.* [36]	×	×	✓	×	×	×	×	×	×	×	×	×	×	✓	×	×	×	×	×	×
Qureshi *et al.* [37]	×	✓	×	×	×	×	✓	×	×	×	✓	×	×	✓	×	×	×	×	×	×
Ayub *et al.* [38]	×	×	×	×	✓	×	×	✓	×	×	×	✓	×	✓	✓	×	×	✓	×	×
Ruben *et al.* [39]	×	✓	✓	×	✓	×	×	✓	×	×	×	✓	×	×	×	×	×	✓	×	✓
Chikouche *et al.* [41]	×	✓	✓	×	×	✓	×	×	×	×	×	✓	×	×	×	×	×	✓	×	×
Lo *et al.* [42]	×	✓	✓	×	✓	✓	×	×	×	×	×	×	×	×	✓	×	×	×	×	✓
Li *et al.* [43]	×	✓	×	×	✓	✓	✓	×	✓	×	×	✓	✓	×	×	×	×	✓	×	×
Challa *et al.* [44]	✓	✓	✓	×	✓	×	×	✓	×	✓	×	✓	×	×	×	×	×	×	×	✓
Zhou *et al.* [45]	×	×	×	×	×	✓	×	×	×	✓	✓	×	×	×	×	×	×	✓	×	×
Li *et al.* [46]	×	✓	×	×	✓	✓	×	×	×	×	×	×	×	✓	×	×	×	✓	×	×
Frikken *et al.* [49]	×	×	×	×	×	×	×	×	×	×	×	×	×	✓	×	×	✓	×	×	×
Turknovic *et al.* [56]	✓	✓	×	×	✓	✓	✓	✓	×	✓	✓	✓	×	×	×	✓	×	×	×	×

I1: DoS attack; I2: Replay attack; I3: MITM attack; I4: Eavesdropping; I5: Impersonation; I6: Session Key Security Attack; I7: Security protection on long-term Secret Key; I8: Stolen device; I9: Side Channel attacks; I10: Insider attack; I11: Password Guessing attack; I12: Anonymity; I13: ML attacks; I14: Physical attack; I15: Masquerade attack; I16: Tracking attack; I17: Dictionary attack; I18: Non-synchronous attack; I19: Spoofing; I20 : Forward and Backward secrecy

in this proposed protocol for the purpose of the biometric verification. The use of the fuzzy extractor is done for protecting the privacy and also strengthening the security of the biometric data. The fuzzy extractor also improves the robustness of the proposed protocol. The authors used the ROR model, i.e., Real-Or-Random for the protocol's security analysis. The proposed scheme is efficient as well as provides superior security.

Section VI outlines the PUF-based AKA protocols deployed in the smart grid sector. The section briefly describes the protocols. Their possible strengths and weaknesses are also documented and comparatively discussed among relevant papers or proposed schemes. Table V describes the related approaches and Fig. 6 presents the categorization of the these approaches based on their underlying cryptographic operations and entities in the architecture.

Fig. 4 presents the categorization of the works specific to IoT on the basis of cryptographic operations and the number of entities in the specific architecture. In the same manner, Figs. 5 and 6, respectively, categorize related WSN and smart grid approaches.

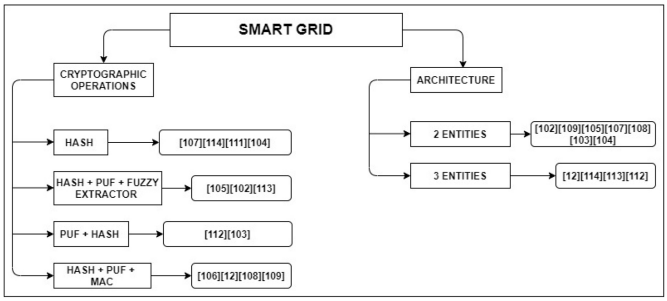

Fig. 6. Smart grid categorization.

VII. EVALUATION SETUP

We will now describe our evaluation setup, prior to presenting the findings in the next section. The evaluations are carried out on our platform using the widely accepted "multiprecision integer and rational arithmetic cryptographic library (MIRACL)[1] Cryptographic SDK: MIRACL" [114]. Each cryptographic primitive is being executed on platform 100 times, and the average execution time for each cryptographic primitive from these 100 runs is recorded. Let T_h, T_{exp}, T_{ecm}, T_{eca}, T_{senc}, T_{sdec}, T_{mul}, T_{add}, T_{bp}, T_{mtp}, T_{FE}, and T_P denote the time needed to execute one-way hash function using "Secure Hash Algorithm SHA-1," modular exponentiation, elliptic curve point multiplication, elliptic curve point addition, symmetric encryption (using "advanced encryption standard (AES-128)"), symmetric decryption (using AES-128), multiplication in a finite field,

[1]MIRACL.

TABLE XXIV
SECURITY ATTACKS AND FEATURE COMPARISON OF THE AKA PROTOCOLS FOR WSN

Protocol	I1	I2	I3	I4	I5	I6	I7	I8	I9	I10	I11	I12	I13	I14	I15	I16	I17	I18	I19	I20
Xie *et al.* [28]	×	×	×	×	✓	×	×	×	×	×	×	✓	×	×	×	✓	✓	×	×	✓
Gope *et al.* [40]	×	✓	×	✓	✓	✓	×	×	×	×	×	×	×	✓	×	✓	×	✓	×	✓
Lo *et al.* [42]	×	✓	✓	×	✓	✓	×	×	×	×	×	×	×	×	✓	×	×	×	×	✓
Li *et al.* [43]	×	✓	×	×	✓	✓	✓	×	✓	×	×	✓	✓	×	×	×	×	✓	×	×
Gope *et al.* [50]	✓	✓	✓	×	✓	✓	✓	✓	✓	×	×	×	×	✓	×	×	×	×	×	×
Osama *et al.* [51]	×	✓	✓	×	×	×	×	✓	×	×	✓	✓	×	✓	×	×	×	✓	×	✓
Kumar *et al.* [52]	✓	✓	✓	×	✓	×	×	✓	×	×	✓	✓	×	✓	×	×	×	✓	×	✓
Alzahrani *et al.* [53]	×	✓	×	×	✓	✓	×	×	×	×	✓	✓	×	×	×	×	×	×	×	✓
Xie *et al.* [54]	×	✓	✓	×	✓	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×
Hwang *et al.* [55]	✓	✓	×	✓	×	✓	✓	✓	×	✓	×	✓	×	×	×	×	×	×	×	✓
Wu *et al.* [57]	×	×	×	×	✓	✓	✓	✓	×	✓	✓	✓	×	×	×	×	×	✓	✓	×
He *et al.* [58]	×	×	×	×	×	✓	✓	×	×	×	×	✓	×	✓	×	×	×	×	×	×
Khan *et al.* [59]	×	×	×	×	✓	✓	✓	×	×	✓	✓	✓	×	✓	×	×	×	×	×	×
Srinivas *et al.* [60]	×	✓	×	×	✓	✓	✓	✓	×	✓	✓	✓	×	×	×	×	×	×	×	×
Kompara *et al.* [62]	×	✓	✓	✓	✓	✓	✓	✓	×	×	×	✓	×	×	×	×	×	✓	×	✓
Wang *et al.* [63]	×	×	✓	×	✓	✓	✓	✓	×	×	×	✓	×	×	×	✓	×	×	✓	✓
Patil *et al.* [64]	✓	✓	✓	×	×	✓	×	×	×	×	×	×	×	×	✓	×	×	×	×	×
Zhu *et al.* [65]	×	×	×	×	✓	×	×	×	×	×	×	×	×	✓	×	×	×	✓	×	✓
Li *et al.* [66]	×	×	×	×	×	×	×	×	×	✓	×	×	×	×	×	×	×	×	×	✓
Aman *et al.* [69]	×	×	×	×	×	×	×	×	✓	×	×	×	×	✓	×	×	×	×	×	×
Wu *et al.* [70]	×	✓	×	×	×	✓	✓	×	×	×	×	×	×	×	×	×	×	✓	×	×
Aman *et al.* [71]	×	✓	✓	✓	✓	×	×	×	×	×	×	×	×	✓	×	×	×	×	✓	×
Valmiki *et al.* [72]	×	✓	✓	×	✓	×	×	×	×	×	×	✓	×	×	×	×	×	×	×	×
Ferrag *et al.* [73]	✓	✓	✓	✓	✓	✓	✓	×	×	×	✓	×	×	×	✓	✓	✓	×	✓	✓
Byun *et al.* [80]	×	✓	×	×	✓	×	×	✓	×	×	✓	×	×	×	×	×	✓	✓	×	×
Das *et al.* [81]	✓	×	×	×	×	✓	✓	✓	×	×	✓	×	×	×	×	×	×	×	×	×
Yoney *et al.* [82]	×	✓	✓	×	✓	✓	✓	✓	×	×	✓	✓	×	×	×	×	×	×	×	✓
Park *et al.* [83]	×	✓	✓	×	✓	✓	×	✓	×	×	✓	✓	×	×	×	×	×	×	×	✓
Das *et al.* [88]	×	✓	✓	×	✓	✓	×	✓	×	×	✓	✓	×	×	×	×	×	×	×	✓
Chang *et al.* [89]	×	✓	×	×	✓	✓	×	✓	×	×	×	✓	×	×	×	×	×	×	×	✓
Quan *et al.* [90]	✓	✓	✓	×	✓	✓	×	✓	×	✓	✓	✓	×	×	×	×	×	×	×	×
Wei *et al.* [91]	×	✓	✓	×	✓	✓	×	✓	×	×	×	✓	×	×	×	✓	×	×	×	×
Wang *et al.* [93]	×	✓	✓	×	✓	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×
Afghah *et al.* [94]	✓	✓	✓	×	✓	×	×	✓	✓	×	×	×	×	×	×	×	×	×	✓	×

I1: DoS attack; I2: Replay attack; I3: MITM attack; I4: Eavesdropping; I5: Impersonation; I6: Session Key Security Attack; I7: Security protection on long-term Secret Key; I8: Stolen device; I9: Side Channel attacks; I10: Insider attack; I11: Password Guessing attack; I12: Anonymity; I13: ML attacks; I14: Physical attack; I15: Masquerade attack; I16: Tracking attack; I17: Dictionary attack; I18: Non-synchronous attack; I19: Spoofing; I20 : Forward and Backward secrecy

addition in a finite field, bilinear pairing, map-to-point, fuzzy extractor (generation function or reproduction function), and PEF operation, respectively. It is assumed that $T_{FE} \approx T_{ecm}$ and $T_P \approx T_{ecm}$.

1) *Platform 1:* Each cryptographic primitive is executed under MIRACL in a server setting with the following configuration: "Model: MacBook Pro (15-inch, 2019) with CPU Architecture: 64-bit, Processor: 2.3-GHz Intel Core i9, Memory: 32-GB, OS: macOS Mojave 10.14.6." The findings are presented in Table VI.
2) *Platform 2:* An IoT smart device (sensor node or SM) or user device is considered under the setting: "Raspberry PI 3 B+ Rev 1.3, with CPU: 64-bit, Processor: 1.4 GHz Quad-core, 4 cores, Memory (RAM): 1 GB, and OS: Ubuntu 20.04 LTS, 64 bit" [115]. The findings are reported in Table VI.

VIII. PERFORMANCE AND SECURITY ANALYSIS

This section presents a comparative summary of the performance and security of several protocols examined in the preceding sections. Generally, protocols are bounded by time and cost complexities, due to, for instance, the use of cryptographic functions (e.g., hash functions, XOR operations, and PUF circuitry).

A. Computation Cost

We let the computation cost for (PUF) function be *0.43* ms, and T_p denotes the time complexity of PUF. Time complexities of other cryptographic functions are presented in Table VI. The other protocols' computation costs are considered and compared in terms of milliseconds.

In Table VII, one can observe that the protocol of Braeken [23] is more computationally efficient than the other IoT-related protocols. Similarly, for Tables VIII–XI, we observe that the protocols of Ayub *et al.* [37], Das *et al.* [28], Kompara *et al.* [61], and Lo and Yohan [41], are the most computationally efficient in their respective categories.

From Table XII, one can observe that the protocols of Gope *et al.* [49] and Das *et al.* [87] are the most computationally efficient. Similarly, for Tables XIII–XV, one can observe that the protocols of Ever [81], Kaveh *et al.* [111], and Gope and Sikdar [101] are the most computationally efficient in their respective categories.

B. Communication Cost

Here, we assume that both the hash function and PUF produce 160 bits for all protocols, which is 20B, and the output of *SHA-1* is a 160-bit hash value [i.e., message digest (*MD*)].

TABLE XXV
SECURITY ATTACKS AND FEATURE COMPARISON OF THE AKA PROTOCOLS FOR SMART GRID

Protocol	I1	I2	I3	I4	I5	I6	I7	I8	I9	I10	I11	I12	I13	I14	I15	I16	I17	I18	I19	I20
Bansal *et al.* [12]	×	✓	✓	×	✓	✓	×	×	×	×	×	×	✓	✓	✓	×	×	×	×	×
Ghosal *et al.* [101]	×	✓	×	✓	×	×	×	×	×	×	×	×	×	×	×	×	×	×	✓	×
Gope *et al.* [102]	×	✓	✓	×	✓	✓	✓	×	×	×	×	✓	×	✓	×	×	×	×	×	✓
Tahavori *et al.* [103]	×	✓	✓	×	✓	×	×	×	×	×	✓	✓	×	×	×	×	×	×	×	✓
Saeed *et al.* [104]	×	✓	×	×	✓	×	×	×	×	×	×	×	×	×	×	×	×	×	×	✓
Gope *et al.* [105]	×	×	✓	✓	×	✓	✓	×	✓	×	×	×	×	✓	×	×	×	×	×	✓
Reza *et al.* [106]	×	×	×	×	×	×	×	×	×	×	×	×	✓	✓	×	×	×	×	×	×
Bhanse *et al.* [107]	×	✓	✓	×	✓	×	×	×	×	✓	×	×	×	×	×	×	×	×	×	✓
Braeken *et al.* [109]	✓	✓	✓	×	✓	✓	✓	×	✓	×	×	✓	×	×	×	×	×	×	×	×
Malik *et al.* [110]	×	✓	✓	×	✓	✓	✓	✓	×	×	×	✓	×	×	×	×	×	×	×	✓
Gope *et al.* [111]	✓	×	✓	✓	×	✓	✓	×	×	×	×	×	×	×	×	×	×	×	×	✓
Kaveh *et al.* [112]	✓	✓	×	✓	✓	×	×	×	×	×	×	✓	×	✓	×	×	×	×	×	×
Banerjee *et al.* [113]	✓	✓	✓	×	✓	×	×	✓	×	✓	✓	✓	×	×	×	×	×	×	×	×
Das *et al.* [114]	✓	✓	✓	×	✓	✓	✓	✓	×	✓	✓	✓	×	×	×	×	×	×	×	×

I1: DoS attack; I2: Replay attack; I3: MITM attack; I4: Eavesdropping; I5: Impersonation; I6: Session Key Security Attack; I7: Security protection on long-term Secret Key; I8: Stolen device; I9: Side Channel attacks; I10: Insider attack; I11: Password Guessing attack; I12: Anonymity; I13: ML attacks; I14: Physical attack; I15: Masquerade attack; I16: Tracking attack; I17: Dictionary attack; I18: Non-synchronous attack; I19: Spoofing; I20 : Forward and Backward secrecy.

In Tables XVI and XVII, we can observe that the protocols of Braeken [23] and Das *et al.* [28] are most efficient communicationwise in their respective categories.

In Tables XVIII–XXII, we can observe that the protocols of Aman *et al.* [70], Naqvi *et al.* [67], He *et al.* [57], Kaveh *et al.* [111], and Braeken *et al.* [108] are more efficient communicationwise in their respective categories.

C. Security and Functionality Features

In Table XXIII, one can observe that the protocol of Turknovic *et al.* [55] appears to be more efficient than the other protocols. In Table XXIV, the protocol of Ferrag *et al.* [72] appears to be more efficient than the other WSN related protocols, and in Table XXV, the protocol of Srinivas *et al.* [113] appeared to be more efficient than the other smart grid-related protocols.

IX. CONCLUSION

We surveyed the extant literature on PUF-based AKA protocols, designed for IoT, WSN, and smart grid settings. Specifically, we discussed the associated characteristics, security, types, and various associated applications, and performed a comparative analysis among the existing competing authentication schemes to determine communication and computation costs, and security features.

One can observe that the majority of the PUF-based AKA protocols are vulnerable to PUF modeling attacks, such as approximation attacks. Another limitation observation is the performance impact due to rising temperature on PUF-embedded devices. Hence, these two limitations could potentially be focused on in future designs of PUF-based AKA protocols.

REFERENCES

[1] C. W. O'Donnell, G. E. Suh, and S. Devadas, *PUF-Based Random Number Generation*, document CSG Tech. Memo 481, MIT Comput. Sci. Artif. Intell. Lab., Cambridge, MA, USA, 2004.

[2] R. Maes and I. Verbauwhede, "Physically unclonable functions: A study on the state of the art and future research directions," in *Towards Hardware-Intrinsic Security*. Heidelberg, Germany: Springer, 2010. pp. 3–37.

[3] A. Jain and A. M. Joshi, "Device authentication in IoT using reconfigurable PUF," in *Proc. 2nd IEEE Middle East North Africa Commun. Conf. (MENACOMM)*, 2019, pp. 1–4.

[4] J. Long, W. Liang, K.-C. Li, D. Zhang, M. Tang, and H. Luo, "PUF-based anonymous authentication scheme for hardware devices and IPs in edge computing environment," *IEEE Access*, vol. 7, pp. 124785–124796, 2019.

[5] A. Braeken, "PUF-based authentication and key exchange for Internet of Things," in *IoT Security: Advances in Authentication*. Hoboken, NJ, USA: Wiley, 2020, pp. 185–204.

[6] W. Bian, P. Gope, Y. Cheng, and Q. Li, "Bio-AKA: An efficient fingerprint based two factor user authentication and key agreement scheme," *Future Gener. Comput. Syst.*, vol. 109, pp. 45–55, Aug. 2020.

[7] H. Akhundov, E. van der Sluis, S. Hamdioui, and M. Taouil, "Public-key based authentication architecture for IoT devices using PUF," 2020, *arXiv:2002.01277*.

[8] G. Bansal, N. Naren, and V. Chamola, "RAMA: Real-time automobile mutual authentication protocol using PUF," in *Proc. Int. Conf. Inf. Netw. (ICOIN)*, 2020, pp. 265–270.

[9] D. Fang, Y. Qian, and R. Q. Hu, "A flexible and efficient authentication and secure data transmission scheme for IoT applications," *IEEE Internet Things J.*, vol. 7, no. 4, pp. 3474–3484, Apr. 2020.

[10] A. K. Boke, S. Nakhate, and A. Rajawat, "Efficient key generation techniques for securing IoT communication protocols," *IETE Tech. Rev.*, vol. 38, pp. 282–293, Feb. 2021.

[11] G. Bansal, N. Naren, V. Chamola, B. Sikdar, N. Kumar, and M. Guizani, "Lightweight mutual authentication protocol for V2G using physical unclonable function," *IEEE Trans. Veh. Technol.*, vol. 69, no. 7, pp. 7234–7246, Jul. 2020.

[12] Q. Wang, M. Gao, and G. Qu, "PUF-PassSE: A PUF based password strength enhancer for IoT applications," in *Proc. 20th Int. Symp. Qual. Electron. Design (ISQED)*, 2019, pp. 198–203.

[13] M. Barbareschi, A. De Benedictis, E. La Montagna, A. Mazzeo, and N. Mazzocca, "A PUF-based mutual authentication scheme for cloud-edges IoT systems," *Future Gener. Comput. Syst.*, vol. 101, pp. 246–261, Dec. 2019.

[14] D. Liu *et al.*, "Research on end-to-end security authentication protocol of NB-IoT for smart grid based on physical unclonable function," in *Proc. IEEE 11th Int. Conf. Commun. Softw. Netw. (ICCSN)*, 2019, pp. 239–244.

[15] Q. Jiang, X. Zhang, N. Zhang, Y. Tian, X. Ma, and J. Ma, "Two-factor authentication protocol using physical unclonable function for IoV," in *Proc. IEEE/CIC Int. Conf. Commun. China (ICCC)*, 2019, pp. 195–200.

[16] J. W. Byun, "An efficient multi-factor authenticated key exchange with physically unclonable function," in *Proc. Int. Conf. Electron. Inf. Commun. (ICEIC)*, 2019, pp. 1–4.

[17] M. Barbareschi, A. De Benedictis, E. La Montagna, A. Mazzeo, and N. Mazzocca, "PUF-enabled authentication-as-a-service in fog-IoT systems," in *Proc. IEEE 28th Int. Conf. Enabling Technol. Infrastruct. Collaborative Enterprises (WETICE)*, 2019, pp. 58–63.

[18] W. Liang, S. Xie, J. Long, K. C. Li, D. Zhang, and K. Li, "A double PUF-based RFID identity authentication protocol in service-centric

Internet of Things environments," *Inf. Sci.*, vol. 503, pp. 129–147, Nov. 2019.

[19] R. Melki, H. N. Noura, and A. Chehab, "Lightweight multi-factor mutual authentication protocol for IoT devices," *Int. J. Inf. Security*, vol. 19, no. 6, pp. 679–694, 2020.

[20] S. Garg, K. Kaur, G. Kaddoum, and K.-K. R. Choo, "Towards secure and provable authentication for Internet of Things: Realizing industry 4.0," *IEEE Internet Things J.*, vol. 7, no. 5, pp. 4598–4606, May 2020.

[21] S. D. Suganthi, R. Anitha, V. Sureshkumar, S. Harish, and S. Agalya, "End to end light weight mutual authentication scheme in IoT-based healthcare environment," *J. Rel. Intell. Environ.*, vol. 6, no. 2, pp. 3–13, 2020.

[22] U. Chatterjee *et al.* "Building PUF based authentication and key exchange protocol for IoT without explicit CRPs in verifier database," *IEEE Trans. Dependable Secure Comput.*, vol. 16, no. 3, pp. 424–437, May/Jun. 2019.

[23] A. Braeken, "PUF based authentication protocol for IoT," *Symmetry*, vol. 10, no. 8, p. 352, 2018.

[24] U. Chatterjee *et al.*, "PUFSSL: An OpenSSL extension for PUF based authentication," in *Proc. IEEE 23rd Int. Conf. Digit. Signal Process. (DSP)*, 2018, pp. 1–5.

[25] K. Rahim, H. Tahir, and N. Ikram, "Sensor based PUF IoT authentication model for a smart home with private blockchain," in *Proc. Int. Conf. Appl. Eng. Math. (ICAEM)*, 2018, pp. 102–108.

[26] K. Das, M. Wazid, N. Kumar, M. Khan, K. Choo, and Y. Park, "Design of secure and lightweight authentication protocol for wearable devices environment," *IEEE J. Biomed. Health Inform.*, vol. 22, no. 4, pp. 1310–1322, Jul. 2018.

[27] Q. Xie, D. S. Wong, G. Wang, X. Tan, K. Chen, and L. Fang, "Provably secure dynamic id-based anonymous two-factor authenticated key exchange protocol with extended security model," *IEEE Trans. Inf. Forensics Security*, vol. 12, pp. 1382–1392, 2017.

[28] A. K. Das, M. Wazid, N. Kumar, A. V. Vasilakos, and J. J. Rodrigues, "Biometrics-based privacy-preserving user authentication scheme for cloud-based Industrial Internet of Things deployment," *IEEE Internet Things J.*, vol. 5, no. 6, pp. 4900–4913, Dec. 2018.

[29] M. N. Aman and B. Sikdar, "ATT-Auth: A hybrid protocol for industrial IoT attestation with authentication," *IEEE Internet Things J.*, vol. 5, no. 6, pp. 5119–5131, Dec. 2018.

[30] U. Chatterjee, R. S. Chakraborty, and D. Mukhopadhyay, "A PUF-based secure communication protocol for IoT," *ACM Trans. Embedded Comput. Syst.*, vol. 16, no. 3, pp. 1–25, 2017.

[31] M. Rostami, M. Majzoobi, F. Koushanfar, D. S. Wallach, and S. Devadas, "PUF authentication and key-exchange by substring matching," U.S. Patent 9 628 272, 2017.

[32] M. N. Aman, K. C. Chua, and B. Sikdar, "Physically secure mutual authentication for IoT," in *Proc. IEEE Conf. Dependable Secure Comput.*, 2017, pp. 310–317.

[33] C. Huth, A. Aysu, J. Guajardo, P. Duplys, and T. Güneysu, "Secure and private, yet lightweight, authentication for the IoT via PUF and CBKA," in *Proc. Int. Conf. Inf. Security Cryptol.*, 2016, pp. 28–48.

[34] P. Gope, J. Lee, and T. Q. S. Quek, "Lightweight and practical anonymous authentication protocol for RFID systems using physically unclonable functions," *IEEE Trans. Inf. Forensics Security*, vol. 13, pp. 2831–2843, 2018.

[35] T. Idriss, H. Idriss, and M. Bayoumi, "A PUF-based paradigm for IoT security," in *Proc. IEEE 3rd World Forum Internet Things (WF-IoT)*, 2016, pp. 700–705.

[36] M. A. Qureshi and A. Munir, "PUF-IPA: A PUF-based identity preserving protocol for Internet of Things authentication," in *Proc. IEEE 17th Annu. Consum. Commun. Netw. Conf. (CCNC)*, 2020, pp. 1–7.

[37] M. F. Ayub, M. A. Saleem, I. Altaf, K. Mahmood, and S. Kumari, "Fuzzy extraction and PUF based three party authentication protocol using USB as mass storage device," *J. Inf. Security Appl.*, vol. 55, Dec. 2020, Art. no. 102585.

[38] R. De Smet, T. Vandervelden, K. Steenhaut, and A. Braeken, "Lightweight PUF based authentication scheme for fog architecture," *Wireless Netw.*, vol. 27, no. 2, pp. 947–959, 2021.

[39] P. Gope, O. Millwood, and N. Saxena, "A provably secure authentication scheme for RFID-enabled UAV applications," *Comput. Commun.*, vol. 166, no. 4, pp. 19–25, 2021.

[40] N. Chikouche, P.-L. Cayrel, and B. O. Boidje, "A privacy-preserving code-based authentication protocol for Internet of Things," *J. Supercomput.*, vol. 75, no. 12, pp. 8231–8261, 2019.

[41] N.-W. Lo and A. Yohan, "BLE-based authentication protocol for micropayment using wearable device," *Wireless Personal Commun.*, vol. 112, no. 4, pp. 2351–2372, 2020.

[42] X. Li, J. Niu, S. Kumari, F. Wu, A. K. Sangaiah, and K.-K. R. Choof "A three-factor anonymous authentication scheme for wireless sensor networks in Internet of Things environments," *J. Netw. Comput. Appl.*, vol. 103, pp. 194–204, Feb. 2018.

[43] S. Challa *et al.*, "Secure signature-based authenticated key establishment scheme for future IoT applications," *IEEE Access*, vol. 5, pp. 3028–3043, 2017.

[44] L. Zhou, X. Li, K.-H. Yeh, C. Su, and W. Chiu, "Lightweight IoT-based authentication scheme in cloud computing circumstance," *Future Gener. Comput. Syst.*, vol. 91, pp. 244–251, Feb. 2019.

[45] S. Li, T. Zhang, B. Yu, and K. He, "A provably secure and practical PUF-based end-to-end mutual authentication and key exchange protocol for IoT," *IEEE Sensors J.*, vol. 21, no. 4, pp. 5487–5501, Feb. 2021.

[46] M. N. Aman, M. H. Basheer, and B. Sikdar, "Data provenance for IoT with light weight authentication and privacy preservation," *IEEE Internet Things J.*, vol. 6, no. 6, pp. 10441–10457, Dec. 2019.

[47] M. Barbareschi, A. De Benedictis, and N. Mazzocca, "A PUF-based hardware mutual authentication protocol," *J. Parallel Distrib. Comput.*, vol. 119, pp. 107–120, Sep. 2018.

[48] K. B. Frikken, M. Blanton, and M. J. Atallah, "Robust authentication using physically unclonable functions," in *Information Security* (Lecture Notes in Computer Science 5735), P. Samarati, M. Yung, F. Martinelli, and C. A. Ardagna. Heidelberg, Germany: Springer, 2009, pp. 262–277.

[49] P. Gope, A. K. Das, N. Kumar, and Y. Cheng, "Lightweight and physically secure anonymous mutual authentication protocol for real-time data access in industrial wireless sensor networks," *IEEE Trans. Ind. Informat.*, vol. 15, no. 9, pp. 4957–4968, Sep. 2019.

[50] O. Moh'd Alia, "Dynamic relocation of mobile base station in wireless sensor networks using a cluster-based harmony search algorithm," *Inf. Sci.*, vols. 385–386, pp. 76–95, Apr. 2017.

[51] D. Kumar, S. K. Pachigolla, S. S. Manhas, and K. Rawat, "Cryptanalysis and improvement of mutual authentication protocol for real-time data access in industrial wireless sensor networks," *Int. J. Comput. Appl.*, to be published.

[52] B. A. Alzahrani, A. Irshad, A. Albeshri, and K. Alsubhi, "A provably secure and lightweight patient-healthcare authentication protocol in wireless body area networks," *Wireless Personal Commun.*, vol. 117, no. 1, pp. 47–69, 2021.

[53] L. Xie, W. Wang, X. Shi, and T. Qin, "Lightweight mutual authentication among sensors in body area networks through physical unclonable functions," in *Proc. IEEE Int. Conf. Commun. (ICC)*, May 2017, pp. 1–6.

[54] P. Gope and T. Hwang, "A realistic lightweight anonymous authentication protocol for securing real-time application data access in wireless sensor networks," *IEEE Trans. Ind. Electron.*, vol. 63, no. 11, pp. 7124–7132, Nov. 2016.

[55] M. Turkanović, B. Brumen, and M. Hölbl, "A novel user authentication and key agreement scheme for heterogeneous ad hoc wireless sensor networks, based on the Internet of Things notion," *Ad Hoc Netw.*, vol. 20, pp. 96–112, Sep. 2014.

[56] F. Wu, L. Xu, S. Kumari, and X. Li, "An improved and anonymous two-factor authentication protocol for health-care applications with wireless medical sensor networks," *Multimedia Syst.*, vol. 23, no. 2, pp. 195–205, 2017.

[57] D. He, N. Kumar, J. Chen, C.-C. Lee, N. Chilamkurti, and S.-S. Yeo, "Robust anonymous authentication protocol for health-care applications using wireless medical sensor networks," *Multimedia Syst.*, vol. 21, no. 1, pp. 49–60, 2015.

[58] M. K. Khan and S. Kumari, "An improved user authentication protocol for healthcare services via wireless medical sensor networks," *Int. J. Distrib. Sensor Netw.*, vol. 10, no. 4, 2014, Art. no. 347169.

[59] J. Srinivas, D. Mishra, and S. Mukhopadhyay, "A mutual authentication framework for wireless medical sensor networks," *J. Med. Syst.*, vol. 41, no. 5, p. 80, 2017.

[60] H. A. Salam and B. M. Khan, "Use of wireless system in healthcare for developing countries," *Digit. Commun. Netw.*, vol. 2, no. 1, pp. 35–46, 2016.

[61] M. Kompara, S. H. Islam, and M. Hölbl, "A robust and efficient mutual authentication and key agreement scheme with untraceability for WBANs," *Comput. Netw.*, vol. 148, pp. 196–213, Jan. 2019.

[62] J. Wang, L. Wu, K.-K. R. Choo, and D. He, "Blockchain-based anonymous authentication with key management for smart grid edge computing infrastructure," *IEEE Trans. Ind. Informat.*, vol. 16, no. 3, pp. 1984–1992, Mar. 2020.

[63] A. S. Patil, R. Hamza, A. Hassan, N. Jiang, H. Yan, and J. Li, "Efficient privacy-preserving authentication protocol using PUFs with blockchain smart contracts," *Comput. Security*, vol. 97, Oct. 2020, Art. no. 101958.

[64] F. Zhu, P. Li, H. Xu, and R. Wang, "A lightweight RFID mutual authentication protocol with PUF," *Sensors*, vol. 19, no. 13, p. 2957, 2019.

[65] S. Li, B. Yu, and Y. Huang, "A PUF-based group key transfer protocol for Bluetooth," *Int. J. Netw. Security*, vol. 21, no. 4, pp. 618–626, 2019.

[66] C. Miao, G. Dai, X. Zhao, Z. Tang, and Q. Chen, "3D self-deployment algorithm in mobile wireless sensor networks," *Int. J. Distrib. Sens. Netw.*, vol. 11, no. 4, 2015, Art. no. 721921.

[67] S. A. R. Naqvi, S. A. Hassan, H. Pervaiz, and Q. Ni, "Drone-aided communication as a key enabler for 5G and resilient public safety networks," *IEEE Commun. Mag.*, vol. 56, no. 1, pp. 36–42, Jan. 2018.

[68] M. N. Aman, K. C. Chua, and B. Sikdar, "A light-weight mutual authentication protocol for IoT systems," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, 2017, pp. 1–6.

[69] F. Wu, X. Li, L. Xu, S. Kumari, M. Karuppiah, and J. Shen, "A lightweight and privacy-preserving mutual authentication scheme for wearable devices assisted by cloud server," *Comput. Elect. Eng.*, vol. 63, pp. 168–181, Oct. 2017.

[70] M. N. Aman, K. C. Chua, and B. Sikdar, "Mutual authentication in IoT systems using physical unclonable functions," *IEEE Internet Things J.*, vol. 4, no. 5, pp. 1327–1340, Oct. 2017.

[71] V. Siddhartha, G. S. Gaba, and L. Kansal, "A lightweight authentication protocol using implicit certificates for securing IoT systems," *Procedia Comput. Sci.*, vol. 167, pp. 85–96, Jan. 2020.

[72] M. A. Ferrag, L. Maglaras, A. Argyriou, D. Kosmanos, and H. Janicke, "Security for 4G and 5G cellular networks: A survey of existing authentication and privacy-preserving schemes," *J. Netw. Comput. Appl.*, vol. 101, pp. 55–82, Jan. 2018.

[73] B. Li, Z. Fei, and Y. Zhang, "UAV communications for 5G and beyond: Recent advances and future trends," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 2241–2263, Apr. 2019.

[74] H. Ullah, N. G. Nair, A. Moore, C. Nugent, P. Muschamp, and M. Cuevas, "5G communication: An overview of vehicle-to-everything, drones, and healthcare use-cases," *IEEE Access*, vol. 7, pp. 37251–37268, 2019.

[75] S. Meng, X. Su, Z. Wen, X. Dai, Y. Zhou, and W. Yang, "Robust drones formation control in 5G wireless sensor network using mmWave," *Wireless Commun. Mobile Comput.*, vol. 2018, May 2018, Art. no. 5253840.

[76] R. Amin, I. Pali, and V. Sureshkumar, "Software-defined network enabled vehicle to vehicle secured data transmission protocol in VANETs," *J. Inf. Security Appl.*, vol. 58, May 2021, Art. no. 102729.

[77] S. Koulali, E. Sabir, T. Taleb, and M. Azizi, "A green strategic activity scheduling for UAV networks: A sub-modular game perspective," *IEEE Commun. Mag.*, vol. 54, no. 5, pp. 58–64, May 2016.

[78] M. Wazid, A. K. Das, V. Odelu, N. Kumar, M. Conti, and M. Jo, "Design of secure user authenticated key management protocol for generic IoT networks," *IEEE Internet Things J.*, vol. 5, no. 1, pp. 269–282, Feb. 2018.

[79] J. W. Byun, "A generic multifactor authenticated key exchange with physical unclonable function," *Security Commun. Netw.*, vol. 2019, Mar. 2019, Art. no. 5935292.

[80] A. K. Das, P. Sharma, S. Chatterjee, and J. K. Sing, "A dynamic password-based user authentication scheme for hierarchical wireless sensor networks," *J. Netw. Comput. Appl.*, vol. 35, no. 5, pp. 1646–1656, 2012.

[81] Y. K. Ever, "Secure-anonymous user Authentication scheme for e-healthcare application using wireless medical sensor networks," *IEEE Syst. J.*, vol. 13, no. 1, pp. 456–467, Mar. 2019.

[82] Y. Park and Y. Park, "Three-factor user authentication and key agreement using elliptic curve cryptosystem in wireless sensor networks," *Sensors*, vol. 16, no. 12, p. 2123, 2016.

[83] R. Amin, S. H. Islam, G. P. Biswas, M. K. Khan, and M. S. Obaidat, "Design and analysis of an enhanced patient-server mutual authentication protocol for telecare medical information system," *J. Med. Syst.*, vol. 39, no. 11, p. 137, 2015.

[84] R. Amin, N. Kumar, G. P. Biswas, R. Iqbal, and V. Chang, "A light weight authentication protocol for IoT-enabled devices in distributed Cloud Computing environment," *Future Gener. Comput. Syst.*, vol. 78, pp. 1005–1019, Jan. 2018.

[85] J. W. Byun, "End-to-end authenticated key exchange based on different physical unclonable functions," *IEEE Access*, vol. 7, pp. 102951–102965, 2019.

[86] C. Herder, M.-D. Yu, F. Koushanfar, and S. Devadas, "Physical unclonable functions and applications: A tutorial," *Proc. IEEE*, vol. 102, no. 8, pp. 1126–1141, Aug. 2014.

[87] A. K. Das, S. Kumari, V. Odelu, X. Li, F. Wu, and X. Huang, "Provably secure user authentication and key agreement scheme for wireless sensor networks," *Security Commun. Netw.*, vol. 9, no. 16, pp. 3670–3687, 2016.

[88] C.-C. Chang and H.-D. Le, "A provably secure, efficient, and flexible authentication scheme for ad hoc wireless sensor networks," *IEEE Trans. Wireless Commun.*, vol. 15, no. 1, pp. 357–366, Jan. 2016.

[89] Z. Quan, T. Chunming, Z. Xianghan, and R. Chunming, "A secure user authentication protocol for sensor network in data capturing," *J. Cloud Comput.*, vol. 4, no. 1, p. 6, 2015.

[90] Q. Jiang, J. Ma, F. Wei, Y. Tian, J. Shen, and Y. Yang, "An untraceable temporal-credential-based two-factor authentication scheme using ECC for wireless sensor networks," *J. Netw. Comput. Appl.*, vol. 76, pp. 37–48, Dec. 2016.

[91] R. Amin, S. Islam, M. K. Khan, A. Karati, D. Giri, and S. Kumari, "A two-factor RSA-based robust authentication system for multi-server environments," *Security Commun. Netw.*, vol. 2017, Aug. 2017, Art. no. 5989151.

[92] W. Wang, X. Shi, and T. Qin, "Encryption-free authentication and integrity protection in body area networks through physical unclonable functions," *Smart Health*, vol. 12, pp. 66–81, Apr. 2019.

[93] F. Afghah, B. Cambou, M. Abedini, and S. Zeadally, "A RERAM physically unclonable function (RERAM PUF)-based approach to enhance authentication security in software defined wireless networks," *Int. J. Wireless Inf. Netw.*, vol. 25, no. 2, pp. 117–129, 2018.

[94] X. Li, "Deployment of drone base stations for cellular communication without apriori user distribution information," in *Proc. 37th Chin. Control Conf. (CCC)*, Jul. 2018, pp. 7274–7281.

[95] M. J. Reddy, P. S. Prakash, and P. C. Reddy, "Homogeneous and heterogeneous energy schemes for hierarchical cluster based routing protocols in WSN: A survey," in *Proc. 3rd Int. Conf. Trends Inf. Telecommun. Comput.*, 2013, pp. 591–595.

[96] G. Han, X. Jiang, A. Qian, J. J. P. C. Rodrigues, and L. Cheng, "A comparative study of routing protocols of heterogeneous wireless sensor networks," *Sci. World J.*, vol. 2014, Jun. 2014, Art. no. 415415.

[97] R. D. Pietro, L. V. Mancini, C. Soriente, A. Spognardi, and G. Tsudik, "Data security in unattended wireless sensor networks," *IEEE Trans. Comput.*, vol. 58, no. 11, pp. 1500–1511, Nov. 2009.

[98] N. Zhao *et al.*, "Caching unmanned aerial vehicle-enabled small-cell networks: Employing energy-efficient methods that store and retrieve popular content," *IEEE Veh. Technol. Mag.*, vol. 14, no. 1, pp. 71–79, Mar. 2019.

[99] L. K. Ketshabetswe, A. M. Zungeru, M. Mangwala, J. M. Chuma, and B. Sigweni, "Communication protocols for wireless sensor networks: A survey and comparison," *Heliyon*, vol. 5, no. 5, 2019, Art. no. e01591.

[100] A. Ghosal and M. Conti, "Key management systems for smart grid advanced metering infrastructure: A survey," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 3, pp. 2831–2848, 3rd Quart., 2019.

[101] P. Gope and B. Sikdar, "Privacy-aware authenticated key agreement scheme for secure smart grid communication," *IEEE Trans. Smart Grid*, vol. 10, no. 4, pp. 3953–3962, Jul. 2019.

[102] M. Tahavori and F. Moazami, "Lightweight and secure PUF-based authenticated key agreement scheme for smart grid," *Peer-to-Peer Netw. Appl.*, vol. 13, pp. 1616–1628, May 2020.

[103] S. Aghapour, M. Kaveh, D. Martín, and M. R. Mosavi, "An ultra-lightweight and provably secure broadcast authentication protocol for smart grid communications," *IEEE Access*, vol. 8, pp. 125477–125487, 2020.

[104] P. Gope, "PMAKE: Privacy-aware multi-factor authenticated key establishment scheme for advance metering infrastructure in smart grid," *Comput. Commun.*, vol. 152, pp. 338–344, Feb. 2020.

[105] S. M. Reza *et al.*, "Salsa20 based lightweight security scheme for smart meter communication in smart grid," *Telkomnika*, vol. 18, no. 1, pp. 228–233, 2020.

[106] P. Bhanse, B. Mishra, and D. Jena, "A novel smart meter authentication scheme for secure smart grid communication," in *Proc. IEEE Region 10 Conf. (TENCON)*, 2019, pp. 1275–1279.

[107] M. Delavar, S. Mirzakuchaki, M. H. Ameri, and J. Mohajeri, "PUF-based solutions for secure communications in advanced metering infrastructure (AMI)," *Int. J. Commun. Syst.*, vol. 30, no. 9, p. e3195, 2017.

[108] A. Braeken, P. Kumar, and A. Martin, "Efficient and provably secure key agreement for modern smart metering communications," *Energies*, vol. 11, no. 10, p. 2662, 2018.

[109] M. Qasaimeh, R. S. Al-Qassas, and S. Aljawarneh, "Recent development in smart grid authentication approaches: A systematic literature review," *Cybern. Inf. Technol.*, vol. 19, no. 1, pp. 27–52, 2019.

[110] P. Gope and B. Sikdar, "An efficient privacy-preserving authentication scheme for energy Internet-based vehicle-to-grid communication," *IEEE Trans. Smart Grid*, vol. 10, no. 6, pp. 6607–6618, Nov. 2019.

[111] M. Kaveh, D. Martín, and M. R. Mosavi, "A lightweight authentication scheme for V2G communications: A PUF-based approach ensuring cyber/physical security and identity/location privacy," *Electronics*, vol. 9, no. 9, p. 1479, 2020.

[112] S. Banerjee, V. Odelu, A. K. Das, S. Chattopadhyay, J. J. Rodrigues, and Y. Park, "Physically secure lightweight anonymous user authentication protocol for Internet of Things using physically unclonable functions," *IEEE Access*, vol. 7, pp. 85627–85644, 2019.

[113] J. Srinivas, A. K. Das, M. Wazid, and N. Kumar, "Anonymous lightweight chaotic map-based authenticated key agreement protocol for industrial Internet of Things," *IEEE Trans. Dependable Secure Comput.*, vol. 17, no. 6, pp. 1133–1146, Nov./Dec. 2020.

[114] "MIRACL Cryptographic SDK: Multiprecision Integer and Rational Arithmetic Cryptographic Library." 2020. [Online]. Available: https://github.com/miracl/MIRACL (accessed Aug. 2021).

[115] "Raspberry Pi 3 Model B+." 2020. [Online]. Available: https://www.raspberrypi.org/products/raspberry-pi-3-model-b-plus/ (accessed Jan. 2021).

[116] P. Mall and R. Amin, "EuDaimon: PUF-based robust and lightweight authenticated session key establishment protocol for IoT-enabled smart society," *IEEE Syst. J.*, early access, Aug. 17, 2021, doi: 10.1109/JSYST.2021.3101201.

[117] U. Ruhrmair and J. Sölter, "PUF modeling attacks: An introduction and overview," in *Proc. Des. Autom. Test Eur. Conf. Exhibit. (DATE)*, 2014, pp. 1–6.

[118] J. Shi, Y. Lu, and J. Zhang, "Approximation attacks on strong PUFs," *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.*, vol. 39, no. 10, pp. 2138–2151, Oct. 2020.

[119] P. Mall, M. Z. A. Bhuiyan, and R. Amin, "A lightweight secure communication protocol for IoT devices using physically unclonable function," in *Proc. Int. Conf. Security Privacy Anonymity Comput. Commun. Storage*, 2019, pp. 26–35.

[120] C. Lai, H. Li, R. Lu, and X. Shen, "SE-AKA: A secure and efficient group authentication and key agreement protocol for LTE networks," *Comput. Netw.*, vol. 57, no. 17, pp. 3492–3510, 2013.

[121] J.-K. Tsay and S. F. Mjølsnes, "A vulnerability in the UMTS and LTE authentication and key agreement protocols," in *Proc. Int. Conf. Math. Methods Models Archit. Comput. Netw. Security*, 2012, pp. 65–76.

[122] R. Maes, *Physically Unclonable Functions: Constructions, Properties and Applications*. Heidelberg, Germany: Springer, 2013.

[123] K. Furuhashi, M. Shiozaki, A. Fukushima, T. Murayama, and T. Fujino, "The arbiter-PUF with high uniqueness utilizing novel arbiter circuit with delay-time measurement," in *Proc. IEEE Int. Symp. Circuits Syst. (ISCAS)*, 2011, pp. 2325–2328.

[124] C. Böhm, M. Hofer, and W. Pribyl, "A microcontroller SRAM-PUF," in *Proc. 5th Int. Conf. Netw. Syst. Security*, 2011, pp. 269–273.

[125] Q. Chen, G. Csaba, P. Lugli, U. Schlichtmann, and U. Rührmair, "The bistable ring PUF: A new architecture for strong physical unclonable functions," in *Proc. IEEE Int. Symp. Hardw.-Orient. Security Trust*, 2011, pp. 134–141.

[126] D. Suzuki and K. Shimizu, "The glitch PUF: A new delay-PUF architecture exploiting glitch shapes," in *Proc. Int. Workshop Cryptograph. Hardw. Embedded Syst.*, 2010, pp. 366–382.

[127] B. Chatterjee, D. Das, and S. Sen, "RF-PUF: IoT security enhancement through authentication of wireless nodes using in-situ machine learning," in *Proc. IEEE Int. Symp. Hardw. Orient. Security Trust (HOST)*, 2018, pp. 205–208.