Received August 26, 2019, accepted October 4, 2019, date of publication October 16, 2019, date of current version October 29, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2947723

Review on Security of Internet of Things Authentication Mechanism

TARAK NANDY[1], (Member, IEEE), MOHD YAMANI IDNA BIN IDRIS[1,2], RAFIDAH MD NOOR[1,2], MISS LAIHA MAT KIAH[1], (Senior Member, IEEE), LAU SIAN LUN[3], NOR BADRUL ANNUAR JUMA'AT[1], (Senior Member, IEEE), ISMAIL AHMEDY[1], NORJIHAN ABDUL GHANI[1], AND SANANDA BHATTACHARYYA[4]

[1]Faculty of Computer Science and Information Technology, University of Malaya, Kuala Lumpur 50603, Malaysia
[2]Centre for Mobile Cloud Computing, Faculty of Computer Science and Information Technology, University of Malaya, Kuala Lumpur 50603, Malaysia
[3]School of Science and Technology, Sunway University, Selangor 47500, Malaysia
[4]Information Technology Department, Maldives Business School, Male' 20175, Maldives

Corresponding authors: Tarak Nandy (tarak@ieee.org) and Rafidah Md Noor (fidah@um.edu.my)

This work was supported in RU Grants (Under Faculties) GPF009D-2018 in part by the Malaysia Research University Network (MRUN) Long Term Research Grant Scheme (LRGS) (LR003-2019 and LRGS MRUN/F2/01/2019/001) and partnership grant between the University of Malaya and Sunway University under Grant RK004-2017.

ABSTRACT Internet of things (IoT) is considered as a collection of heterogeneous devices, such as sensors, Radio-frequency identification (RFID) and actuators, which form a huge network, enabling non-internet components in the network to produce a better world of services, like smart home, smart city, smart transportation, and smart industries. On the other hand, security and privacy are the most important aspects of the IoT network, which includes authentication, authorization, data protection, network security, and access control. Additionally, traditional network security cannot be directly used in IoT networks due to its limitations on computational capabilities and storage capacities. Furthermore, authentication is the mainstay of the IoT network, as all components undergo an authentication process before establishing communication. Therefore, securing authentication is essential. In this paper, we have focused on IoT security particularly on their authentication mechanisms. Consequently, we highlighted enormous attacks and technical methods on the IoT authentication mechanism. Additionally, we discussed existing security verification techniques and evaluation schemes of IoT authentication. Furthermore, analysis against current existing protocols have been discussed in all parts and provided some recommendation. Finally, the aim of our study is to help the future researcher by providing security issues, open challenges and future scopes in IoT authentication.

INDEX TERMS Authentication, authentication protocols, Internet of Things, network attacks, security, wireless sensor network.

I. INTRODUCTION

It has been anticipated that all the things in the world are going to be internetworked [1]. At present, internet-based services, which is a global network, are connections of computers and computing devices. The idea behind the Internet of Things is to expand the internet by not only connecting internetworking devices but also the non-IP components, like television, light, fan, refrigerator, and air-conditioner. IoT is not based on only at home but also in businesses like manufacturing organizations, vehicular networks, industries, grid companies, health organization and so on. IoT is envisaged to be able to provide an advanced level of services to society and businesses. Therefore, all the things around the world will be fitted with embedded electronics and information technology so that it can produce valuable information based on the requirements and can work like important nodes of the network. Additionally, with the help of embedded electronics, embedded systems, embedded processors and embedded communication systems such small elements of environments can be connected to the network, depending on the applications and business requirements, to produce a huge internetworking environment, which is incomparable to the current network size. It is stated that more than 20.5 billion IoT devices will

The associate editor coordinating the review of this manuscript and approving it for publication was Luis Javier Garcia Villalba.

be connected by 2020 and over three trillion US dollars will be spent on only hardware of IoT [2]. IoT is one of the building blocks behind the concept of smart home [3] and smart cities [4].

In the colossal of IoT network, which is connected with huge numbers of sensors and other devices, identifying one component raises a fundamental challenge, because that can cause privacy issues, governance of the system, access control, and overall architecture. Security and privacy are the most important factors in an IoT network [5]–[7]. On the other hand, there are three security requirements: confidentiality, integrity, and availability. IoT needs to achieve these three requirements in order to fulfill security aspects. Moreover, the environment of IoT may differ from a centralized network to a de-centralized network, cloud to fog network. Therefore, security can be more tighten by enforcing detection techniques of unusual behavior or pattern of the network. This can be achieved in various ways, like a comparison header analyzer intrusion detection system (IDS) [8], based on a vector space representation using a Multilayer Perceptron (MLP) [9] or machine learning [10]–[12], deep learning [13]. Besides, authentication in the IoT network takes place mostly by three components, which are the sensor, user, and Gateway Nodes (GWN) or Authentication Server (AS). A user authenticates himself by sending messages among sensors and GWN whereas, sensors also authenticates itself by communicating with GWN. Furthermore, authentication takes place in both secure and insecure networks so they are prone to different attacks. Most of the authentication protocols maintain three phases: identification, authentication, and authorization. Before authenticating itself, users or sensors need to register in the network and during the login procedure authentication takes place. As during registration, login, and authentication, several communications happen among components so data privacy must be considered. To focus on these issues, several protocols have chosen different mechanisms to authenticate users. FIGURE 1 provides the flow of the authentication process, where, in most cases, users are not available to GWN to send its information for authentication. Therefore, remotely deployed sensor node helps them to authenticate in the IoT network. Additionally, different authentication protocols use different techniques like RFID, biometric or alphanumeric password for authenticating a user [14]. In addition, the designing phase of authentication protocols always considers the lightweight manner with respect to computation and storage because sensor nodes are computationally challenged and have minimum storage capacities.

Authentication is one of the major parts of the security of IoT networks. As per the IoT network design is a concern, components can communicate with each other and can share data among themselves. If there is no filter, then important credentials can be stolen by network attacks and that can cause harm to the system or users. Authentication works on this situation to validate the identity of legitimate users and devices in a network. A myriad of authentication protocols are designed over the last few decades but none of these provides complete protection to the networks. Protocol designers are sometimes unaware of new threats in IoT networks. This motivates the authors of this paper to review on authentication, which is very important for future authentication protocol developer. Moreover, the authentication mechanism needs to be improved by comparing the existing authentication protocols. Therefore, the contributors to this paper include all the aspects of authentication protocols of IoT.

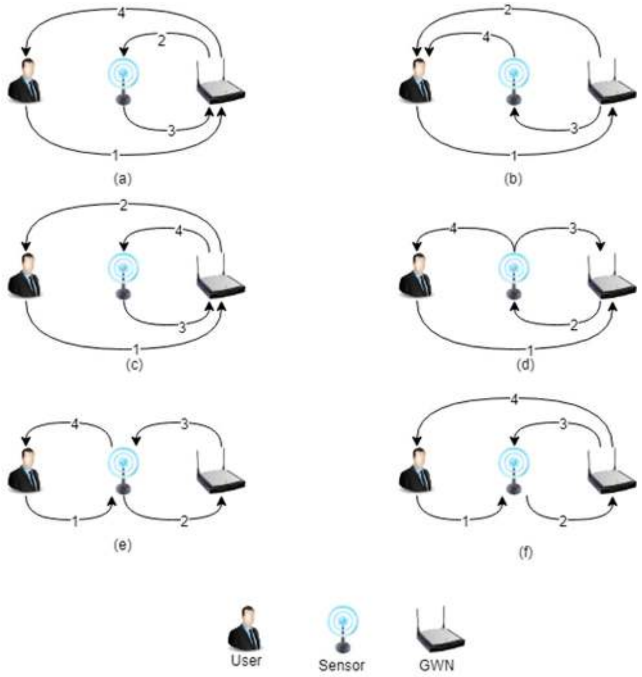

FIGURE 1. Authentication model of IoT network.

A. CONTRIBUTION OF RESEARCH

The main contribution of this work is to produce a comprehensive idea to the researcher about IoT authentication security and its peripherals. To formulate the idea, this research presented a well-developed taxonomy of attacks and a classification of technical methods used in IoT authentication systems. Additionally, network attacks have conversed against current IoT authentication protocols that can mitigate various threats. In addition, this paper elaborates on important evaluation techniques needed for authentication and compares it with existing protocols. Furthermore, this research extended to consider enormous security verification techniques, which are most important for the authentication mechanism. Additionally, this research produces important challenges and open issues that need to consider for future research proposals on designing an authentication mechanism.

The rest of the paper is formatted in the following manner (See FIGURE 2). In section II, this paper shows the classification of attacks and existing protocols to protect the IoT network from several attacks. Different technical methods of

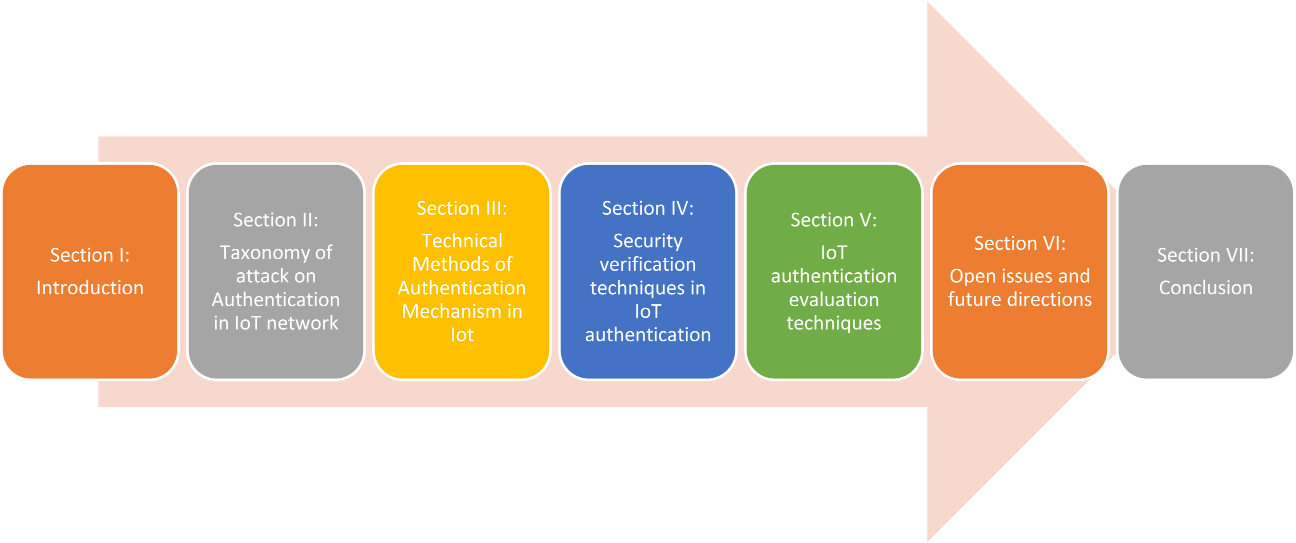
Section I:
Introduction
Section II:
Taxonomy of attack on Authentication in IoT network
Section III:
Technical Methods of Authentication Mechanism in Iot
Section IV:
Security verification techniques in IoT authentication
Section V:
IoT authentication evaluation techniques
Section VI:
Open issues and future directions
Section VII:
Conclusion

FIGURE 2. Organization of the document.

TABLE 1. Description of authentication model of iot network.

Flow of message **FIGURE 1 reference**	**1**	**2**	**3**	**4**	**Description**
(a)	User to GWN	GWN to sensor	Sensor to GWN	GWN to user	Users send the authentication request to gateway node then GWN sends user information to the nearest sensor of the user. After that sensor acknowledges the user's information and then GWN authenticates the user.
(b)	User to GWN	GWN to user	GWN to sensor	Sensor to user	Users send the authentication request to the gateway node then GWN sends the GWN authentication key to the user and sends user information to the nearest sensor to the user. After that, the sensor authenticates the user.
(c)	User to GWN	GWN to user	Sensor to GWN	GWN to sensor	Users send the authentication request to the gateway node then GWN sends the GWN authentication key to the user and sends user information to the nearest sensor to the user. After that, sensor responses to the GWN with sensor and user credentials to store.
(d)	User to GWN	GWN to sensor	Sensor to GWN	Sensor to user	Users send the authentication request to gateway node then GWN sends user information to the nearest sensor of the user. Then, the sensor, responses back to GWN with keys and acknowledge the user simultaneously.
(e)	User to sensor	Sensor to GWN	GWN to sensor	Sensor to user	Users send the authentication request to the nearest available sensor. Then, the sensor request back to GWN, GWN sends an acknowledgment to the sensor. After that, the sensor acknowledges the user.
(f)	User to sensor	Sensor to GWN	GWN to sensor	GWN to user	Users send the authentication request to the nearest available sensor. Then, the sensor request back to GWN, GWN sends an acknowledgment to the sensor and authenticates the user simultaneously.

the IoT authentication mechanism is provided in section III. After that in section IV, security verification techniques have been discussed followed by IoT authentication evaluation techniques in section V. Furthermore, open challenges and future directions based on IoT authentication are discussed in section VI. Lastly, this discussion has been concluded by pointing out important issues in the current phenomenon in section VII.

II. TAXONOMY OF ATTACK ON AUTHENTICATION IN IoT NETWORK

Attackers target network to gain access over it and get valuable information to sell over a black market [15] or fulfill their requirements. Among all the network attacks, this paper will concentrate on a range of attacks related to IoT authentications. FIGURE 3 illustrates the well-formulated taxonomy of attacks on IoT authentications.

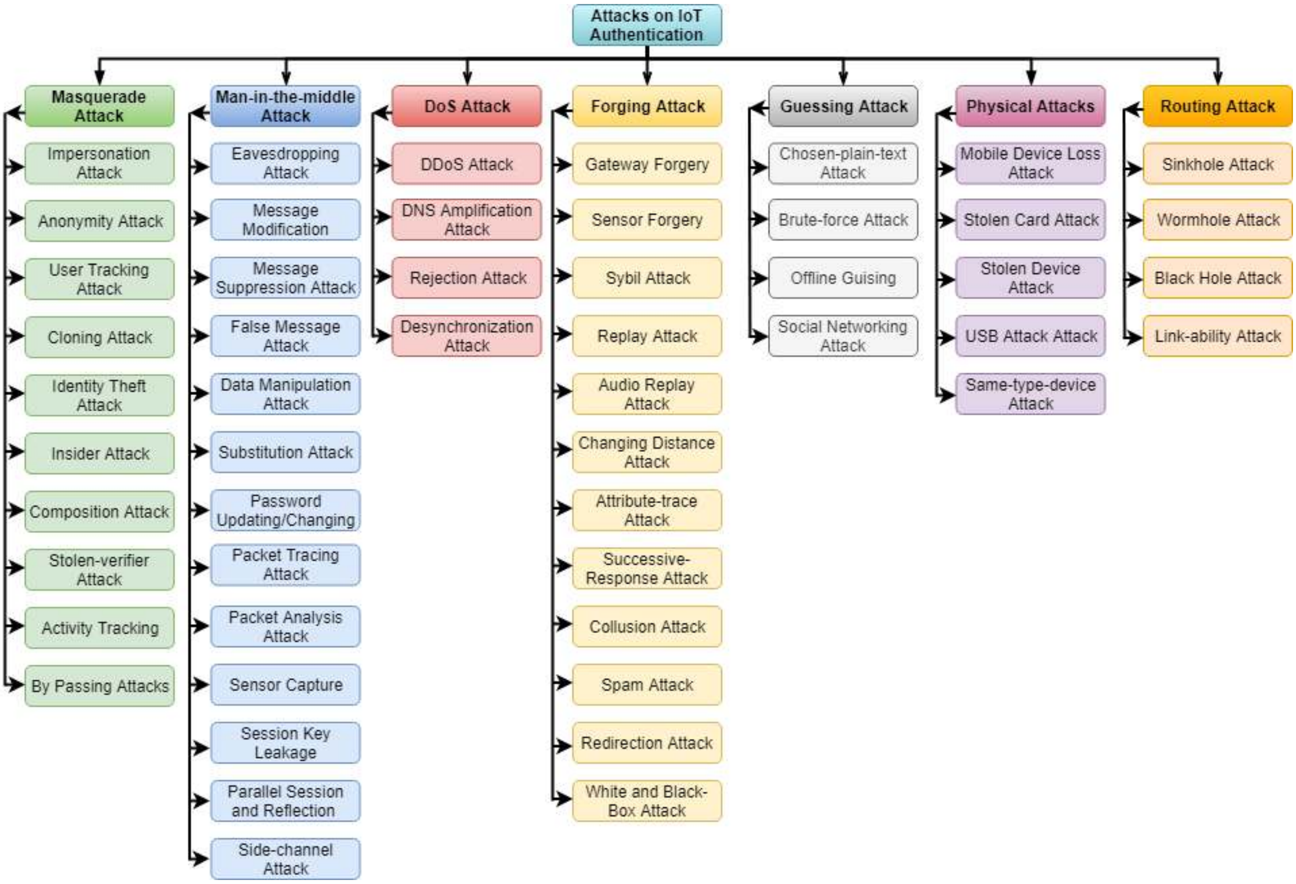

FIGURE 3. Taxonomy of attacks on IoT authentication.

Furthermore, TABLE 3 demonstrates the description of every major attack as per as authentication is a concern in IoT networks. As per the document, the classification of all the attacks is clustered in seven major categories, which are masquerade attack, man-in-the-middle attack, DoS attack, forging attack, guessing attack, physical attack, routing attack. Firstly, the masquerade attack distinguishes itself from other attacks on fake identity aspects; on which attacker counterfeit identification of legitimate users. Forging attacks can be differentiated by its nature, where an attacker tries to imitate the existing component or system. Man-in-the-Middle (MitM), on the other hand, snoop network traffic between two communicators. In a DoS attack, the adversary floods the network with packets to jam communication and penetrate the network. Instead of imitating the existing components or flooding the network, adversaries predict and try to explore the possibilities of getting confidential authentication credentials of legal users in guessing attacks. Guessing attack has shown to be dangerous, but further exploitation on the network happens when an attacker tries to get access to the IoT network through physical components. This exploitation is typically called a physical attack. Lastly, a routing attack is to create a fake route to send or receive packets in an IoT network. Moreover, all the above categories of attacks in IoT authentications are elaborately described in the following sections using the counterpart of the existing protection mechanism.

A. MASQUERADE ATTACK

IoT authentication is based on identity and if the identity is compromised, then the network can be vulnerable. In the *masquerade attack*, the adversary uses fake identification to authorize himself as a genuine user in the network. If the IoT network is not properly protected, it can be attacked by *masquerade attacks*, which can be prepared using stolen identification like a user id or password or detecting user's behavior tracking. This type of attack in the IoT network is very common but it depends on the level of authorization a network has managed to attain. As such, masquerade attackers can have a full smorgasbord of cybercrime opportunities if they have gained the highest access authority to a business organization. FIGURE 3 elaborates a full range of possible masquerade attacks in IoT network based on authentication security.

Impersonation attack is a sophisticated attack in IoT, where the adversary intercepts the authentication request of the previous session of another user and uses that information

TABLE 2. Acronyms and its definition.

Acronyms	Definition	Acronyms	Definition
AES	Advanced Encryption Standard	**Ipv4**	Internet Protocol version 4
AOMDV	Ad hoc on demand Multipath Distance Vector	**Ipv6**	Internet Protocol version 6
AS	Authentication server	**LLN**	Low power and lossy network
AVISPA	Automated Validation of Internet Security Protocols and Application	**LTE**	Long term evolution
BAKE	Biometric Authenticated Key Exchange	**MiM**	Man-in-the-middle
BAN	Burrows-Abadi-Needham	**MIoT**	Mobile Internet of things
BS	Base station	**MLP**	Multilayer Perceptron
CPA	Chosen-plaintext attack	**MOD**	Modulo
DB	Database	**NFC**	Near field communication
DDoS	Distributed Denial of service	**OTP**	One time password
DNS	Domain name system	**PDR**	Packet delivery ratio
DoS	Denial of service	**RFID**	Radio-frequency identification
E2ED	End-to-End Delay	**ROM**	Random oracle model
ECC	Elliptic-curve cryptography	**ROR**	Real of random
ECDSA	Elliptic Curve Digital Signature Algorithm	**RSA**	Rivest–Shamir–Adleman
GWN	Gateway node	**SC**	Smart card
HED	Heuristic-based detection	**SN**	Sensor node
HMAC	Hash-based Message Authentication Code	**SoSs**	Systems of Systems
HSN	Health Social Networks	**TP**	Throughput
IDS	Intrusion detection system	**UAV**	Unmanned aerial vehicle
IIoT	Industrial internet of Things	**USB**	Universal serial bus
IoE	Internet of environment	**VANET**	Vehicular ad-hoc network
IoS	Internet of services	**WSN**	Wireless sensor network
IoT	Internet of things	**XOR**	Exclusive OR
IoV	Internet of vehicles		

TABLE 3. Description of attacks on IoT authentication.

Attacks	Description
Masquerade Attack	In this attack, adversary counterfeit identity of the legitimate user to get access to the network.
Man-in-the-middle Attack	In this attack, attackers inquire impertinently communication between two communicators.
DoS Attack	In this attack, attackers flood the network by spreading inconvenient packets and disrupt actual communication to penetrate the network.
Forging Attack	In this attack, an adversary emulates a system or authenticated user to gain access to the network.
Guessing Attack	In this attack, attackers predict and explore the possibilities of getting advantages over the credentials of legal users.
Physical Attack	In this attack, network enemies try to get access to the physical components. In addition, they may penetrate the network or inject malicious scripts into the network, after getting physical access
Routing Attack	In this attack, attackers create an improper route to send or receive packets in a network.

to authenticate itself. In contrast, Tu, et al. [16] proposed a novel techniques to handle the *impersonation attack* in fog computing using Q-learning algorithm. FIGURE 4 shows the before and after *impersonation attack* in the IoT network.

User impersonation allows an attacker to steal the information of an actual user to get into the system for unusual activities. A *user impersonation attack* can be done in several ways. It is practical that an actual user may be leaked server's private

TABLE 4. Description of different types of masquerade attacks.

Masquerade Attacks	Description
Impersonation Attack	In this attack, an adversary successfully assumes the identity of a legitimate user.
Anonymity Attack	In this attack, an adversary hides their identity and perform attack anonymously.
User Tracking Attack	In this attack, an attacker track users' footsteps and steels information.
Cloning Attack	In this attack, an adversary creates an instance of a legal user.
Identity Theft Attack	In this attack, an adversary steals the identification of a genuine user to perform the suspicious task.
Insider Attack	In this attack, an authorized user of the network performs a malicious task from inside the network.
Composition Attack	In this attack, attackers merge or overlap the same kind of dataset from a different body.
Stolen-verifier Attack	In this attack, an intruder steals verification data of current or past authentication sessions form the authentication server and then try to get into the server using the compromised data.
Activity Tracking	In this attack, attackers monitor the activity of a genuine user
By-Passing Attack	In this attack, an attacker captures a packet from the user and responds to the user as a genuine receiving node.

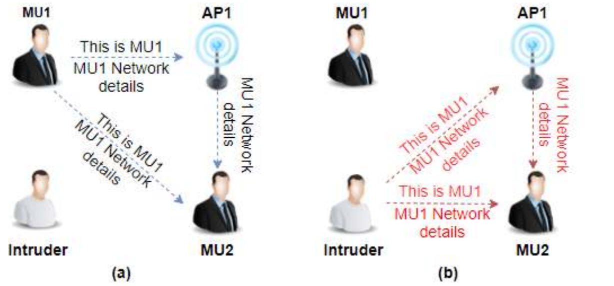

FIGURE 4. (a) Before and (b) after - The impersonation attack, AP: Access point. MU: Mobile user.

information to the attacker. The legal user also can act like an attacker. Amin *et al.* [17] explained in their protocol on how to protect the IoT network from *user impersonation attack* during authentication. Furthermore, a plethora of protocols have been designed to protect IoT networks from attackers during authentication, but many of them are designed to protect specific kinds of attacks. Therefore, all of these protocols are open for many other attacks; *sensor impersonation* is one of them. During the process of authentication, users, sensors, GWNs or servers, exchange messages among themselves to come on a mutual goal. In this situation, an attacker can sense the network, get information sent by the sensor and modify the data to act as a legal sensor.

Hence, the improved scheme like Jiang *et al. et al.* [18] protocol, can resist sensor node *impersonation attack*. In such cases, IoT users deserve to be anonymized as their activities can be tracked and the pattern of the user's behavior can be predicted. An attacker can predict users' position and their network using capabilities if the authentication protocols are weak. In the same way, a central problem in sensor network security is that sensors are susceptible to physical capture attacks. Once a sensor is compromised, the adversary can easily launch clone attacks by replicating the compromised node, distributing the clones throughout the network, and starting a variety of *insider attacks*. Attackers can clone to the smart card, tags to get more opportunities to explore the network. Authentication protocols suffer from the challenges to protect *cloning attack* from either a high computation or storage overhead or poor detection accuracy. Wallrabenstein [19] proposed IoT Device Authentication using Physical Un-cloneable Functions. On the other hand, an *identity theft attack* is one of the tricky methods to get the identity of an authorized user in various unauthorized ways, such as data breaches, unsecured websites, social networks, phishing, public computers, and skimming. Authentication protocols are victimized by *identity theft attacks* in almost all the IoT sectors, including IoV, IIoT, and MIoT. Researchers have introduced several different techniques [20], [50] to counterpart the attack. In addition, In a network, a genuine user can behave as an attacker. An authorized user can also act like another legal user by using his/ her credentials. Therefore, an internal user who has authorized access to the system and the network launches an *insider attack*. Therefore, data protection by using anonymization techniques to hide personal information from the published dataset is essential.

However, attackers can use a *composition attack* to merge or overlap the same kind of dataset from a different body. Ganta *et al.* [51] discussed *composition attack* in auxiliary information and Baig *et al.* [52] show how to prevent *composition attack* in non-interactive data publishing setting by combining sampling and generation. Furthermore, an intruder can steal verification data form the authentication server in the current or past authentication sessions. Then the adversary tries to get into the server using the compromised data. An advanced three-way authentication technique for IoT is designed by Cui, *et al.* [53] to prevent various attacks, among them *stolen-verifier attack* is one of the most challenging. Additionally, the proliferation of software and technology growth allows users to provide the specific function of their activities, household device management or personal assistance. That third-party software can be hacked and user's activity can be monitored and used against them. Besides, IoT infrastructures are more prone to welcome these threats. Viana *et al.* [54] introduced conflict management in Systems of Systems (SoSs). The paper presented a framework for managing unpredictability in the system. In addition, many authentication protocols use the session key to protect from network attacks like a replay attack, but this session key can be compromised and used against the system to be a masquerade. However, as the authentication process needs many communication and message passing among nodes, the attacker can get a message and process among themselves and pass it back to the sender bypassing the actual node. This type of attack is called a *node by-passing attack*. IoT authentication schemes are in jeopardy of *node by-passing attacks* by *GWN by-passing attacks*, *base station by-passing attack* or *sensor* by-passing attack. Sarvabhatla and Vorugunti [21] designed a secure biometric-based user authentication scheme, which provides *base station by-passing attack* protection. Chang *et al.* [22] proposed two-factor authentication that can protect *GWN by-passing attack* whereas, authentication protocol for an IoT-enabled LTE network by Saxena *et al.* [23], gives protection towards *secret key by-passing attack*. The details about the IoT authentication protocols to protect against *masquerade attacks* are tabulated in TABLE 5.

B. MAN-IN-THE-MIDDLE ATTACK

In Man in the middle attack, an attacker secretly taps a network and absorbs communication data between two parties who trust that they are directly connected and communicating with each other. In this scenario, the attacker can drop, modifies, and alters the communication data as well as can predict network and security patterns. Additionally, they use legitimate users' data to establish new communication in the system. FIGURE 3 shows the classification and FIGURE 5 illustrates the man-in-the-middle attack in the IoT authentication scenario. In addition, TABLE 6 shows a description of all MitM attacks.

In a MitM attack, eavesdroppers try to steal authentication data by unauthorized way, while communication takes place between nodes, over an IoT network. Attackers try to find and establish a weak network connection between sensors and server and transfer network signal itself. Not only that but also, they install network monitoring software [49], which helps to snoop all transmitted authenticated data. However, eavesdropping is difficult to identify because of abnormality during transmission. Li *et al.* [55] proposed an interesting anti-eavesdropping scheme by friendly jammers to an industrial crowd-sensing network. Alternatively, *message modification* is a type of active attack, where an attacker sniffs actual data from the network and pass the modified data to the receiver. Asaduzzaman *et al.* [56] designed a protocol to offer better security over *message modification attack* near NFC architecture. Zhang, et al. [57] describes different abnormalities in VANETs, including *massage suppression attacks*. In *massage suppression attacks*, attacker multicast prevalent spoofed message over the network to prevent actual nodes to get original messages and force them to refresh cache every time. Pu and Zhou [58] shown a heuristic-based detection scheme (HED) to analyze and defend the *message suppression attack* in low power and lossy networks (LLNs). Likewise, a *false message attack* adversary sends inappropriate data to the victim to misguide the user. Moreover, data can be transferred to the server as well as the end-user. Nevertheless, several protocols are designed to sense and prevent false messaging attacks [57], [59], [60]. Similarly, in a *data manipulation attack*, the attacker does not delete the data after retrieving from the actual source. Instead of deleting or tampering the data, they alter the actual content of the information and sends in to the targeted location. To emphasis, Khan *et al.* [61] designed a distributed intrusion detection system (IDS) to detect and protect network form *data manipulation attacks*. On the other hand, a *substitution attack*occurs when an attacker deliberately replaces the authentication or authorization algorithm by a forgery code to validate fraud user or gain access to the system. As in the technique the actual encryption method is superseded, is vulnerable to different attacks.

However, during the past few years, hackers compromised several IoT networks to harvest user information including user id and hashed password even in worst-case plain text password. This compromised account is often offered in the black market [15] or leaked publicly. In addition, intruders often intercept data during the transaction in a network and can change the password of a legitimate user. As IoT is a collection of heterogeneous devices with internetworking systems and most of the peripherals are connected in WSN, devices always populate data and send over networks. Therefore, attackers can use powerful devices to sniff those packets, disseminate information, and use for their purpose. Moreover, a network can be accessed through a wired or wireless medium. Ferrag and Ahmim [62] and Yao *et al.* [63] designed different protocols to prevent *packet tracking attacks*. Similarly, after getting the raw packets from the targeted network, hackers try to extract information from the pool of [28] data. Therefore, they use strong tools to disseminate data [65] and to produce powerful information that they can use to intercept the user or network. *Packet analysis attacks* are prevented by several mechanisms in IoT [62], [63]. Furthermore, adversaries intend to capture sensors in WSN to get information about network patterns and users' details. They try to hack the sensor by penetrating the network if the security of the network is weak.

However, researchers have noticed those attacks and designed IoT authentication protocols to protect them against this type of attack [28], [69]. For the same reason, authentication protocols use session keys to prevent several attacks to occur in the network. However, this session keys can be compromised to design a new type of attack. If an attacker can get the session key of a particular session, then they can redesign the user's data and can create fake users and sessions to attack a network. Wu *et al.* [28] authentication and key agreement scheme ensure to protect against *session key leakage attack*. Similarly, after getting the session key and user details by network tapping, an eavesdropper can create a valid login request

TABLE 5. IoT authentication protocols against masquerade attack.

Masquerade attacks Protocols	Impersonation attack	Anonymity Attack	Tracking Attack	Cloning Attack	Identity Theft Attack	Insider Attack	Composition Attack	Stolen-Verifier Attack	Activity Tracking	By-Passing Attacks
Amin, et al. [17]	No	Yes	No	No	No	Yes	No	No	No	No
Jiang, et al. [18]	Yes	Yes	Yes	No	No	Yes	No	No	No	No
Wallrabenstein [19]	No	No	No	Yes	No	No	No	No	No	No
He, et al. [20]	No	No	No	No	Yes	No	No	No	No	No
Sarvabhatla and Vorugunti [21]	Yes	No	No	No	No	Yes	No	Yes	No	Yes
Chang, et al. [22]	Yes	Yes	Yes	No	No	Yes	No	Yes	No	Yes
Saxena, et al. [23]	Yes	Yes	No	No	Yes	No	No	No	No	Yes
Chang and Le [24]	Yes	No	No	No	No	Yes	No	Yes	No	No
Dolev, et al. [25]	Yes	Yes	No	No	No	No	No	No	No	No
Farash, et al. [26]	Yes	No	No	No	No	Yes	No	Yes	No	No
Banerjee, et al. [27]	No	No	Yes	No	Yes	No	No	No	Yes	No
Wu, et al. [28]	Yes	Yes	Yes	No	No	Yes	No	No	No	No
Gope, et al. [29]	Yes	Yes	Yes	No	No	No	No	No	No	No
Kang, et al. [30]	Yes	Yes	No	No	No	Yes	No	No	No	No
Li, et al. [31]	Yes	Yes	Yes	No	No	Yes	No	No	No	No
Li, et al. [32]	Yes	Yes	Yes	No	No	Yes	No	No	No	No
Li, et al. [33]	Yes	Yes	Yes	No	No	Yes	No	No	No	No
Roy, et al. [34]	Yes	Yes	No	No	No	No	No	No	No	No
Wang, et al. [35]	Yes	Yes	Yes	No	No	Yes	No	No	No	No
Amin, et al. [36]	Yes	Yes	No	No	No	Yes	Yes	Yes	No	No
Yeh [37]	Yes	Yes	No	No	No	No	No	No	No	No
Challa, et al. [38]	Yes	Yes	Yes	No	No	Yes	No	No	No	No
Jiang, et al. [39]	Yes	Yes	Yes	No	No	Yes	No	No	No	No
Srinivas, et al. [40]	Yes	Yes	No	No	No	Yes	Yes	No	No	No
Shen, et al. [41]	Yes	No	No	No	No	No	No	No	No	No
Punithavathi, et al. [42]	Yes	No	No	No	No	Yes	No	No	No	No
Dammak, et al. [43]	Yes	Yes	No	No	No	Yes	No	No	No	No
Bali and Kumar [44]	No	Yes	No	No	No	No	No	No	No	No
Gope and Hwang [45]	No	Yes	No	No	No	No	No	No	No	No
Malina, et al. [46]	No	Yes	No	No	No	No	No	No	No	No
Aman, et al. [47]	No	No	No	Yes	No	No	No	No	No	No
de Almeida, et al. [48]	No	No	No	No	No	No	No	No	Yes	No

and start a new session with a sensor by masquerading a valid user. This type of attack is known as a *parallel session and reflection attacks*. Roy *et al.* [34] designed an authentication scheme with user biometrics and fuzzy extractor that protect against *parallel sessions and reflection attacks*. In general, IoT devices collect data and transmit them over the network in order to connect. During this process, devices emit signals, which is called "*side-channel*". These signals indicate the level of power consumption, electronic and aquatic emissions at any given time. At the same time, an intruder can overtake the encryption credentials by trespassing an IoT device using the *side-channel attack*. Moon *et al.* [77] proposed a

TABLE 6. **Description of different types of man-in-the-middle attacks.**

MitM Attacks	Description
Eavesdropping Attack	In this attack, an attacker tries to find and establish a weak network connection between sensors and servers and transfers network signals.
Message Modification	In this attack, an adversary modifies the actual message after receiving it from a user.
Message Suppression Attack	In this attack, an attacker drops original packets after receiving from a user.
False Message Attack	In this attack, an adversary tries to send an inappropriate message to the user.
Data Manipulation Attack	In this attack, an adversary manipulates and changes the received data.
Substitution Attack	In this attack, an attacker deliberately replaces the authentication or authorization algorithm by a forgery code to gain access to the system.
Password Updating/Changing	In this attack, an adversary changes or updates the actual password to access the network.
Packet Tracing Attack	In this attack, an attacker track user transmitted packets using powerful software like Wireshark[49].
Packet Analysis Attack	In this attack, an attacker performs an analysis of users' packets to get valuable information.
Sensor Capture Attack	In this attack, an adversary captures sensor node and manipulate their functionality.
Session Key Leakage	In this attack, an attacker tries to get the previous session key to authenticate themselves in the current session.
Parallel Session and Reflection Attacks	In this attack, an adversary clones another session key and perform task concurrently in a network using the same session identifier.
Side-Channel Attack	In this attack, an attacker overtakes the encryption credentials by trespassing an IoT device.

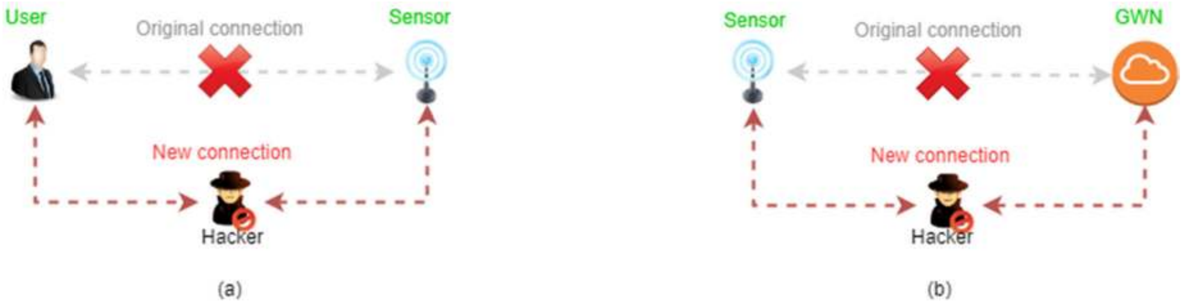

FIGURE 5. **Man-in-the-middle attack in IoT network during authentication. (a) User and sensor scenario and (b) sensor and GWN scenario.**

countermeasure of *side-channel attack* in IoT through a bit checking mechanism. TABLE 7 illustrates IoT authentication protocols, which give support to protect against man in the middle attack. Though the MitM attack is a serious issue in IoT authentication techniques, protocols are less attentive in different types of attacks in MitM. Among all most of the authentication protocols concentrated on *eavesdropping attack* and *sensor capture attack*.

C. DOS ATTACK

During denial of service (DoS), attack an advisory denies a service from a server, network to an authorized user by creating a large number of requests to the server at a time. *DoS attack* is quite common in IoT based network, where an unauthorized user sends thousands of requests to the authentication server to shut down the operation temporarily. To contrast, de Almeida *et al.* [48] developed a method to defense *Dos attack* in a network by providing packet-level authentication. In addition, a *distributed denial of service attack* is an advanced *DoS attack* where *DoS* is performed in a distributed manner. To execute *DDoS attacks*, attackers use a huge network of botnets to put down the service of a network. As a result, genuine users cannot access the service from a particular network. Consequently, Liu *et al.* [78] developed an enhanced distributed low-rate attack mitigation mechanism for IoT networks.

On the other hand, as per FIGURE 6, the *DNS amplification attack* takes advantage of DNS behavior in order to amplify the attack. A DNS server holds the public IP addresses and their accompanying hostnames. Therefore, the DNS resolver requests the IP of a hostname to the DNS server. If the server does not contain the information, it refers to one of the root DNS servers, which refers to another DNS server to provide the IP, which boosts this attack.

During the *DNS amplification attack*, attacker spoof the IP of victims IP send a request to provide DNS list to the server. Because of spoofing all replies go to the victim's system and the attacker can amplify the attack up to 100%. To protect the *DNS amplification attack*, IoT needs

TABLE 7. IoT authentication protocols to protect against MITM attacks.

MitM Attacks Protocols	Eavesdropping attack	Message modification attack	Message suppression attack	False message attack	Data manipulation attack	Substitution attack	Password Updating/Changing	Packet tracing attack	Packet analysis attack	Sensor capture	Session key leakage	Parallel Session and Reflection Attacks	Side-channel attack
Chang and Le [24]	No	No	No	No	No	No	No	No	No	Yes	No	No	No
Banerjee, et al. [27]	Yes	No	No	No	No	No	No	No	No	Yes	No	No	No
Wu, et al. [28]	Yes	No	No	No	No	No	No	No	No	Yes	Yes	No	Yes
Kang, et al. [30]	Yes	No	No	No	No	No	No	No	No	No	No	No	No
Li, et al. [31]	Yes	No	No	No	No	No	No	No	No	Yes	No	No	No
Li, et al. [32]	No	No	No	No	No	No	No	No	No	No	No	No	Yes
Li, et al. [33]	Yes	No	No	No	No	No	No	No	No	No	No	No	No
Roy, et al. [34]	No	No	No	No	No	No	No	No	No	No	No	Yes	No
Wang, et al. [35]	Yes	No	No	No	No	No	No	No	No	Yes	No	No	No
Amin, et al. [36]	No	No	No	No	No	No	No	No	No	Yes	No	No	No
Challa, et al. [38]	Yes	No	No	No	No	No	No	No	No	No	No	No	No
Srinivas, et al. [40]	No	No	No	No	No	No	No	No	No	Yes	No	No	No
Shen, et al. [41]	Yes	No	No	No	No	No	No	No	No	No	No	No	No
Dammak, et al. [43]	No	No	No	No	No	No	No	No	No	Yes	No	No	No
Zhang, et al. [57]	No	No	Yes	Yes	No	No	No	No	No	No	No	No	No
Pu and Zhou [58]	No	No	Yes	No	No	No	No	No	No	No	No	No	No
Kim, et al. [59]	No	No	No	Yes	No	No	No	No	No	No	No	No	No
Khan, et al. [61]	No	No	No	No	Yes	No	No	No	No	No	No	No	No
Mahmood, et al. [66]	No	Yes	No	Yes	No	No	No	No	No	No	No	No	No
Ferrag, et al. [67]	No	Yes	No	Yes	No	No	No	Yes	Yes	No	No	No	No
Griffin [68]	No	No	No	No	No	Yes	No	No	No	No	No	No	No
Wu, et al. [69]	No	No	No	No	No	No	No	No	No	Yes	No	No	No
Kumari, et al. [70]	No	No	No	No	No	No	No	No	No	No	No	Yes	No
Sciancalepore, et al. [71]	No	No	No	No	No	No	No	No	No	No	No	No	Yes
Jan, et al. [72]	Yes	No	No	No	No	No	No	No	No	No	No	No	No
Hu, et al. [73]	Yes	No	No	No	No	No	No	No	No	No	No	No	No
Song, et al. [74]	Yes	No	No	No	No	No	No	No	No	No	No	No	No
Hong, et al. [75]	Yes	No	No	No	No	No	No	No	No	No	No	No	No
Xue, et al. [76]	No	No	No	No	No	No	Yes	No	No	No	No	No	No

more research. Similarly, *Flooding* is a type of *Denial of Service attack* that is aimed to put a server or network down by flooding it with a huge number of traffics. *Syn-flood* is one of the most hazardous in IoT network, where the IoT network and application server become so weighted down initiating incomplete connection request that it no longer process a genuine request from the authenticated node. Additionally, when a node tries to communicate via exchanging common interest information, various attacks take place to capture the transmitted data without a proper certificate. After that, the captured data can be rejected and prevent from further travel to the destination. This type of attack is known as

TABLE 8. Description of different types of DOS attacks.

DoS Attacks	Description
DDoS attack	In this attack, attackers deny service from a server or network to an authorized user by creating a large number of requests to the server at a time. This action is performed in a distributed fashion.
DNS Amplification attack	In this attack, an attacker increases the replies from a server to a user by spoofing its IP and performing false DNS requests.
Rejection attack	In this attack, an adversary ignores the request of communication from a legal user.
Desynchronization attack	In this attack, an attacker blocks communication between RFID redder and backend server. Therefore, the tag's information from the RFID device and server mismatches.

TABLE 9. IoT authentication protocols to protect against DOS attacks.

DoS Attacks Protocols	DoS/DDoS attack	DNS Amplification attack	Flooding attack	Desynchronization Attack
Dolev, et al. [25]	Yes	No	No	No
Farash, et al. [26]	Yes	No	No	No
Gope, et al. [29]	Yes	No	No	Yes
Li, et al. [31]	No	No	No	Yes
Wang, et al. [35]	Yes	No	No	Yes
Challa, et al. [38]	Yes	No	No	No
Bali and Kumar [44]	No	No	Yes	No
Gope and Hwang [45]	Yes	No	No	No
Moosavi, et al. [64]	Yes	No	Yes	No
Jan, et al. [72]	Yes	No	No	No
Hong, et al. [75]	Yes	No	No	No
Sarvabhatla, et al. [79]	Yes	No	No	No
Huh, et al. [80]	Yes	No	No	No
Anagnostopoulos, et al. [81]	No	Yes	No	No
Salman, et al. [82]	Yes	No	No	No

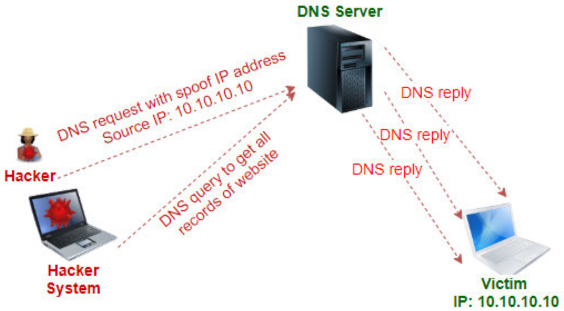

FIGURE 6. DNS amplification attack.

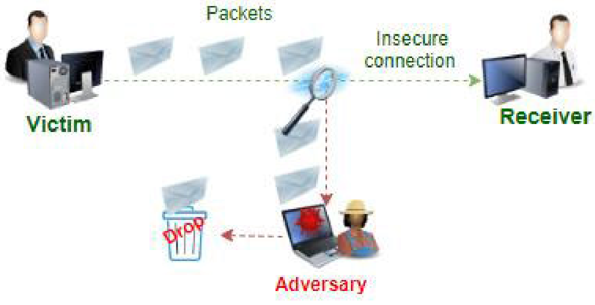

FIGURE 7. Rejection attack.

the *Rejection attack*. Alternatively, RFID related authentication systems use a backend database to authenticate the user. Therefore, the attacker performs a *desynchronization attack* to block the communication between the RFID reader and backend database server so that the tag's key stored in the database and the tag's memory mismatches and denies access. A way of *rejection attack* has been demonstrated in FIGURE 7. Moreover, an illustration of IoT authentication protocols, which protect from DoS attacks, is shown in TABLE 9.

D. FORGING ATTACK

Forging attack allows an attacker to steal authentication information of a genuine user in a network and use the information as an authenticated user to gain access

TABLE 10. Description of different types of forging attacks.

Forging Attacks	Description
Gateway Forgery	In this attack, the attacker acts as a gateway to a genuine user. To do so, the attacker gets messages from the user and response to the user with morph data.
Sensor Forgery	In this attack, the attacker acts as a sensor to the genuine user. To do so, the attacker gets messages from the user and response to the user with morph data.
Sybil Attack	In this attack, an attacker node holds multiple instances to communicate in a network. These achievements are possible by disabling or forging legitimate nodes in the network.
Replay Attack	In this attack, an attacker capture the data send by the user and forward it to the next hop as an actual user.
Audio Replay Attack	In this attack, an attacker spoof the network and tries to act like an automatic speaker verifier.
Changing Distance Attack	In this attack, an attacker performs malicious activities by manipulating the distance between the objects in IoT.
Attribute-Trace Attack	In this attack, an attacker tracks the attributes that send during the communication and utilizes those attributes for further communication as a user.
Successive-Response Attack	In this attack, the attacker acts like another user and sends the request to the gateway or server repeatedly so that the server can send multiple responses for an established communication and the attacker can guess other credentials that have used during this communication.
Collusion Attack	In this attack, an attacker can combine two different datasets and produce a completely new dataset to perform the attack.
Spam Attack	In this attack, an attacker sends information to the network along with malicious code to inject the virus into the network.
Redirection Attack	In this attack, an attacker forwards messages to the other route to execute an unexpected task.
White and Black-Box Attack	When an adversary attacks a network and gain full access to the target model, known as a white-box attack but the attacker does not possess many ideas about explicit knowledge and can design an attack then it is called a black-box attack.

over confidential data. It can be further classified in *user forgery attack, sensor forgery attack, gateway forgery attack, Sybil attack, replay attack, audio replay attack, changing distance attack, attribute-trace attack, successive-response attack, collusion attack, spam attack, redirection attack, white and black-box attack.* FIGURE 3 shows the classification and TABLE 10 illustrates the description of *forgery attacks* in IoT authentication.

An attacker can behave like a normal user if he/ she gets or intends to get authenticated data from a process of authentication in the IoT network. In a different phase, the adversary may use prediction to the different messages to gain access to the user's data or the network, which is known as *user forgery attack*. To protect the IoT systems from *user forgery attack* Wu *et al.* [28] invented an effective authentication protocol. On the other hand, sensor plays a major role in IoT authentication, as all the authentication messages pass through any of the sensors. Due to a lack of computation and storage capacity, IoT authentication protocols use simple and robust encryption and decryption techniques, which make attackers to open the gate for *sensor forging attack*. In WSN, hackers use malicious scripts to get access to the authentication process data from the sensor and after modifying them pass to victims as the original message. In between, there is a chance to grab the information from the authentication request if the message is not properly encrypted. To highlight, Wu *et al.* [28] describe how their protocol protects *sensor forgery attack*. Unlike *sensor forgery*, if the protocol has breached, antagonists also can forge the gateway node. In this situation, adversary takes advantage over GWN, and then mitigates authentication requests, after that gets users and network information and finally morph existing data. Wu *et al.* [28] proposes a protocol that protects the IoT network from *gateway forgery attack* by spreading important information in different messages. On the other hand, in the *Sybil attack*, a malicious node possesses multiple identifications in order to establish communication in an IoT network, which could be achieved by disabling or forging legitimate nodes in the network. In this attack, a single node or device can harm multiple devices from a different network. Suryani *et al.* [83] claimed that their protocol prevents *Sybil attack* during authentication using two-phase security protection. FIGURE 9 gives a clear view of the *Sybil attack*. Alternatively, in a *replay attack,* an attacker intercepts and acquires the data send by the sender and send it to the destination as an original sender. However, timestamp and sequence number with the packet can be implemented to prevent the *replay attack*. Moreover, there is various information pass through the IoT network and during authentication, the node transfers its user id and password to the other node or authentication server. Therefore, that information can be captured and used to authenticate an intruder. In contrast, to take advantage of a *replay attack*, attackers need to access the raw network data and that is possible either via network tap, ARP poisoning or

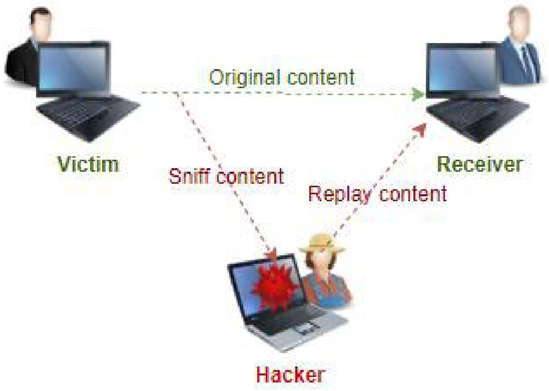

FIGURE 8. Replay attack.

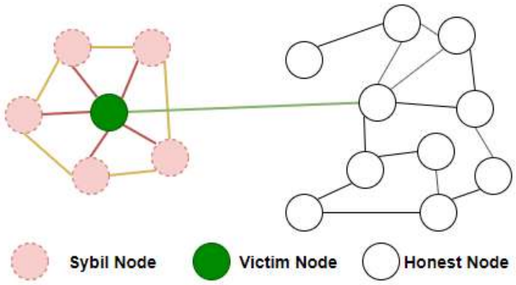

FIGURE 9. Sybil attack.

via installing the malware in the victim's computer. A *replay attack* is further illustrated in FIGURE 8.

IoT devices are heterogeneous in nature and dynamic in behavior. Moreover, IoT devices can be static and mobile. Therefore, the system tries to detect if the authentication distance and access distance of the devices fluctuates. Sometimes, adversaries try to increase the success probability of attacks by changing the distance between devices. This phenomenon is known as changing *distance attacks.* Chen *et al.* [84] introduces a fingerprint-based authentication protocol to prevent *changing distance attack*. On the contrary, an amount of IoT systems are required to tag with formalized attributes to authenticate the activities of the auditor. For example, Health Social Networks (HSN) use attribute tagging widely. Where the attribute-oriented authentication scheme empowers to generate an HSN attribute for every HSN user to protect from *attribute tracking attack*. In 2012, Liang *et al.* [90] proposed attribute security in HSN. After that, Uddin *et al.* [86] proposed tier-based health architecture in a patient-centric agent to monitor patient health. Comparably, a user sends authentication requests to the network to participate. In return, the authentication server exchanges several other packets with the user to reply, acknowledge or response. Therefore, attackers take advantage of those packets by sending a successive packet so that the previous packet, which was sent by the original sender, will discard and the attacker can intrude into the system. Lu *et al.* [87] claimed that their privacy preservation protocol successfully prevents *successive-response attack* on IoV network. Nevertheless, in the *collusion attack,* the execution of operation can combine, manipulate and produce a completely new dataset, especially files, to disguise the server. However, spoofing multiple packets from various user's authentication information and create a set of new authentication packets can also count as a *collusion attack*. Nevertheless, unnecessary and irrelevant packets send to the enormous number of users through the internet just to fulfill phishing or spreading malware. On the other hand, the main target of *spam attacks* is to introduce viruses, worm, spyware, Trojan horse to various legitimate systems. It spread through email by some offensive link, website, or the web content as well as without proper sender mail id. Paavolainen *et al.* [88] converse about various risks on blockchain in IoT by *spam attack*. Likewise, open redirect abuse is not much popular in IoT but it can cause a problem on security as it redirects to malicious content instead of the actual one. However, detecting IP and protocol creating spam can reduce the possibilities of *redirection attacks*.

Likewise, internet attacks are classified into different categories. Among them, when an adversary attacks and gains full access and control to the target model are known as a *white-box attack*. In contrast, while performing a *black-box attack*, the hacker does not have any idea about explicit knowledge but can design queries to achieve corresponding desire [89].

Additionally, cybercriminals attacking the IoT networks will be driven by the financial gain as the black market [15] for malware and the dark web continue to mature. During the authentication process, users, sensors and GWNs or servers send data among themselves to authenticate, authorize for registration or login. During that period, an intruder can attack the network and if the protocol is soft enough to penetrate, he/ she artifices message and uses as per his/ her requirement. Morphing user's data and intentionally passing wrong messages are common behavior for intruders. In spite of detecting the forgery attacks, prevention is very important. Therefore, researchers developed a protocol mechanism to protect the IoT network from various attacks. TABLE 11 describes most of the effective work by a few years to prevent a forgery attack in IoT authentication.

E. GUESSING ATTACK

IoT authentication server stores authentication information of users and different peripherals in IoT network, such as device id, user id, device secret key, user password. Adversaries try to get those credentials to access the system. If they have direct access to the server then they can extract passwords from the server, but if they cannot get those physically, then attackers try to guess the password to authenticate themselves as a valid user. This is known as a *guessing attack*. Description of all possible *guessing attacks* are discussed in TABLE 12. *guessing attacks* can be done using a *dictionary attack* or *brute force attack.* Wu *et al.* [28] proposed an authentication scheme for multi gateway WSN. Additionally, to authorize in a network, the attacker tries a plethora of possibilities.

TABLE 11. Forgery attack preventive IoT authentication protocols.

Forgery attacks Protocols	Gateway forgery	User forgery	Sensor forgery	Sybil attack	Replay attack	Changing distance attack	Attribute-trace attack	Successive-response attack	Collusion attack	Spam attack	Redirection Attack	White and Black-box attack
Saxena, et al. [23]	No	No	No	No	Yes	No	No	No	No	No	Yes	No
Wu, et al. [28]	Yes	Yes	Yes	No	No	No	No	No	No	No	No	No
Suryani, et al. [83]	No	No	No	Yes	No	No	No	No	No	No	No	No
Chen, et al. [84]	No	No	No	No	Yes	Yes	No	No	No	No	No	No
Raja and Beno [85]	No	No	No	Yes	No	No	No	No	No	No	No	No
Uddin, et al. [86]	No	No	No	No	No	No	Yes	No	Yes	No	No	No
Lu, et al. [87]	No	No	No	No	Yes	No	No	Yes	No	No	No	No
Paavolainen, et al. [88]	No	No	No	No	No	No	No	No	No	Yes	No	No
Du, et al. [89]	No	No	No	No	No	No	No	No	No	No	No	Yes

TABLE 12. Description of different types of guessing attacks.

Guessing Attacks	Description
Chosen-Plaintext Attack	In this attack, the attacker chooses random plaintext to cryptanalysis a protocol and get information from that.
Brute-Force Attack	In this attack, an attacker uses a trial and error method to get into a protected dataset.
Offline Guising	In this attack, an adversary user software to guess and try credential in offline mode.
Social Networking Attack	In this attack, an adversary tries to guess credentials by using information about common interests and other personal information.

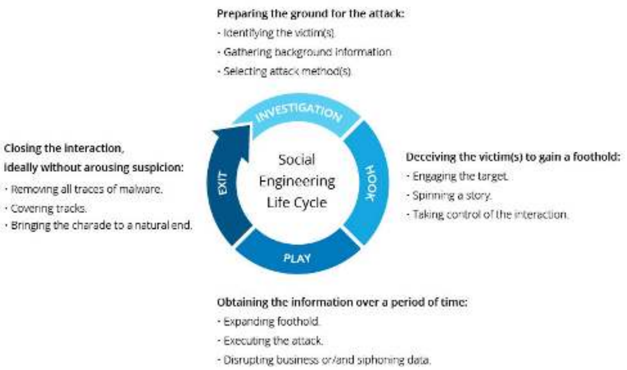
Preparing the ground for the attack:
- Identifying the victim(s).
- Gathering background information.
- Selecting attack method(s).
INVESTIGATION
Closing the interaction,
ideally without arousing suspicion:
· Removing all traces of malware.
· Covering tracks.
· Bringing the charade to a natural end.
EXIT
Social Engineering Life Cycle
HOOK
Deceiving the victim(s) to gain a foothold:
- Engaging the target.
- Spinning a story.
- Taking control of the interaction.
PLAY
Obtaining the information over a period of time:
- Expanding foothold.
- Executing the attack.
- Disrupting business or/and siphoning data.

FIGURE 10. Social engineering attack lifecycle [97].

Consequently, in the *chosen-plaintext attack (CPA)* cryptanalysis process, adversary guesses plain text and encrypt with known possible encryption techniques to obtain the corresponding cipher text. Duan *et al.* [91] proposed a policy privacy solution by two-layer cooperating method for protecting IoT. Additionally, devices need several ways to authenticate IoT peripherals in a network, such as a password, smart card or biometric. Among them, the password system is popular but vulnerable. It can easily be victimized by attacks like *brute-force*, where attackers use software to guess the password to be authenticated. *Random password* and *common password guessing* are most effective among all other possibilities. Wang *et al.* [81] discussed how an attacker cracks IoT device user account by trespassing SMS authentication code using a *Brute-force attack*. On the other hand, attackers may perform eavesdropping on an authentication process or penetrate to the network to steal authentication code using a *Brute-force attack.* Similarly, attacker may perform eavesdropping on an authentication process or penetrate to the network to steal valuable user information or files to use them against a legal user of his/ her choosing. Therefore, if the user cracks the encryption process of the message, he/ she can try an *offline-guessing attack* on credentials. In an online password-guessing scenario, an attacker tries to guess a password by logging to the system. However, online password guessing is less powerful than offline password guessing since the attacker hasa maximum limit of tries. Alternatively, offline guessing can be performed without logging into the actual system and there is no such limitation exists. In different circumstances, social networking is an attack vector that relies based on human interaction. On which, a perpetrator tries to get common and social information of a victim to intercept him by guessing or predicting credentials. Baiting, Scareware, Pretexting, phishing, Spear phishing are common *social networking attacks* in IoS [95]. Harwood [96] describes the way to defend internet attacks on the web and

TABLE 13. IoT authentication protocols to protect against guessing attacks.

Guessing attacks Protocols	CPA	Brute-force Attack	Offline Guising	Social Networking Attack
Jiang, et al. [18]	No	No	Yes	No
Farash, et al. [26]	No	No	Yes	No
Kang, et al. [30]	No	No	Yes	No
Li, et al. [31]	No	No	Yes	No
Roy, et al. [34]	No	No	Yes	No
Wang, et al. [35]	No	No	Yes	No
Challa, et al. [38]	No	No	Yes	No
Jiang, et al. [39]	No	Yes	Yes	No
Punithavathi, et al. [42]	No	No	Yes	No
Dammak, et al. [43]	No	No	Yes	No
Duan, et al. [91]	Yes	No	No	No
Shen, et al. [92]	No	No	No	Yes
Wang, et al. [93]	No	Yes	No	No
Cho, et al. [94]	No	Yes	No	No

TABLE 14. Description of different types of physical attacks.

Physical Attacks	Description
Mobile Device Loss Attack	In this attack, an adversary performs attacks on IoT network-based extracted data from the lost mobile device.
Stolen Card Attack	In this attack, an adversary plans attacks on IoT network-based extracted data from stolen smart card.
Stolen Device Attack	In this attack, an attacker implements attacks on behalf of credentials on stolen devices from the IoT network.
USB Attack	In this attack, an adversary injects malicious scripts to the network by connecting USB or flash drives.
Same-Type-Device Attack	In this attack, an attacker uses the same details of another detail to be pretended as an actual device.

provided various opportunities in IoT platforms. A lifecycle of social engineering attack shown in FIGURE 10 [97]. Additionally, a list of IoT authentication protocols, which support against *guessing attack,* are represented in TABLE 13.

F. PHYSICAL ATTACKS

IoT devices situate as scattered in the network. These devices can be accessed physically if there are no physical securities. Moreover, there can be thousands of IoT devices; therefore, it is not possible to protect them from *physical attacks*. However, *physical attacks* are not only held on static devices, which can be easily tracked, but also in mobile devices, which are difficult to trace. *Physical attacks* can be occurred by *mobile devices loss attack, stolen card attack, stolen device attack, USB attack same-type-device attack. Additionally,*TABLE 14 illustrates the description of all possible physical attacks on IoT authentication.

To illustrate, mobile devices are the backbone of any IoT network. During authentication, the user often uses mobile devices instead of static devices. However, to get access to the network, they have to pass through any sensor that is connected to the GWN or any authentication server. Now if a device of any legal user is lost and grab by an attacker, they can guess or retrieve the data from the mobile device, which is a way to open the door for attackers to the network. To resist that type of attacks, authentication researchers developed protocols. Likewise, Li *et al.* [33] proposed a robust authentication protocol for IIoT that can prevent *mobile device loss attack*. Consecutively, Li *et al.* [31] presented an authentication protocol with privacy-preserving for IoT. However, many authentication protocols use the smart card (SC) to tighten the security in the IoT network. Nevertheless, the *stolen card attack* makes those protocols weak.

On the other hand, in the *stolen card attack*, an adversary steals the smart card, which is authenticated in the network, from a genuine user, extracts information from the card and makes a copy of those. Similarly, Intruder can perform *power analysis attacks* to get information from a smartcard [98]. Wu *et al.* [28] and Li *et al.* [31] designed authentication protocol, which can efficiently protect *stolen card attacks*.

Unlike the stolen card, a stolen device is also a possibility. In this situation, an adversary may use the same technique to retrieve the data from the stolen device and can duplicate the device, also can predict the network authentication pattern.

TABLE 15. IoT authentication protocols to protect against physical attacks.

Physical attacks Protocols	Mobile Device Loss Attack	Stolen Card Attack	Stolen Device Attack	USB Attack	Same-type-device Attack
Wu, et al. [28]	No	Yes	No	No	No
Li, et al. [31]	Yes	Yes	No	No	No
Li, et al. [33]	Yes	No	No	No	No
Chen, et al. [84]	No	No	No	No	Yes
Nissim, et al. [99]	No	No	No	Yes	No
Lin, et al. [100]	No	Yes	Yes	No	No

TABLE 16. Description of different types of routing attacks.

Routing Attacks	Description
Sinkhole Attack	In this attack, an adversary node acts as a sink node in the IoT network, so that it can capture all traffic from this particular network.
Wormhole Attack	In this attack, an attacker node creates a false route for the packets to traverse and misleads the distance between nodes.
Black hole attack	In this attack, an attacker node sends a route reply message to the sender and captures the messages without forwarding them.
Link-ability attack	In this attack, an adversary finds the link between transmitted data in a different session and plans hazardous activities.

Furthermore, an innocent computer user may not know the severity of USB devices in their system. On which, USB peripherals can carry malicious script to steal information or take advantage of the system. USB attacks have various ways to gain access to the architecture as discussed well by Nissim *et al.* [99], such as a keyboard, flash drive, mouse, and data cable. In contrast, a mobile device transmits data to the receiver during authentication. However, protocols may not be designed to authenticate the sender device identity, which can provoke the *same-type-device attack*. An attacker can acquire a device, which is the same as the same manufacturer and same brand as of the legitimate transmitter, and he/ she pretends the transmitter by sending the same signal as the real transmitter. A lightweight acoustic fingerprint-based wireless device authentication protocol is designed by Chen *et al.* [84] to protect the network from the *same-type-device attack*. TABLE 15 lists the existing IoT authentication protocols supports against physical attacks.

G. ROUTING ATTACK

Non-legitimate node forwards data packets to the improper destination, which is known as *routing attack*. Classification of routing attacks is shown in FIGURE 3, and the description of all possible routing attacks are listed in TABLE 16. This type of attack approaches in two different ways either via changing the final destination address of the data packet or via sending the data packet to the wrong next hop in the routing path. In 2017, Ma *et al.* [101] proposed an M-RPL protocol to protect lightweight IPv6 routing protocol by creating hierarchical clustering network topology and providing alter path from different clusters to a route if the network is compromised.

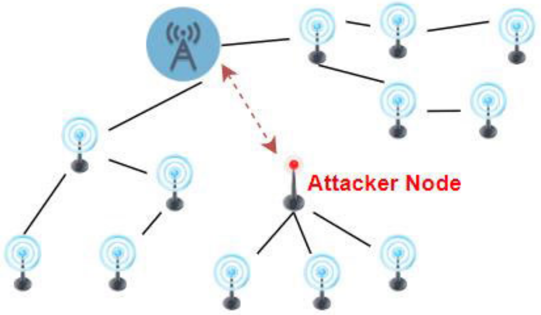

FIGURE 11. Sinkhole attack.

In the *routing attack*, a *sinkhole attack* is a type of selective forwarding attack [102]. In a wireless sensor network, all the data collected by the sensor nodes are forwarded to the sink node to process, therefore, the sink node is very important for the lifetime of the WSN. However, an adversary node can act as a sink node and tamper all the data in a WSN, which makes the network in jeopardy. This node can be as dangerous as attract neighboring nodes. Moreover, in the *sinkhole attack*, the attacker node convinces the neighboring nodes to get the traffic from them and then digest all packets. *Sinkhole attack* can open the path for *wormhole attack*. *Sinkhole attack* is illustrated in FIGURE 11. Similarly, a *wormhole attack* is considered as a serious attack in a wireless sensor network. There are two major components in the *wormhole attack*, i.e. several spiteful nodes and tunnels. In addition, the wormhole node creates a false route, which is shorter than the original route in an IoT network and misleads the distance between nodes i.e. routing mechanism.

TABLE 17. IoT authentication protocols to protect against routing attacks.

Routing attacks Protocols	Sinkhole Attack	Wormhole attack	Black hole attack	Link-ability attack
Malina, et al. [46]	Yes	No	No	No
Ferrag and Ahmim [62]	No	Yes	No	No
Ma, et al. [101]	No	Yes	Yes	No
Amish and Vaghela [103]	Yes	Yes	No	No
Bansal, et al. [104]	Yes	No	Yes	No
Kaur and Singh [105]	No	No	Yes	No
Memon, et al. [106]	No	No	No	Yes

Then, the malicious node occupies the packets from one location and transfers them to the distant situated node by a tunnel (either by in-band or out-band channel) which further distributed locally. However, attackers can perform *wormhole attack* without informing any authenticated nodes or mechanism. Furthermore, the *wormhole attack* launches various other attacks like *selective dropping, eavesdropping, and replay attacks*, which affect data traffic flow. Amish and Vaghela [103] introduced *wormhole attack* detection and prevention mechanism in WSN using Ad hoc on-demand Multipath Distance Vector (AOMDV) routing protocol. *Wormhole attack* is shown in FIGURE 12.

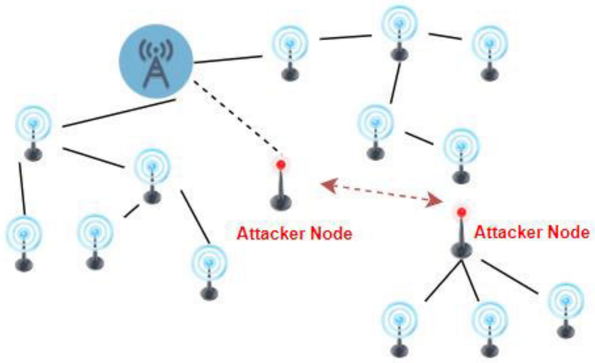

FIGURE 12. Wormhole attack.

On the other hand, in the *Black hole attack*, malicious nodes send a route reply message to the sender in return receive packets from sender node and discard packets instead of forwarding to the destination node. In their research, Motamedi *et al.* [107] show the detection procedure of *Black hole attack* in WSN using unmanned aerial vehicles (UAVs). Furthermore, Bansal *et al.* [104] discussed the anomaly-based detection on leach protocol in WSN and Kaur and Singh [105] presented a way to identify and mitigate the *Black hole attack* in WSN. Nevertheless, various data establish links with the original content of a transmitted data over IoT network. For example, clouds may contain user details and time of purchase of a particular good in a departmental store or can be data of patients associated with his/ her disease information. Therefore, an adversary can attack a network to reduce linked information from a session of transaction. This is called the *link-ability attack.* To prevent *link-ability attack* in a vehicular network, Memon *et al.* [106] introduces pseudonyms changing strategies. Additionally, TABLE 17 shows existing IoT authentication protocols fight against routing protocols.

III. TECHNICAL METHODS OF AUTHENTICATION MECHANISM IN IoT

As authentication is a process of validating users and components identity, so that the authorization process can provide access to the network or an information system, which should be highly secured from vulnerable threats. Therefore, thousands of authentication protocols are designed by the researchers to protect the IoT network from illegal users. However, designing and protection mechanism of authentications are different in different protocols. On the other hand, authentication protocols in IoT cannot cope up with the traditional authentication mechanism because of its limitations. As a result, IoT authentication schemes use *password-based authentication, token-based authentication, biometric authentication, cryptographic authentication, and multi-factor authentication.* Additionally, FIGURE 13 shows the well-structured taxonomy of technical methods of an authentication mechanism in IoT.

Password-based authentication is a very common and useful method to verify a user or device. In which, users need to provide a unique id and a word combing of letters, digits and/ or special characters, known as a *password*. The unique id and password combination are reserved in the database in an authentication server or as low level as in sensors' memory. When a user supplies the combination of user id and password, protocol matches the provided combination with saved credentials and if these matches then, the protocol allows the expected user or device to perform the desired action. A password can be a combination of different patterns or simple words. However, protocols use strong rules for a

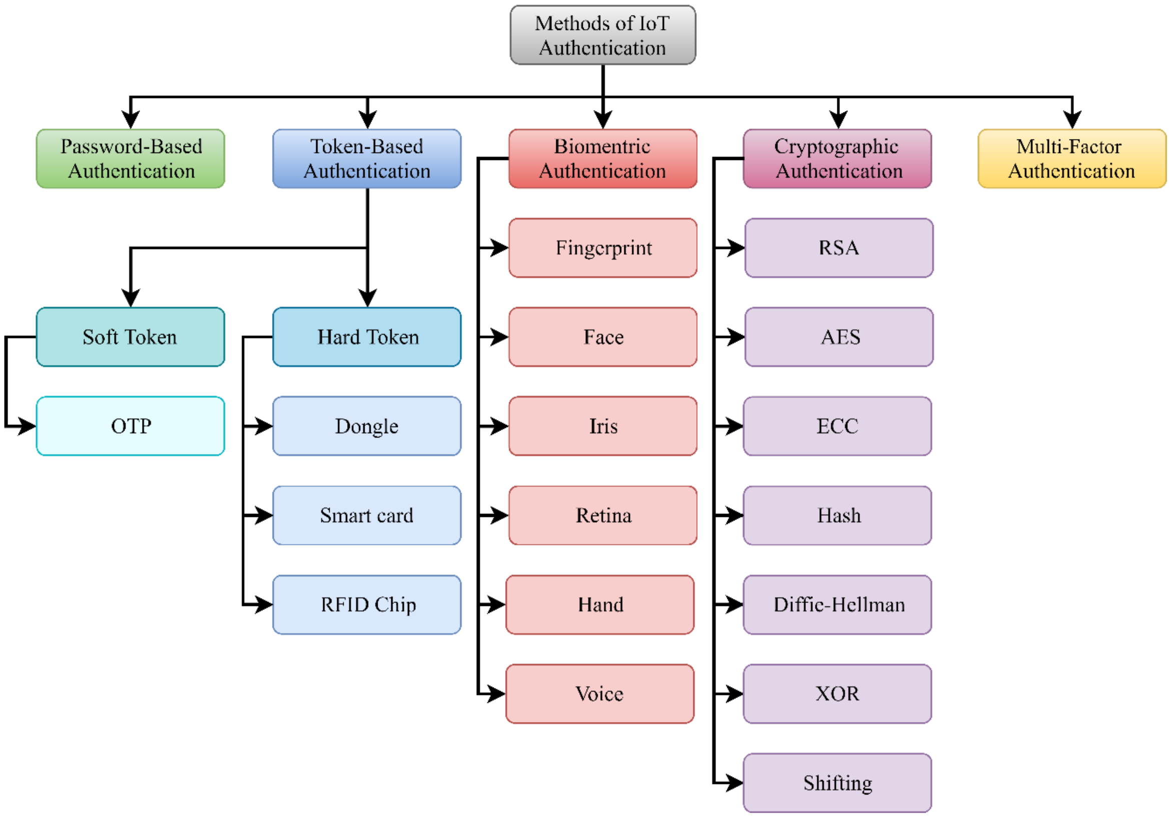
Methods of IoT Authentication
Password-Based Authentication
Token-Based Authentication
Biomentric Authentication
Cryptographic Authentication
Multi-Factor Authentication
Soft Token
OTP
Hard Token
Dongle
Smart card
RFID Chip
Fingerprint
Face
Iris
Retina
Hand
Voice
RSA
AES
ECC
Hash
Diffie-Hellman
XOR
Shifting

FIGURE 13. Technical methods of the authentication mechanism in IoT.

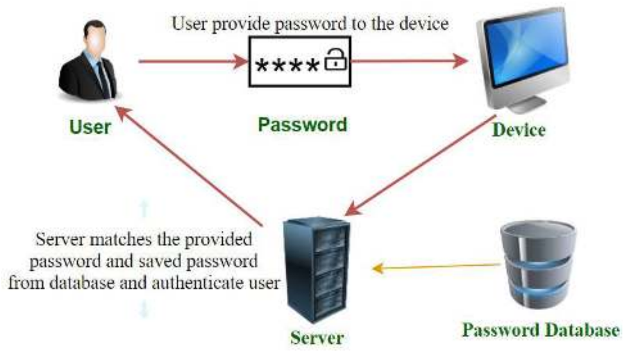
User provide password to the device
User
Password
Device
Server matches the provided password and saved password from database and authenticate user
Server
Password Database

FIGURE 14. Password authentication process.

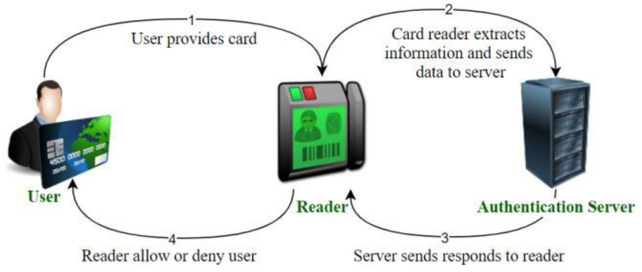
1
User provides card
2
Card reader extracts information and sends data to server
User
Reader
Authentication Server
4
Reader allow or deny user
3
Server sends responds to reader

FIGURE 15. Smartcard authentication process.

password to avoid the password guessing attack. In addition, FIGURE 14 shows the password authentication process.

Nevertheless, a token is a piece of data created by the authentication server to uniquely identify a user or device. *Token-based authentication* [43] can be further classified as *soft and hard token-based authentication*. In a *soft token-based authentication* scenario, the server populates a one-time password (OTP) and sends it to the registered communication media, which is associated with the account and preserves a copy of the transferred OTP. After a while, the server matches the user-provided OTP with the stored one and takes decision on authentication. Furthermore, to make the process more secure, protocols implement associative rules like the expiration of OTP, length of OTP and type of OTP. On the other hand, a small device or card containing a piece of information to verify itself in a tokenization system is called *hard token-based authentication*. Additionally, this system works on a mechanism where every request to a server will response based on the correct combination of tokens. Furthermore, *token-based authentication* is well-accepted methods because of its easiness of transmission via query strings, header attributes and the body of a POST request. Moreover, hard token authentication can be achieved using different methods like dongle [90], smart card [34] and RFID chip [29]. Additionally, the process of authentication via smart card has been shown in FIGURE 15.

On the other hand, *biometric authentication* [30], [32], [34], [40], [42], [68] is based on the biological character of humans. Additionally, the specific biometric scanner collects unique biological data from a user and matches the stored data, which was collected via the registration process. Moreover, biometric uniqueness can be provided in different ways. These methods include *fingerprint authentication, face authentication, iris authentication, retina authentication, hand authentication, and voice authentication. Iris authentication* methods use mathematical pattern recognition to identify the pattern of one or both the irises, which is unique for an individual. Likewise, fingerprint authentication is common in IoT mechanism, where friction ridges of a human finger are checked with pre-reserved of the same information in a server. Similarly, other biometric authentication uses its unique feature to differentiate individuals. FIGURE 16 illustrates the biometric authentication process.

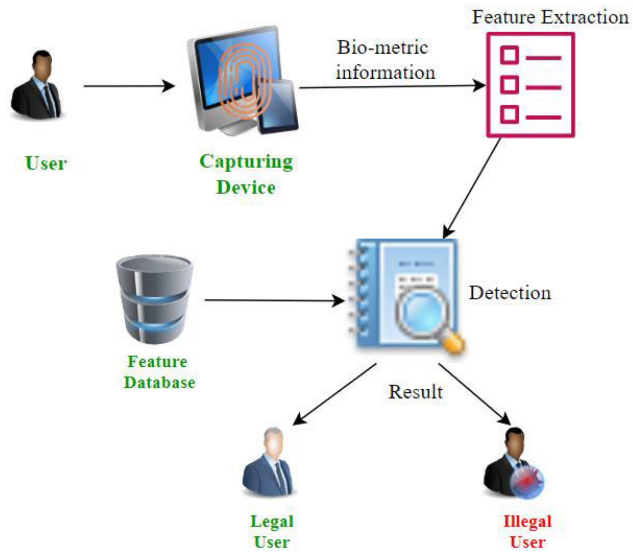

FIGURE 16. Biometric authentication process.

In contrast, cryptographic authentication methods use to encrypt and decrypt techniques to morph actual messages during communication in an insecure network. Additionally, not only to protect variable data in the algorithm but also researchers apply cryptography to protect peripheral authentication values like biometric information, token, password, user id, smart card information during the process of authentication. Furthermore, it is a common practice to use hash and XOR techniques [24], [29], [30], [32], [35], [40] in authentication because IoT devices are tiny and computational-constrained. On the other hand, Fouda *et al.* [108] use Diffie-Hellman along with Hash-based Message Authentication Code (HMAC) technique. In contrast, Mahmood *et al.* [66] criticize Fouda *et al.* [108] protocol and reuse the Diffie-Hellman technique to their authentication protocol and implement RSA and AES algorithm to generate the session key. On the other hand, because of strong cryptanalysis and constant breaking strategies of the lightweight cryptographic algorithm, developers incorporate rate *elliptic curve cryptography (ECC)* [31], [41], [69], [71], which is popular and provided a strong mechanism in IoT authentication, especially in key agreement mechanism. Similarly, developers use techniques like bio hashing [40], fuzzy bit commitment [32] to protect biometric information during authentication.

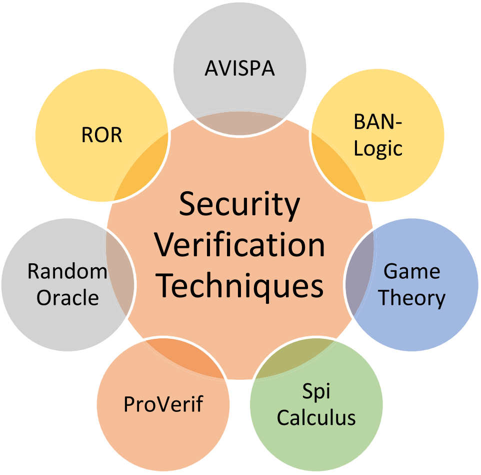

FIGURE 17. Security Verification Techniques.

Alternatively, because of multi-factor authentication's versatility, it gets the most attraction to researchers to make authentication protocol secure and strong. To elaborate, multi-factor authentication consists of two or more ways to identify an independent identity. It may include any combination of password-based authentication, biometric authentication, cryptography authentication or token-based authentication. For example, Srinivas *et al.* [40], Kang *et al.* [30] and Li *et al.* [32] use hash, XOR and biometric together in their protocol. Similarly, Hossain and Hasan [109], Wu, et al. [69] and Li *et al.* [31] employ hash, XOR and ECC. Likewise, all modern protocols apply two or more technical methods to produce effective authentication protocol.

The proliferation pace and diversity of IoT devices in the network make the authentication mechanism more demanding. To address this situation, several methods have introduced in the IoT authentication mechanism. Furthermore, researchers are developing authentication protocols to make more powerful by combining inter-domain techniques. To illustrate further, TABLE 18 lists the technical methods used by current IoT authentication protocols including outcomes.

IV. SECURITY VERIFICATION TECHNIQUES IN IoT AUTHENTICATION

Researchers use security verification techniques to test the performance of an authentication technique in IoT. There are few security verification techniques available for performance testing, which is shown in FIGURE 17,

TABLE 18. Different technical methods used by authentication protocols in IoT.

Protocol	Method	Strengths	Weakness
Amin, et al. [17]	Smartcard	This paper describes the distributed cloud architecture, in which, the private cloud stores the confidential data collected by IoT and designs an authentication protocol.	The protocol is weak to provide user untraceability, forward secrecy and withstands against password guessing attacks.
Jiang, et al. [18]	ECC	This protocol shows a strong foundation against common attacks in IoT authentications.	The protocol is incapable to identify the wrong password login and faces difficulties during the password change phase.
Wallrabenstein [19]	ECC	This paper describes how the physical unclonable functions based authentication protocol can be used in IoT because of the ECC makes the protocol light and PUFs secure against tamper resistance.	The protocol may face excessive computational and resource overhead during wifi communication. Moreover, the protocol is vulnerable to wifi authentication.
Saxena, et al. [23]	Cryptography	This paper describes the weaknesses of the packet system-based authentication mechanism and key agreement protocols of LTE.	The anonymity of the user may not be protected by only symmetric key techniques in IoT authentication.
Chang and Le [24]	Hash and XOR	This paper provides perfect forward secrecy and protects from impersonation attack with node capture, stolen smart card attack, sensor node spoofing attack, stolen verifier attack	The protocol is sensitive to session-specific temporary information attack and password guessing attacks.
Dolev, et al. [25]	Cryptography	This paper uses a strong mechanism to protect against Man-in-the-Middle (MitM) attack and provide mutual authentication.	The protocol is not suited against the cloning attack like license number cloning.
Farash, et al. [26]	Password, Token	This paper presents an excellent result on traceability and anonymity. Moreover, the protocol shows the password protection mechanism.	The protocol is vulnerable against a user-impersonation attack, an off-line password-guessing attack using a stolen-smartcard, session-specific temporary information attack, and a new-smartcard-issue attack.
Banerjee, et al. [27]	Password, Smartcard, Biometric	The scheme supports to change password freely and also dynamic node addition. Additionally, the protocol resists against, stolen smart card attack, stolen verifier attack, GWN bypassing attack, DOS attack, smart card breach attack, and replay attacks.	The registration phase is assumed to happen under a secure communication channel, but in the IoT scenario, deploying a sensor or registering a user may not always possible under a secure channel.
Gope, et al. [29]	Hash, XOR and RFID	This paper presents an RFID based autonomous authentication protocol, which gives security against replay attack, location-tracking attack, forgery attack, cloning attack, DoS attack.	As the backend server of this protocol is so powerful, any forgery attack can be performed if an adversary gets access to the server. Moreover, the scheme is insecure against physical attack also.
Li, et al. [31]	Hash, XOR and ECC	This paper discusses the security in IIoT and proposes a robust authentication protocol using ECC for securing the IIoT environment. Additionally, the protocol protects against various attacks and confirms privacy protection.	Users need to input the password manually in the protocol so it may rely on complex computation, needs user interference and vulnerable for the physical attack as the information is saved and stored.
Li, et al. [32]	Hash, XOR and biometric	This paper investigates security flaws on two factors based on authentication protocol and proposes a biometric-based authentication protocol to provide security from well-known attacks. Additionally, the protocol claims to quickly detect unauthorized login and can perform password change freely.	The protocol has significant issues on smart card attack, anonymity, and traceability.
Roy, et al. [34]	Smartcard, password and biometrics	This paper avoids using computationally expensive ECC multiplication or modular exponential operation. Despite using expensive operation, the protocol uses simple and effective techniques like smartcard, passwords, and biometrics for authentication.	Li, et al. [33] suggested that the computational complexity of the protocol is not appropriate for IoT.

TABLE 18. ***(Continued.)*** **Different technical methods used by authentication protocols in IoT.**

Protocol	Method	Strengths	Weakness
Challa, et al. [38]	ECC, Biometric	This paper provides authentication in the key establishment phase.	The protocol is vulnerable to a side-channel attack. The physical implementation of the key establishment protocol can be leaked by some sent messages in the authentication and key agreement phase. Though the protocol provides authentication, it faces high computational and communication costs.
Jiang, et al. [39]	Biometric, cryptography	This paper investigates Amin, et al. [36] protocol and provides a secure three-factor authentication scheme, which can protect from known current threats, using Robin cryptosystem.	The protocol, however, can not promise the security of the secret key of the gateway node and the session key. Moreover, protection against user tracking attacks, information leakage attacks, and user impersonation attacks are not guaranteed in this protocol.
Srinivas, et al. [40]	Hash, XOR and biometric	This paper proposes an authentication protocol using biometrics to protect from various attacks like impersonation attack, guessing attack, password guessing attack, stolen smart card attack, and identity server spoofing attack,.	Protocols need to be tested in the testbed and evaluated in a real-world environment. Moreover, because of non-public key primitives, protocol faces a lack of dynamic identity mechanism to apply in the WSN environment.
Shen, et al. [41]	ECC	This paper presents two layers of communication and one-to-many certificate less authentication using ECC.	The protocol works in a static situation. Therefore, the mobile user can be tested and over the network using the protocol.
Punithavathi, et al. [42]	Biometric	This paper proposes a Cloud-based lightweight cancelable biometric system for IoT applications.	The scalability of the protocol has not been tested over real-world situations.
Dammak, et al. [43]	Token	This paper presents perfect forward secrecy and token security through the proposed token-based authentication protocol.	Security verification needs to be verified using formal verification tools like the AVISPA tool.
Mahmood, et al. [66]	Diffie–Hellman, AES and RSA	This paper overcomes the Hash-based Message Authentication Code (HMAC) techniques' problem. Moreover, this protocol claimed to reduce 23% communication cost and 33% computational cost compared to Fouda, et al. [108].	The protocol has several security weaknesses like session key agreement, impersonation attack, and user anonymity,
Griffin [68]	Biometric, cryptography	This paper uses a Biometric Authenticated Key Exchange (BAKE) protocol and supports universal access, in which the user can authenticate himself/ herself using a variety of possibilities.	The password is set as per gesture of the hand of the user, which makes critical to remember and takes a long time to produce the password.
Wu, et al. [69]	Hash, XOR, smartcard and ECC	This paper uses a password, hash smartcard, and ECC. Additionally, the protocol shows the password change mechanism of the smartcard.	The protocol phase problem at the password change phase and also vulnerable to impersonation attacks.
Sciancalepore, et al. [71]	ECC	This paper proposes a key management protocol by using the elliptic curve Qu-Vanstone implicit certificate and elliptic curve Diffie-Hellman exchange.	The protocol experiences high communication delays while the size of the certificate chain increases.
Salman, et al. [82]	Password, cryptography	The SDN controller authenticates different devices and gateway based on shared identity on the virtual IpV6 address.	An attacker can sniff the IP address used in the protocol, lead to the weakness of it.
Liang, et al. [90]	Tags	This paper proposes attribute-oriented authentication and transmission scheme in Health Social Network (HSN) to achieve secure and privacy-preserving health information sharing techniques.	The protocol has not considered the social environment where social behavior and social requirements are different for different HSN users.
Fouda, et al. [108]	Hash, Diffie–Hellman	This paper uses Diffie-Hellman and Hash-based Message Authentication Code (HMAC) techniques, compares with the Elliptic Curve Digital Signature Algorithm (ECDSA) and shows better results.	The scheme needs to examine other challenging issues. Furthermore, denial of service attacks in the smart grid environment is not considered.
Hossain and Hasan [109]	Hash, XOR and ECC	This paper uses the BooT-IoT scheme, which produces new identification to a device while joining a network.	The public key matrix may not be safe in the device identity provider in the protocol.
Tewari and Gupta [110]	XOR and RFID	This paper proposes an ultra-lightweight authentication protocol using only XOR and RFID and claims to protect from a different attack like a DDOS attack, replay attack, and tracking attack.	The protocol is not checked against denial of service attacks at both the tag and reader side.

TABLE 19. Security verification techniques used by IoT authentication protocols.

Security verification Techniques Protocols	AVISPA	BAN	Game Theory	Spi Calculas	ProVerif	ROM	ROR	Description
Tu, et al. [16]	No	No	Yes	No	No	No	No	This paper investigates on physical layer security and to detect impersonation attack in fog computing.
Amin, et al. [17]	Yes	Yes	No	No	No	No	No	The paper first shows the problems on Xue, et al. [117] and Chuang and Chen [118]. After that, an authentication mechanism using a smartcard has been proposed.
Jiang, et al. [18]	No	Yes	No	No	Yes	No	No	This paper discusses the loopholes on He, et al. [119] protocol and proposes untraceable two-factor authentication using ECC.
Wallrabenstein [19]	No	No	Yes	No	No	No	No	This paper implements a physical unclonable function based authentication protocol using ECC.
Saxena, et al. [23]	No	No	Yes	No	No	Yes	No	This paper proposes an authentication and key agreement protocol for IoT enabled LTE network. This paper also proves that it reduces bandwidth consumption during authentication.
Dolev, et al. [25]	No	No	No	Yes	No	No	No	This paper proposes vehicular authentication using public key infrastructure.
Farash, et al. [26]	Yes	Yes	No	No	No	No	No	This paper discusses the problem on Turkanović, et al. [120] protocol and comes with improved user authentication and key agreement scheme.
Wu, et al. [28]	No	No	No	No	Yes	No	No	This paper proposes a password and user id based strong authentication scheme for multi gateway scheme and outperforms Amin and Biswas [121] and Turkanović, et al. [120]
Gope, et al. [29]	Yes	No	No	No	No	No	No	This paper proposes a lightweight RFID based authentication protocol for IoT.
Kang, et al. [30]	Yes	Yes	No	No	No	No	No	This paper presents four different types of problems of Kaul and Awasthi [122]proposal and proposes a biometric-based authentication protocol with a key agreement scheme with anonymity.
Li, et al. [31]	No	No	Yes	No	No	Yes	No	This paper proposes a user authentication protocol scheme including privacy protection in IIoT.
Li, et al. [32]	No	Yes	No	No	No	No	No	This paper proposes a three-factor anonymous authentication technique and uses a fuzzy commitment scheme to preserve users' biometric information.
Roy, et al. [34]	No	Yes	Yes	No	Yes	Yes	Yes	This paper proposes an authentication protocol based on the chaotic map using the smartcard, password, and biometrics.
Amin, et al. [36]	Yes	No	No	No	No	No	No	This paper investigates security features on Farash, et al. [26] protocol and designs anonymity preserving three-factor authentication scheme, which outperforms Farash, et al. [26] scheme by identity change and smartcard revocation.
Yeh [37]	No	Yes	Yes	No	No	No	No	This paper proposes an IoT based healthcare system on on-body sensor networks.
Challa, et al. [38]	Yes	Yes	No	No	No	No	No	This paper proposes a signature-based authenticated key establishment scheme for the IoT environment.
Srinivas, et al. [40]	Yes	Yes	No	No	No	No	No	This paper proposes an authentication scheme for multi-gateway wireless sensor networks using biometrics and biohashing.
Dammak, et al. [43]	Yes	No	No	No	No	No	No	This paper proposes token-based user authentication.
Mahmood, et al. [66]	No	No	No	No	Yes	No	No	This paper proposes a hybrid Diffie–Hellman based lightweight authentication scheme using AES and RSA for session key generation.

TABLE 19. ***(Continued.)*** **Security verification techniques used by IoT authentication protocols.**

Security verification Techniques **Protocols**	**AVISPA**	**BAN**	**Game Theorv**	**Spi Calculas**	**Pro-Verif**	**ROM**	**ROR**	**Description**
Wu, et al. [69]	No	No	No	No	Yes	Yes	No	This protocol criticizes Hsieh and Leu [123] protocol and proposes an improved authentication technique.
Salman, et al. [82]	Yes	No	No	No	No	No	No	This paper proposes an identity-based authentication scheme.
Amin and Biswas [121]	Yes	Yes	No	No	No	No	No	This paper criticizes Turkanović, et al. [120] protocol and proposes an improved user authentication and key agreement scheme in multi-gateway based wireless sensor networks.

namely, Automated Validation of Internet Security Protocols and Application (AVISPA), BAN-logic, Game Theory, Analysis by process (Spi calculus), Automated reasoning (ProVerif),Random Oracle Model (ROM), and Real-or-Random (ROR). Furthermore, TABLE 19 illustrates the security verification techniques used by recent IoT authentication protocols.

A. AUTOMATED VALIDATION OF INTERNET SECURITY PROTOCOLS AND APPLICATION (AVISPA)

AVISPA is an automated validation and security analysis tool for network and cryptographic protocol. A number of IoT authentication researchers use AVISPA tools to confirm security attributes. Farash *et al.* [26] proposed user authentication and key agreement scheme and used AVISPA to confirm security properties. Furthermore, Amin *et al.* [17] used AVISPA to ensure the safety mechanism of their proposed protocol. AVISPA is available from Information Society Technology [111].

B. BAN-LOGIC

Authentication protocols are important to be examined properly if their working principles are logically correct because authentication protocols are the backbone of security in many IoT networks. To fulfill this requirement, Burrows *et al.* [112] proposed BAN logic, which ensures if the exchanging information over media is trustworthy or not. Furthermore, BAN logic follows a sequence of three steps, and these are (I) verification of message origin, (II) verification of message freshness and (III) verification of message trustworthiness. Amin *et al.* [17], Farash *et al.* [26], Li *et al.* [32], and Jiang *et al.* [18] used BAN to logically proof the authentication on their proposed work. He, et al. [113] used BAN logic to show if the proposed scheme is valid and practical. Kang *et al.* [30] used the BAN to validate the generated session key between user and server.

C. GAME THEORY

Game theory is the strategic interaction between rational decision-makers. It has been widely used in IoT component authentication to sanguine security. Chang and Le [24] uses a sequence of games under the decisional Diffie-Hellman (ECDDH) problem with a view to proving that the protocol supplies secure and perfect forward secrecy authentication by Ferrag *et al.* [67].

D. SPI CALCULUS

Spi calculus is an extension of pi-calculus developed for describing and analyzing cryptographic protocols [114]. A detailed discussion about Spi calculus has been done by Abadi and Gordon [114]. The authenticity property and the secrecy property has been proved via the session key establishment protocol by Dolev, et al. [25].

E. PROVERIF

Blanchet *et al.* [115] developed the Proverif tool, which is for automated reasoning about the security properties found in cryptographic protocols. Wu *et al.* [69] use Proverif to list the formal verification process in their protocol. Roy, et al. [34] uses the formal security verifier proverif1.93 to show the security of the presented scheme.

F. RANDOM ORACLE

Random oracle is a random function, which response to every unique query with a random response chosen uniformly from its output domain. It is a mathematical function and always choose the fixed random response from its output domain for each repeated unique query. Random oracle can be represented using equation 1.

$$\boldsymbol{D \rightarrow R} \tag{1}$$

Let, D is a domain and R is a range. Therefore, Random Oracle is a randomly chosen function such that among all functions in domain D and range R are chosen randomly. As it is a function, every time if the same input is given to the Random oracle, the same output needs to be returned. The way to think about the random oracle is that it can be considered as a lookup table like FIGURE 19. Such that, one column represents the input and another one represents output, so for each input, a randomly chosen output will be stored in the table. Whenever random oracle needs to compute over some input x, then from the table it can return correspond y

Algorithm 1 Random Oracle

```
Initialize database DB
input ← x
if (x, y) exists in DB then
    return y
else
    Choose y from range R
    Add (x,y) pair in DB
    return y
end if
```

value using equation 2. Furthermore, algorithm 1 represents the random oracle.

$$y = \boldsymbol{RO}(\boldsymbol{x}) \tag{2}$$

where $\boldsymbol{RO}(.)$ is Random Oracle function, and $\boldsymbol{x}, \boldsymbol{y}$ are input and output respectively. This would have been an ideal random oracle, but representing such a table requires exponential space. If the domain $\boldsymbol{D}$ is an n bit value, then there will be 2n rows in FIGURE 19. Instead of this, the random oracle can be simulated using it in a randomized way.

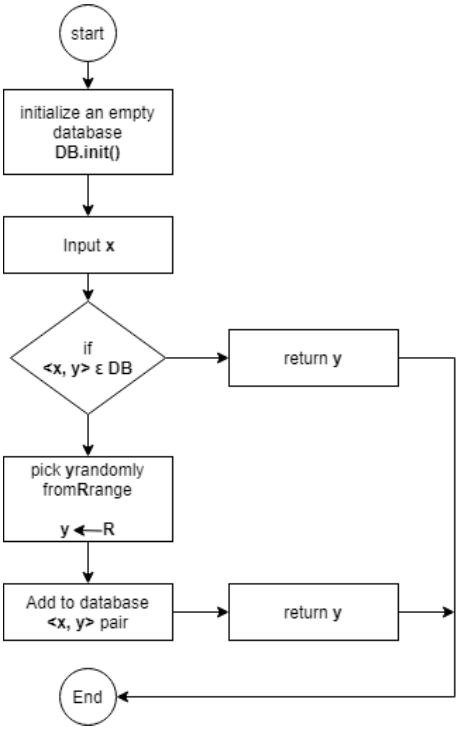
start
initialize an empty database DB.init()
Input x
if <x, y> ε DB
return y
pick yrandomly fromRrange y ← R
Add to database <x, y> pair
return y
End

FIGURE 18. Random oracle flowchart.

On the other hand, random oracle simulation can be represented as a flowchart like FIGURE 18. Random oracle representation of FIGURE 19 requires exponential space, whereas, random oracle representation of FIGURE 18 needs polynomial space. Therefore, the advantage of the random oracle representation of FIGURE 18 over FIGURE 19 is based on the space requirement.

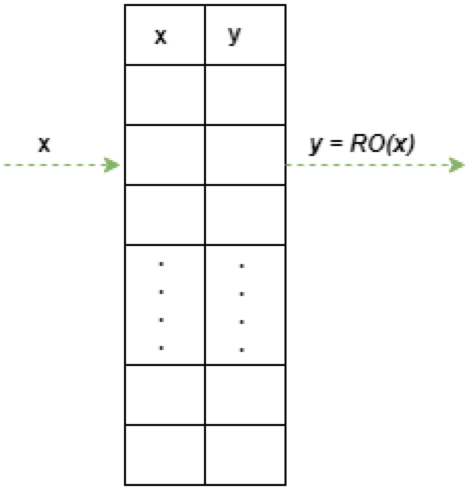

FIGURE 19. Random Oracle representation.

G. REAL-OR-RANDOM MODEL (ROR)

ROR is the two-party authentication key exchange protocol. In this model, an adversary can ask Execute, Send and Test queries. Furthermore, the adversary can ask as many as Test queries to differentiate instances. However, all the Test queries will be answered using the hidden bit, which is the same for all instances and chosen at the beginning. That means the keys returns by the Test oracle are all real or random. Moreover, the same random value will be returned for Test queries from two collaborated instances. However, the motivation of the adversary is to guess the random bit to answer the Test queries and they succeed, if they guess correctly. The Real-or-random model by Abdalla, et al. [116] is widely used to process formal security analysis in the research.

TABLE 19 represents the security verification techniques in IoT authentication protocols, where ten protocols [17], [26], [29], [30], [36], [38], [40], [43], [82], [121] have used AVISPA and ten protocols [17], [18], [26], [30], [32], [34], [37], [38], [40], [121] have used BAN-logic to establish verification of techniques used in the protocols compare to other techniques. Furthermore, only one protocol [25] uses spi calculus and two protocols [24], [34] use ROR techniques. On the other hand, five protocols [23], [24], [31], [34], [69] use ROM, five protocols [18], [28], [34], [66], [69] use ProVerif and seven protocols [16], [19], [23], [24], [31], [34], [37] use Game theory.

From the observation, it is identified that recent protocols prefer BAN-logic and AVISPA for security verification. The main strength of BAN-logic is its simplicity and its usefulness. Therefore, the authors trust this technique more. Moreover, the formulation of BAN is easy to cope up with the authentication protocols and the structure of it is more convenient for this type of verification. On the other hand, AVISPA is also a popular tool among researchers. AVISPA shows the result and analysis of the protocols in detail and in a fruitful manner, which attracts researchers to choose AVISPA to test their scheme. In contrast, ROM, ProVerif and Game Theory have moderate use to verify authentication techniques compare to ROR and Spi Calculus.

V. IoT AUTHENTICATION EVALUATION TECHNIQUES

As the new and challenging authentication techniques are necessary to protect the IoT environment from various emerging attacks, evaluation of those proposed schemes are equally important to check their effectiveness. In this section, we discuss several evaluation techniques with their parameters and supporting equations.

A. AVERAGE RESPONSE TIME

Response time is assumed to be the time taken by the server or GWN to result in the response of a request to the client. This can be affected by few factors, such as server configuration, number of users, network bandwidth, number of request, type of requests and think time.

First response time can be executed by the time of client request and time of first response, which is described in equation 3.

$$T_{res} = t_{res} - t_{req} \tag{3}$$

Here $T_{res}, t_{res}, t_{req}$ are response time, time of client request and time of first response respectively.

Average response time is calculated by the mean of all response time, which is demonstrated in equation 4.

$$T_{ang\_res} = \frac{n}{r} - T_{think} \tag{4}$$

where T_{ang_res} is the average response time, n is the number of concurrent users. r is the number of requests per second the server receives. T_{think} is the average think time (in seconds). However, to obtain an accurate response time result, a user should always include think time in the equation.

B. HANDSHAKE DURATION

Handshaking is the process of negotiation between two network parties in the IoT network. These parties can be user, sensor, actuator, server or other nodes. As shown in FIGURE 20, handshaking takes place by completing the two-roundtrip message, whereas, client's discovery offers by the server and again the client's request acknowledges by the server.

Duration to a handshake T_{hs} is computed at the client-end using equation 5.

$$T_{hs} = T_s + T_{res} + T_p \tag{5}$$

where T_s is the time taken by whole session request, T_{res} is client response time and T_p denotes as processing time at the server.

However, to calculate the handshake duration, a user must perform several random numbers of handshakes between the client and the server. After that, the user should perform a standard deviation to observe the variability and accuracy among the examined data. Standard deviation can be performed using equation 6.

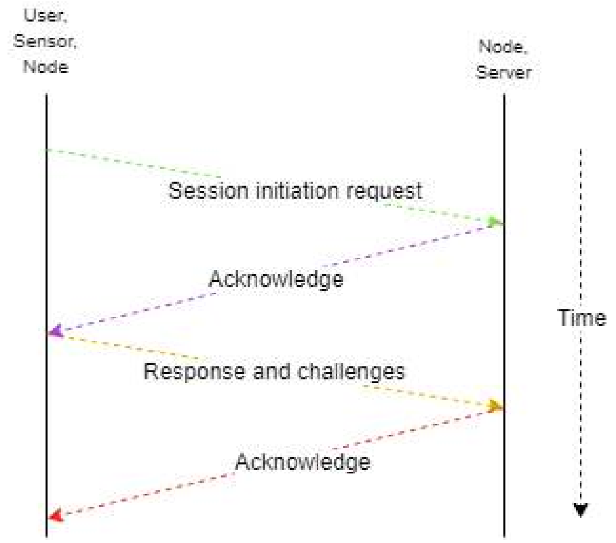

FIGURE 20. Handshaking.

$$\sigma = \sqrt{\frac{1}{N}\sum_{i=1}^{N}(x_i - \mu)^2} \tag{6}$$

where σ denotes standard deviation. N is the number of samples, i is the number of iteration, x_i is the handshake duration and μ is mean value.

C. AVERAGE MEMORY CONSUMPTION

IoT is a mostly wireless sensor network, which is constrained by its low memory. Consequently, memory consumption is important in specialized and autonomous sensor networks. However, memory consumption depends on the various level in IoT, such as user level, sensor level, GWN level or server level. A comparison of memory consumption in various authentication protocols is discussed in TABLE 20.

TABLE 20. Comparison of average memory consumption.

Protocols	Memory cost
Kang, et al. [30]	768 bytes
An [124]	896 bytes
Chou, et al. [125]	1080 bytes
Chang, et al. [126]	768 bytes
Kumari, et al. [127]	896 bytes
Kaul and Awasthi [122]	768 bytes

D. END-TO-END DELAY

End-to-End Delay or E2ED denotes the average time to deliver packets from sender to receiver. E2ED can be calculated by using equation 7.

$$\boldsymbol{E2ED} = \frac{\sum_{k=1}^{n}\left(T_i^r - T_i^s\right)}{n} \tag{7}$$

Here, i is the number of packets and n is the number of received packets, while T_i^r is the received and T_i^s denotes the sent timestamp for ith packet. E2ED is proportional to the number of sensors in the IoT network. Therefore, an increased number of nodes put up the congestion in the network.

E. IMPACT ON THROUGHPUT

Throughput can be described as the amount of data passes through a system in a unit of time. In the IoT network, the total number of transmitted data conserved in a second to calculate throughput. Throughput can be expressed as equation 8.

$$\boldsymbol{TP} = \frac{\sum\left(Q_i^r x l_i\right)}{T_w} \tag{8}$$

Here, TP denotes throughput, while Q_i^r is the Quantity and l_i is the length of the ith kind, and T_w denotes as the whole time of the simulation.

F. PACKET DELIVERY RATIO

Packet Delivery Ratio is calculated based on the number of packets sent by the sender and the number of packets successfully received at the receiver end. However, it depends on several factors like network configuration, device capabilities, bandwidth; therefore, it is difficult to test the network performance. Equation 9 can be used to calculate the Packet Delivery Ratio.

$$\boldsymbol{PDR} = \frac{N_{rp}}{N_{sp}} \tag{9}$$

where PDR is Packet Delivery Ratio; N_{sp} is the total number of sent packets, and N_{rp} is the total number of received packets. It has been identified that throughput falls when the number of nodes increases in a network. In the WSN, packet-sending circumstances are defined in the energy model, like that, energy is consumed when a packet is sent over the network. Therefore, more packet transfer cost core energy consumption. Ultimately, the packet can be discarded due to less energy or long-distance travel.

G. COMMUNICATION COST

As mention in FIGURE 1 communication for authentication in IoT can be different for different protocols. Furthermore, it may carry the contrasting size of the message to communicate in several phases. Consequently, to establish a secure authentication, a process needs a minimum of four messages and these messages travel among user, sensor, and gateway node or authentication server. However, different messages contain different values, so the size of those messages also differs. To illustrate, a brief comparison of the communication cost of different protocols have been shown in TABLE 21.

However, we should also take care of communication cost on behalf of standards, because different standards have different threshold values to transmit. Consequently, the IEEE 802.15.4 communication standard supports 127 bytes, whilst the IEEE 802.15.6 standard has a maximum message frame length of 255 bytes.

H. COMPUTATION COST

In the IoT network, computation also depends on the kind of protocols. As most of the network devices have computation constraints, the heavyweight computation cannot be performed in IoT networks. Therefore, protocol developers always try to create lightweight authentication protocols for IoT networks. Therefore, many of the researchers have adopted the concept of hash, XOR and concatenation to secure the message to pass through the network. ECC, MOD, Fuzzy commitments are also implemented in the IoT authentication mechanism. TABLE 22 describes the notation used to calculate the computational cost and comparison analysis is demonstrated in TABLE 24.

I. STORAGE COST/MEMORY COST

To establish IoT authentication, protocols use different types of mechanisms. Among them, the smart card is one of the popular techniques. A smart card needs some storage capabilities because it stores user credentials, sensors, and GWN information. Different protocols use different operations to achieve authentication. TABLE 23 shows the comparisons of storage cost among different IoT authentication protocols.

J. ENERGY COST

IoT components are subject to power constraints. Therefore, the energy consumption of a protocol is equally important with other factors. Energy is proportional to power. Nevertheless, if a protocol consumes more energy, battery drainage will happen more quickly. Furthermore, the energy cost of transmitting and receiving data can be calculated based on equation 10 and equation 11 consecutively [131], [132].

$$E_{Tx}\left(k, d\right) = Eelec * k + \in amp * k * d^2, d > 1 \tag{10}$$

where $E_{Tx}\left(k, d\right)$ is the energy consumption of transmitting data. k is the transmitted data volume (bit), d is the distance between two objects, $Eelec$ is the energy consumption of data transmission in terms of nJ/bit. $\in$ amp is the energy consumption constant used to expand radio coverage in terms of nJ/(bit∗m2).

Therefore, the energy cost of transmitting data between two objects is proportional to the distance between them. In addition, the energy cost of receiving data is shown below.

$$E_{Rx}\left(k\right) = Eelec * k \tag{11}$$

where $E_{Rx}\left(k\right)$ is the energy consumption for receiving data.

VI. OPEN ISSUES AND FUTURE DIRECTIONS

A vast range of encryption techniques is used in IoT authentication schemes, which include, hash, XOR, ECC. To make

TABLE 21. Comparison of communication cost.

Schemes	Communication Cost	Description
Amin, et al. [17]	2816 bits	The paper assumes the length of the identity (user, server), password, random nonce, and message digest takes 128 bits each.
Farash, et al. [26]	434 bytes	The research focuses on the application layer on the OSI model and ignores other models to compute communication costs. The protocol needs four messages to pass to establish the communication and they are as follows: User – Sensor node: 79 bytes Sensor node – Gateway node: 158 bytes Gateway node – Sensor node: 99 bytes Sensor node – User: 98 bytes
Wu, et al. [28]	7168 bits	This paper focuses on two cases to compute computational cost. Case 1: If the sensor id is available in the database of the home gateway node. Case 2: If the sensor id is not available in the database of the home gateway node. So, computational costs are as follows: Case 1: 2688 bits Case 2: 4480 bits
Li, et al. [31]	2720 bits	The paper assumes the sensor node's identity, gateway node's identity, the output of the hash function, the random number are all 160 bits. Furthermore, the length of the user's identity is 80 bits and the length of the timestamp is 32 bits. Additionally, The subgroup G of ECC is 160 bits, and the size of the element in G is 320 bits and the block size of symmetric cryptography is 128 bits.
Li, et al. [32]	1856 bits	The paper calculates communication cost based on the message passing in the different stages and the stages are as follows: User to Gateway: 2*160+3*128=704 bits Gateway to Sensor: 4*128 = 512 bits Sensor to Gateway: 2*128 = 256 bits Gateway to User: 3*128 = 384 bits Where, length of the random number, timestamp, and output of the one-way hash function, secret key, identity, and password are 128 bits, and the length of ECC point multiplication is 160 bits.
Li, et al. [33]	2688 bits	This paper assumes the sensor node's identity, gateway's identity, the output of the hash function, the random number are all 160 bits. The length of the user's identity and timestamps are, respectively, 80 and 32 bits. The subgroup G of ECC is 160 bits, and the size of the element in G is 320 bits. Besides, the block size of the symmetric cryptography is 128 bits.
Roy, et al. [34]	992 bits	This protocol only considers the login and authentication phase. As the registration phase is once, the cost involved in this phase is not taken as consideration. This protocol only needs two message exchanges of 640 and 352 bits respectively.

TABLE 22. Notation used to calculate computational cost.

Notation	Description
T_H	Hash computational cost
T_{XOR}	XOR computational cost
T_M	time of executing a modular exponentiation
T_{ECC}	Elliptic curve cryptography execution time
T_S	symmetric encryption/decryption cost
T_{CH}	Chebyshev map operation
T_{FE}	Fuzzy extractor operation
T_{SM}	scalar-point multiplication

TABLE 23. Smart card storage cost of IoT authentication protocols. CH* denotes cluster head.

Protocol	Storage cost
Farash, et al. [26]	512
Amin, et al. [36]	640
Xue, et al. [76]	640
Amin and Biswas [121]	640
Das, et al. [128]	768+CH*
Turkanović, et al. [120]	768
Yeh, et al. [129]	896
Turkanovic and Holbl [130]	768+CH*

a more secure authentication mechanism, protocols use the smart card and biometric techniques beside user id and password. Moreover, to protect biometric information in the network, it makes use of other schemes like the fuzzy extractor, fuzzy commitment, bio hashing. However, the ultimate goal of any newly designed authentication protocol is to make lightweight (low computation and storage cost) and to protect from known common attacks, by considering the factor of low computational power and low memory space of IoT peripherals. As IoT based network is under development stage, it needs more supervision. Therefore, some key issues and future challenges are discussed in the subsequent parts.

TABLE 24. Comparison of computational cost.

Schemes	User	Sensor	GWN	RFID-tag	Reader	Server	Execution Time	Total	Description
Amin, et al. [17]	No	No	No	No	No	No	0.009ms	$22T_H$	This protocol takes 0.002ms at the login phase and 0.007ms at the authentication phase on the basis of time. Whereas, it takes $5T_H$ and $17T_H$ at the login and authentication phases respectively.
Jiang, et al. [18]	$8T_H + 2T_{ECC}$	$6T_H$	$9T_H + 1T_{ECC}$	No	No	No	0.2008ms	$23T_H + 3T_{ECC}$	This protocol uses ECC and its cost is 0.2008ms.
Chang and Le [24]	$7T_H + 4T_{XOR}$	$5T_H + 4T_{XOR}$	$8T_H + 1T_{XOR}$	No	No	No	No	$20T_H + 9T_{XOR}$	This paper proposes a protocol that does not require any databases in the gateway node to keep the shared secrets. As this protocol is lightweight and it does not provide perfect forward secrecy, this paper presents another protocol, which guarantees the forward secrecy.
Farash, et al. [26]	$11T_H$	$7T_H$	$14T_H$	No	No	No	No	$32T_H$	This protocol uses an increasing amount of hash computation especially at user and gateway node to make the protocol more secure. This overall cause makes this protocol computationally high.
Gope, et al. [29]	No	No	No	$5T_H$	$2T_H$	$7T_H$	0.91ms	$14T_H$	This protocol uses SHA-256, which is simulated on MSP 430 family with a frequency of 8 MHz, where the execution time, which is denoted by t_H, of SHA256 is 0.065 msec.
Kang, et al. [30]	No	No	No	No	No	No	0.0135ms	$27T_H + 15T_{XOR}$	This protocol consumes computational cost based on following details: Registration phase: $6T_H + 3T_{XOR}$ Login phase: $6T_H + 3T_{XOR}$ Authentication phase: $8T_H + 6T_{XOR}$ Password change phase: $7T_H + 3T_{XOR}$
Li, et al. [31]	$8T_H + 3T_M$	$4T_H + 2T_M$	$7T_H + 1T_M$	No	No	No	No	$19T_H + 6T_M$	This paper uses ECC and takes more time to execute modular exponentiation.
Li, et al. [32]	$8T_H + 2T_{ECC}$	$4T_H$	$9T_H + 1T_{ECC}$	No	No	No	1.2834ms	$21T_H + 3T_{ECC}$	In this paper, the sensor node does not need to calculate the ECC point multiplication operation. Nevertheless, its T_H computation is higher. However, according to Wu, et al. [133], T_{ECC} is larger than T_H, which are 0.427576ms and 0.0000328ms respectively.
Li, et al. [33]	$7T_H + 2T_s + 2T_{ECC}$	$4T_H + 2T_s$	$8T_H + 4T_s + 1T_{ECC}$	No	No	No	3.743ms	$19T_H + 8T_s + 3T_{ECC}$	This protocol uses 2.474ms at the user, 1.255ms at gateway and 3.743ms at the sensor node.
Roy, et al. [34]	$9T_H + 1T_{FE} + 2T_{CH}$	No	No	No	No	$5T_H + 1T_{CH}$	133.14ms	$13T_H + 1T_{FE} + 3T_{CH}$	This protocol is a chaotic map-based scheme for e-health care. They consider user and server computational costs, which are 109.62 ms and 23.52 ms, respectively based on time.
Cho, et al. [94]	No	No	No	$3T_H$	$2T_H$	$5T_H$	0.65ms	$10T_H$	In the proposed protocol, the tag performs two hash computations, four modular computations, and one random number generation.
He, et al. [113]	$8T_H$	$6T_H$	$9T_H$	No	No	No	0.46ms	$23T_H$	This protocol uses temporal-credential-based mutual authentication and key agreement scheme
Yeh, et al. [129]	$1T_H + 2T_{ECC}$	$3T_H + 2T_{ECC}$	$4T_H + 4T_{ECC}$	No	No	No	No	$8T_H + 8T_{ECC}$	This protocol uses ECC and smartcard.
Shi and Gong [134]	$6T_H + 3T_{ECC}$	$4T_H + 2T_{ECC}$	$4T_H + T_{ECC}$	No	No	No	No	$14T_H + 6T_{ECC}$	This protocol uses ECC.
Choi, et al. [135]	$7T_H + 3T_{SM}$	$4T_H + 2T_{SM}$	$4T_H + 1T_{SM}$	No	No	No	No	$15T_H + 6T_{SM}$	This protocol uses ECC.
Yang, et al. [136]	No	No	No	$2T_H$	$3T_H$	$5T_H$	0.65	$10T_H$	This protocol uses only hash function and XOR operations.

TABLE 25. Lists of figures in the document.

A. DETECTION OF ATTACK

It is obvious that secure access to the information in a network is the prime concern in the application layer in IoT. However, if the system is incapable to deliver the demanded service, it is of no use. In addition, attacks are used to reduce the ability of a network to communicate with its legitimate resources. Attacks are dangerous threats as it cripples the network by repelling unnecessary traffic in a network or forge the traffic to disconnect the communication. In case attacks are frequent in IoT authentication, it renders the server partially or completely unavailable to provide any service. Subsequently, recent attacks create threats for IoT networks. Therefore, sensing attacks in IoT authentication is important, because sensors are the soft targets of the attackers.

B. TIME BASED AUTHENTICATION

On the other hand, timely respond to the sender is important as authentication needs on time. Additionally, protocols use timestamp and session keys to protect from attacks. However, they are vulnerable to new attacks. Therefore, IoT authentication may concentrate on hierarchical and distributed approaches that consider timing.

C. TECHNOLOGY AND STANDARD

A vast technology and communication standards are used in the IoT network. However, different technology and strong standards are still missing in IoT to ensure access control, confidentiality, privacy and security among users and things. Moreover, this is unable to cope with the defined protection constraints, which in return ensures

TABLE 26. Lists of tables in the document.

trustworthiness among users and devices; provides security of using the IoT authentication service on the public network.

D. STRONG AUTHENTICATION PROTOCOLS

As the number of attacks is huge in IoT networks especially during the first stage of network access that is authentication mitigating attacks and clustering, different network packets by its behavior are important to increase the throughput of a system. Therefore, detecting external as well as internal attacks are challenging. However, scopes are there to design a strong authentication protocol to prevent and protect the IoT network from all potential attacks.

E. FORMAL WAY OF SECURITY AUTHENTICATION

Although authentication protocols use different evaluation techniques to confirm the security of protocols for IoT networks, there is a need for a formal way to define security aspects of authentication in IoT.

F. CONSISTENT NETWORK

IoT authentication mechanism takes place over both secure and insecure networks, where the login and authentication phase may perform in an insecure network but the registration phase must undergo through a secure network. However, this provision may not be available everywhere, which may invite attackers to enter into the system. Therefore, it is desirable to consider the registration phase under an insecure network.

G. OFFLINE ACCESS

Sensor components are the backbone of the IoT network, as they distribute the network and store confidential communication data in it. As per the networks need, sensor nodes have been deployed in various challenging environments like a battlefield, agriculture, or in natural calamities like a forest fire, tsunami, earthquake detection or areas like nuclear threats. However, a situation may arise where the sensor node disconnects from GWN or AS due to network linkage error [137]. This scenario may turn to be difficult for many reasons; users may need to access isolated sensor nodes immediately to get valuable information for decision-making or those isolated sensor nodes may loss crucial data stored in it due to low power capacities. Therefore, authentication protocols need to validate legitimate users on isolated sensors. However, this new mechanism should not encourage adversaries to penetrate the sensor and grab information, which also needs to be under consideration.

H. NEW TECHNIQUES IN AUTHENTICATION

To make the authentication protocol lightweight, researchers use XOR and hash functions. Moreover, protocols use different commitments to ensure the security of authenticated data. However, there is a lot of scopes to introduce new and different techniques for authenticating data. Quantum computing, quantum bit commitment, and quantum cryptography are the open challenges to introduce in IoT authentication.

I. ANONYMITY

As the share of data is huge, anonymization becomes an important factor in IoT. An adversary can attack an IoT network to get users' detail, which may reveal confidential information i.e. health records. On the other hand, a hacker can track the position of a user or an object and can perform harm to them or their property especially on VANET. Therefore, future research should focus on data anonymization while improving the authentication mechanism for IoT, which demotes traceability.

Additionally, the WSN application layer is in the developing stage. However, plethora of attacks are at different levels, but we need more attention to this level to encourage the researcher to implementing a well-constructed and robust lightweight application for IoT authentication.

VII. CONCLUSION

The current concept of network and connectivity is going to be changed in the next few years. As it is predicted that the number of connected devices in the world will take over the headcount of human beings soon, which can be possible because of the expansion of the Internet of Things. However, security on IoT is still searching for its way to improve so that it can provide reliability and protection against threats. Again, authentication is one of the main important parts in security, because it is the gateway of a user or device to introduce in a network. In addition, a slew of authentication protocols are designed, broken, and again redesigned to protect the network from attacks. Therefore, this paper shows the potential threats in IoT authentication and existing protocols to protect them.

To our best knowledge, there is no research conducted similar to us as of now. All of the other research work focus on IoT security, authentication protocols, and attack models on IoT. We believe that our study will benefit readers to get knowledge about a huge range of attacks and methods in IoT authentication and help the upcoming researcher to formulate their proposal to create strong IoT authentication protocol to serve better to end-users.

APPENDIX

TABLE 25 and TABLE 26 represent the lists of figures and the lists of tables use in this document respectively.

ACKNOWLEDGMENT

The authors of this research would like to thank the anonymous reviewers for their insights, comments, and suggestions to improve the quality of the manuscripts.

REFERENCES

[1] ITU's Strategy and Policy Unit (SPU), "ITU Internet reports 2005: The Internet of Things," Int. Telecommun. Union, Geneva, Switzerland, ITU Internet Rep. 2005, 2005.

[2] *Hype Cycle for the Internet of Things 2017*, G. Inc., Stamford, CT, USA, Jul. 2017.

[3] R. Lutolf, "Smart Home concept and the integration of energy meters into a home based system," in *Proc. 7th Int. Conf. Metering App. Tariffs Electr. Supply*, vol. 367, Nov. 1992, pp. 277–278.

[4] A. Zanella, N. Bui, A. Castellani, L. Vangelista, and M. Zorzi, "Internet of Things for smart cities," *IEEE Internet Things J.*, vol. 1, no. 1, pp. 22–32, Feb. 2014. doi: 10.1109/jiot.2014.2306328.

[5] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A survey," *Comput. Netw.*, vol. 54, no. 15, pp. 2787–2805, Oct. 2010.

[6] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions," *Future Generat. Comput. Syst.*, vol. 29, no. 7, pp. 1645–1660, 2013.

[7] C. M. Medaglia and A. Serbanati, ''An overview of privacy and security issues in the Internet of Things,'' in *The Internet Things*, D. Giusto, A. Iera, G. Morabito, L. Atzori, Eds. New York, NY, USA: Springer, 2010, pp. 389–395.

[8] M. N. Napiah, M. Y. I. B. Idris, R. Ramli, and I. Ahmedy, ''Compression header analyzer intrusion detection system (CHA—IDS) for 6LoWPAN communication protocol,'' *IEEE Access*, vol. 6, pp. 16623–16638, 2018. doi: 10.1109/ACCESS.2018.2798626.

[9] B. S. Khater, A. A. Wahab, M. Idris, M. A. Hussain, and A. A. Ibrahim, ''A lightweight perceptron-based intrusion detection system for fog computing,'' *Appl. Sci.*, vol. 9, no. 1, p. 178, Jan. 2019. doi: 10.3390/app9010178.

[10] H. H. Bosman, G. Iacca, A. Tejada, H. J. Wörtche, and A. Liotta, ''Spatial anomaly detection in sensor networks using neighborhood information,'' *Inf. Fusion*, vol. 33, pp. 41–56, Jan. 2017. doi: 10.1016/j.inffus.2016.04.007.

[11] D. Zissis, ''Intelligent security on the edge of the cloud,'' in *Proc. Int. Conf. Eng., Technol. Innov. (ICE/ITMC)*, R. JardimGoncalves, J. P. Mendonca, M. Pallot, A. Zarli, J. Martins, and M. Marques Eds., Jun. 2017, pp. 1066–1070.

[12] M. Domb, E. Bonchek-Dokow, and G. Leshem, ''Lightweight adaptive random-forest for IoT rule generation and execution,'' *J. Inf. Secur. Appl.*, vol. 34, pp. 218–224, Jun. 2017. doi: 10.1016/j.jisa.2017.03.001.

[13] F. Y. Yavuz, D. Ünal, and E. Gül, ''Deep learning for detection of routing attacks in the Internet of Things,'' *Int. J. Comput. Intell. Syst.*, vol. 12, no. 1, pp. 39–58, Nov. 2018. doi: 10.2991/ijcis.2018.25905181.

[14] *ITU Internet Reports 2005: The Internet of Things Executive Summary*, I. T. Uninon, Geneva, Switzerland, 2005.

[15] A. Sulleyman. *NHS Cyber Attack: Why Stolen Medical Information is so Much More Valuable than Financial Data*. Accessed: Jul. 4, 2019. [Online]. Available: https://www.independent.co.uk/life-style/gadgets-and-tech/news/nhs-cyber-attack-medical-data-records-stolen-why-so-valuable-to-sell-financial-a7733171.html

[16] S. Tu, M. Waqas, S. U. Rehman, M. Aamir, O. U. Rehman, Z. Jianbiao, and C.-C. Chang, ''Security in fog computing: A novel technique to tackle an impersonation attack,'' *IEEE Access*, vol. 6, pp. 74993–75001, 2018. doi: 10.1109/access.2018.2884672.

[17] R. Amin, N. Kumar, G. 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. doi: 10.1016/j.future.2016.12.028.

[18] 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. doi: 10.1016/j.jnca.2016.10.001.

[19] J. R. Wallrabenstein, ''Practical and secure IoT device authentication using physical unclonable functions,'' presented at the IEEE 4th Int. Conf. Future Internet Things Cloud, New York, NY, USA, 2016.

[20] B.-Z. He, C.-M. Chen, Y.-P. Su, and H.-M. Sun, ''A defence scheme against identity theft attack based on multiple social networks,'' *Expert Syst. Appl.*, vol. 41, no. 5, pp. 2345–2352, Apr. 2014. doi: 10.1016/j.eswa.2013.09.032.

[21] M. Sarvabhatla and C. S. Vorugunti, ''A secure biometric-based user authentication scheme for heterogeneous WSN,'' presented at the 4th Int. Conf. Emerg. Appl. Inf. Technol., 2014.

[22] I.-P. Chang, T.–F. Lee, T.-H. Lin, and C.-M. Liu, ''Enhanced two-factor authentication and key agreement using dynamic identities in wireless sensor networks,'' *Sensors*, vol. 15, no. 12, pp. 29841–29854, Nov. 2015. doi: 10.3390/s151229767.

[23] N. Saxena, S. Grijalva, and N. S. Chaudhari, ''Authentication protocol for an IoT-enabled LTE network,'' *ACM Trans. Internet. Technol.*, vol. 16, no. 4, Dec. 2016, Art. no. 22. doi: 10.1145/2981547.

[24] 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. doi: 10.1109/twc.2015.2473165.

[25] S. Dolev, L. Krzywiecki, N. Panwar, and M. Segal, ''Vehicle authentication via monolithically certified public key and attributes,'' *Wireless Netw.*, vol. 22, no. 3, pp. 879–896, Apr. 2016.

[26] M. S. Farash, M. Turkanović, S. Kumari, and M. Hölbl, ''An efficient user authentication and key agreement scheme for heterogeneous wireless sensor network tailored for the Internet of Things environment,'' *Ad Hoc Netw.*, vol. 36, pp. 152–176, Jan. 2016. doi: 10.1016/j.adhoc.2015.05.014.

[27] S. Banerjee, C. Chunka, S. Sen, and R. S. Goswami, ''An enhanced and secure biometric based user authentication scheme in wireless sensor networks using smart cards,'' *Wireless Pers. Commun.*, vol. 107, no. 1, pp. 243–270, Jul. 2019. doi: 10.1007/s11277-019-06252-x.

[28] F. Wu, L. Xu, S. Kumari, X. Li, J. Shen, K.-K. R. Choo, M. Wazid, and A. K. Das, ''An efficient authentication and key agreement scheme for multi-gateway wireless sensor networks in IoT deployment,'' *J. Netw. Comput. Appl.*, vol. 89, pp. 72–85, Jul. 2017. doi: 10.1016/j.jnca.2016.12.008.

[29] P. Gope, R. Amin, S. K. H. Islam, N. Kumar, and V. K. Bhalla, ''Lightweight and privacy-preserving RFID authentication scheme for distributed IoT infrastructure with secure localization services for smart city environment,'' *Future Gener. Comput. Syst.*, vol. 83, pp. 629–637, Jun. 2018. doi: 10.1016/j.future.2017.06.023.

[30] D. Kang, J. Jung, H. Kim, Y. Lee, and D. Won, ''Efficient and secure biometric-based user authenticated key agreement scheme with anonymity,'' *Secur. Commun. Netw.*, vol. 2018, Jun. 2018, Art. no. 9046064. doi: 10.1155/2018/9046064.

[31] X. Li, J. Niu, M. Z. A. Bhuiyan, F. Wu, M. Karuppiah, and S. Kumari, ''A robust ECC-based provable secure authentication protocol with privacy preserving for industrial Internet of Things,'' *IEEE Trans. Ind. Informat.*, vol. 14, no. 8, pp. 3599–3609, Aug. 2018. doi: 10.1109/TII.2017.2773666.

[32] X. Li, J. Niu, S. Kumari, F. Wu, A. K. Sangaiah, and K.-K. R. Choo, ''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. doi: 10.1016/j.jnca.2017.07.001.

[33] X. Li, J. Peng, J. Niu, F. Wu, J. Liao, and K. R. Choo, ''A robust and energy efficient authentication protocol for industrial Internet of Things,'' *IEEE Internet Things J.*, vol. 5, no. 3, pp. 1606–1615, Jun. 2018. doi: 10.1109/JIOT.2017.2787800.

[34] S. Roy, S. Chatterjee, A. K. Das, S. Chattopadhyay, S. Kumari, and M. Jo, ''Chaotic map-based anonymous user authentication scheme with user biometrics and fuzzy extractor for crowdsourcing Internet of Things,'' *IEEE Internet Things*, vol. 5, no. 4, pp. 2884–2895, Aug. 2018. doi: 10.1109/JIOT.2017.2714179.

[35] K.-H. Wang, C.-M. Chen, W. Fang, and T.-Y. Wu, ''On the security of a new ultra-lightweight authentication protocol in IoT environment for RFID tags,'' *J. Supercomput.*, vol. 74, no. 1, pp. 65–70, 2018. doi: 10.1007/s11227-017-2105-8.

[36] R. Amin, S. K. H. Islam, G. P. Biswas, M. K. Khan, L. Leng, and N. Kumar, ''Design of an anonymity-preserving three-factor authenticated key exchange protocol for wireless sensor networks,'' *Comput. Netw.*, vol. 101, pp. 42–62, Jun. 2016. doi: 10.1016/j.comnet.2016.01.006.

[37] K.-H. Yeh, ''A secure IoT-based healthcare system with body sensor networks,'' *IEEE Access*, vol. 4, pp. 10288–10299, 2016. doi: 10.1109/access.2016.2638038.

[38] S. Challa, M. Wazid, A. K. Das, N. Kumar, A. G. Reddy, E.-J. Yoon, and K.-Y. Yoo, ''Secure signature-based authenticated key establishment scheme for future IoT applications,'' *IEEE Access*, vol. 5, pp. 3028–3043, 2017. doi: 10.1109/access.2017.2676119.

[39] Q. Jiang, S. Zeadally, J. Ma, and D. He, ''Lightweight three-factor authentication and key agreement protocol for Internet-integrated wireless sensor networks,'' *IEEE Access*, vol. 5, pp. 3376–3392, 2017. doi: 10.1109/access.2017.2673239.

[40] J. Srinivas, S. Mukhopadhyay, and D. Mishra, ''Secure and efficient user authentication scheme for multi-gateway wireless sensor networks,'' *Ad Hoc Netw.*, vol. 54, pp. 147–169, Jan. 2017. doi: 10.1016/j.adhoc.2016.11.002.

[41] J. Shen, S. Chang, J. Shen, Q. Liu, and X. Sun, ''A lightweight multi-layer authentication protocol for wireless body area networks,'' *Future Gener. Comput. Syst.*, vol. 78, pp. 956–963, Jan. 2018. doi: 10.1016/j.future.2016.11.033.

[42] P. Punithavathi, S. Geetha, M. Karuppiah, S. K. H. Islam, M. M. Hassan, and K.-K. R. Choo, ''A lightweight machine learning-based authentication framework for smart IoT devices,'' *Inf. Sci.*, vol. 484, pp. 255–268, May 2019. doi: 10.1016/j.ins.2019.01.073.

[43] M. Dammak, O. R. M. Boudia, M. A. Messous, S. M. Senouci, and C. Gransart, ''Token-based lightweight authentication to secure IoT networks,'' in *Proc. 16th IEEE Annu. Consum. Commun. Netw. Conf. (CCNC)*, Jan. 2019, pp. 1–4. doi: 10.1109/CCNC.2019.8651825.

[44] R. S. Bali and N. Kumar, "Secure clustering for efficient data dissemination in vehicular cyber–physical systems," *Future Gener. Comput. Syst.*, vol. 56, pp. 476–492, Mar. 2016. doi: 10.1016/j.future.2015.09.004.

[45] P. Gope and T. Hwang, "BSN-care: A secure IoT-based modern healthcare system using body sensor network," *IEEE Sensors J.*, vol. 16, no. 5, pp. 1368–1376, Mar. 2016. doi: 10.1016/j.ins.2019.01.073.

[46] L. Malina, J. Hajny, R. Fujdiak, and J. Hosek, "On perspective of security and privacy-preserving solutions in the Internet of Things," *Comput. Netw.*, vol. 102, pp. 83–95, Jun. 2016. doi: 10.1016/j.comnet.2016.03.011.

[47] 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. doi: 10.1109/jiot.2017.2703088.

[48] M. P. De Almeida, R. T. De Sousa, L. J. G. Villalba, and T.-H. Kim, "New DoS defense method based on strong designated verifier signatures," *Sensors*, vol. 18, no. 9, p. 2813, Sep. 2018. doi: 10.3390/s18092813.

[49] Wireshark. (2006). *The Wireshark Team*. [Online]. Available: https://www.wireshark.org

[50] M. Heydari, S. M. S. Sadough, S. A. Chaudhry, M. S. Farash, and M. R. Aref, "An improved authentication scheme for electroni payment systems in global mobility networks," *Inf. Technol. Control*, vol. 44, no. 4, pp. 387–403, Jan. 2015. doi: 10.5755/j01.itc.44.4.9197.

[51] S. R. Ganta, S. P. Kasiviswanathan, and A. Smith, "Composition attacks and auxiliary information in data privacy," presented at the 14th ACM SIGKDD Int. Conf. Knowl. Discovery Data Mining, Las Vegas, NV, USA, 2008.

[52] M. M. Baig, J. Li, J. Liu, X. Ding, and H. Wang, "Data privacy against composition attack," in *Database Systems for Advanced Applications*, S.-G. Lee, Z. Peng, X. Zhou, Y.-S. Moon, R. Unland, and J. Yoo, Eds. Berlin, Germany: Springer, 2010, pp. 320–334.

[53] J. Cui, Z. Zhang, H. Li, and R. Sui, "An improved user authentication protocol for IoT," presented at the Int. Conf. Cyber-Enabled Distrib. Comput. Knowl. Discovery (CyberC), 2018.

[54] T. Viana, A. Zisman, and A. K. Bandara, "Towards a framework for managing inconsistencies in systems of systems," in *Proc. Int. Colloq. Softw.-Intensive Syst. Syst. 10th Eur. Conf. Softw. Archit.*, Nov. 2016, Art. no. 8.

[55] X. Li, Q. Wang, H. N. Dai, and H. Wang, "A novel friendly jamming scheme in industrial crowdsensing networks against eavesdropping attack," *Sensors*, vol. 18, no. 6, p. E1938, Jun. 2018. doi: 10.3390/s18061938.

[56] A. Asaduzzaman, S. Mazumder, S. Salinas, and M. F. Mridha, "A security-aware near field communication architecture," in *Proc. Int. Conf. Netw., Syst. Secur. (NSysS)*. New York, NY, USA, Jan. 2017, pp. 33–38.

[57] C. Zhang, K. Chen, X. Zeng, and X. Xue, "Misbehavior detection based on support vector machine and Dempster–Shafer theory of evidence in VANETs," *IEEE Access*, vol. 6, pp. 59860–59870, 2018. doi: 10.1109/access.2018.2875678.

[58] C. Pu and X. Zhou, "Suppression attack against multicast protocol in low power and lossy networks: Analysis and defenses," *Sensors*, vol. 18, no. 10, Sep. 2018. doi: 10.3390/s18103236.

[59] T. Kim and H. Kim, "Vehicle-to-vehicle message content plausibility check through low-power beaconing," in *Proc. IEEE 86th Veh. Technol. Conf. (VTC-Fall)*, New York, NY, USA, Sep. 2017, pp. 1–6.

[60] F. Xu, X. Zheng, X. Li, and Z. Zhou, "Partial cooperative spectrum sensing schedule in cognitive network," *Sci. China F, Inf. Sci.*, vol. 52, no. 12, pp. 2332–2341, Dec. 2009. doi: 10.1007/s11432-009-0222-6.

[61] R. Khan, K. McLaughlin, J. Hastings, D. Laverty, and S. Sezer, "Demonstrating cyber-physical attacks and defense for synchrophasor technology in smart grid," in *Proc. 16th Annu. Conf. Privacy, Secur. Trust (PST)*, K. McLaughlin, Ed. New York, NY, USA, Aug. 2018, pp. 257–266.

[62] M. A. Ferrag and A. Ahmim, "ESSPR: An efficient secure routing scheme based on searchable encryption with vehicle proxy re-encryption for vehicular peer-to-peer social network," *Telecommun. Syst.*, vol. 66, no. 3, pp. 481–503, 2017. doi: 10.1007/s11235-017-0299-y.

[63] L. Yao, L. Kang, P. F. Shang, and G. W. Wu, "Protecting the sink location privacy in wireless sensor networks," *Pers. Ubiquitous Comput.*, vol. 17, no. 5, pp. 883–893, Jun. 2013. doi: 10.1007/s00779-012-0539-9.

[64] S. R. Moosavi, T. N. Gia, E. Nigussie, A. M. Rahmani, S. Virtanen, H. Tenhunen, and J. Isoaho, "End-to-end security scheme for mobility enabled healthcare Internet of Things," *Future Gener. Comput. Syst.*, vol. 64, pp. 108–124, Nov. 2016. doi: 10.1016/j.future.2016.02.020.

[65] G. Daneels, "Real-Time data dissemination and analytics platform for challenging IoT environments," presented at the Global Inf. Infrastruct. Netw. Symp. (GIIS), 2017.

[66] K. Mahmood, S. A. Chaudhry, H. Naqvi, T. Shon, and H. F. Ahmad, "A lightweight message authentication scheme for smart grid communications in power sector," *Comput. Elect. Eng.*, vol. 52, pp. 114–124, May 2016. doi: 10.1016/j.compeleceng.2016.02.017.

[67] M. A. Ferrag, L. A. Maglaras, H. Janicke, J. Jiang, and L. Shu, "Authentication protocols for Internet of Things: A comprehensive survey," *Secur. Commun. Netw.*, vol. 2017, Nov. 2017, Art. no. 6562953. doi: 10.1155/2017/6562953.

[68] P. H. Griffin, "Secure authentication on the Internet of Things," in *Proc. SoutheastCon*, Mar./Apr. 2017, pp. 1–5. doi: 10.1109/SECON.2017.7925274.

[69] F. Wu, L. Xu, S. Kumari, and X. Li, "A privacy-preserving and provable user authentication scheme for wireless sensor networks based on Internet of Things security," *J. Ambient Intell. Hum. Comput.*, vol. 8, no. 1, pp. 101–116, Feb. 2017. doi: 10.1007/s12652-016-0345-8.

[70] S. Kumari, M. K. Khan, and M. Atiquzzaman, "User authentication schemes for wireless sensor networks: A review," *Ad Hoc Netw.*, vol. 27, pp. 159–194, Apr. 2015. doi: 10.1007/s12652-016-0345-8.

[71] S. Sciancalepore, G. Piro, G. Boggia, and G. Bianchi, "Public key authentication and key agreement in IoT devices with minimal airtime consumption," *IEEE Embedded Syst. Lett.*, vol. 9, no. 1, pp. 1–4, Mar. 2017. doi: 10.1109/les.2016.2630729.

[72] M. A. Jan, F. Khan, M. Alam, and M. Usman, "A payload-based mutual authentication scheme for Internet of Things," *Future Gener. Comput. Syst.*, vol. 92, pp. 1028–1039, Mar. 2019. doi: 10.1016/j.future.2017.08.035.

[73] P. Hu, H. Ning, T. Qiu, H. Song, Y. Wang, and X. Yao, "Security and privacy preservation scheme of face identification and resolution framework using fog computing in Internet of Things," *IEEE Internet Things J.*, vol. 4, no. 5, pp. 1143–1155, Oct. 2017. doi: 10.1109/les.2016.2630729.

[74] T. Song, R. Li, B. Mei, J. Yu, X. Xing, and X. Cheng, "A privacy preserving communication protocol for IoT applications in smart homes," *IEEE Internet Things J.*, vol. 4, no. 6, pp. 1844–1852, Dec. 2017. doi: 10.1109/les.2016.2630729.

[75] H. Hong, B. Hu, and Z. Sun, "Toward secure and accountable data transmission in Narrow Band Internet of Things based on blockchain," *Int. J. Distrib. Sensor Netw.*, vol. 15, no. 4, Apr. 2019, Art. no. 1550147719842725. doi: 10.1177/1550147719842725.

[76] K. Xue, C. Ma, P. Hong, and R. Ding, "A temporal-credential-based mutual authentication and key agreement scheme for wireless sensor networks," *J. Netw. Comput. Appl.*, vol. 36, no. 1, pp. 316–323, Jan. 2013. doi: 10.1016/j.jnca.2012.05.010.

[77] J. Moon, I. Y. Jung, and J. H. Park, "IoT application protection against power analysis attack," *Comput. Electr. Eng.*, vol. 67, pp. 566–578, Apr. 2018. doi: 10.1016/j.compeleceng.2018.02.030.

[78] G. Liu, W. Quan, N. Cheng, H. Zhang, and S. Yu, "Efficient DDoS attacks mitigation for stateful forwarding in Internet of Things," *J. Netw. Comput. Appl.*, vol. 130, pp. 1–13, Mar. 2019. doi: 10.1016/j.jnca.2019.01.006.

[79] M. Sarvabhatla, L. N. Kodavali, and C. S. Vorugunti, "An energy efficient temporal credential based mutual authentication scheme for WSN," in *Proc. 3rd Int. Conf. ECO-Friendly Comput. Commun. Syst.*, Dec. 2014, pp. 73–78. doi: 10.1109/Eco-friendly.2014.90.

[80] S. Huh, S. Cho, and S. Kim, "Managing IoT devices using blockchain platform," in *Proc. 19th Int. Conf. Adv. Commun. Technol. (ICACT)*, Feb. 2017, pp. 464–467.

[81] M. Anagnostopoulos, G. Kambourakis, P. Kopanos, G. Louloudakis, and S. Gritzalis, "DNS amplification attack revisited," *Comput. Secur.*, vol. 39, pp. 475–485, Nov. 2013. doi: 10.1016/j.cose.2013.10.001.

[82] O. Salman, S. Abdallah, I. H. Elhajj, A. Chehab, and A. Kayssi, "Identity-based authentication scheme for the Internet of Things," presented at the IEEE Symp. Comput. Commun., New York, NY, USA, 2016.

[83] V. Suryani, S. Sulistyo, and W. Widyawan, "Two-phase security protection for the Internet of Things object," *J. Inf. Process. Syst.*, vol. 14, no. 6, pp. 1431–1437, Dec. 2018.

[84] D. Chen, N. Zhang, Z. Qin, X. Mao, Z. Qin, X. Shen, and X.-Y. Li, "S2M: A lightweight acoustic fingerprints-based wireless device authentication protocol," *IEEE Internet Things J.*, vol. 4, no. 1, pp. 88–100, Feb. 2017. doi: 10.1109/JIOT.2016.2619679.

[85] K. N. Raja and M. M. Beno, "Secure data aggregation in wireless sensor network-Fujisaki okamoto(FO) authentication scheme against sybil attack," *J. Med. Syst.*, vol. 41, no. 7, p. 107, Jul. 2017. doi: 10.1007/s10916-017-0743-2.

[86] M. A. Uddin, A. Stranieri, I. Gondal, and V. Balasubramanian, "Continuous patient monitoring with a patient centric agent: A block architecture," *IEEE Access*, vol. 6, pp. 32700–32726, 2018. doi: 10.1109/ACCESS.2018.2846779.

[87] R. Lu, X. Lin, X. Liang, and X. Shen, "FLIP: An efficient privacy-preserving protocol for finding like-minded vehicles on the road," in *Proc. IEEE Global Telecommun. Conf. (GLOBECOM)*, Dec. 2010, pp. 1–5. doi: 10.1109/GLOCOM.2010.5684211.

[88] S. Paavolainen, T. Elo, and P. Nikander, "Risks from spam attacks on blockchains for Intemet-of-Things devices," presented at the IEEE 9th Annu. Inf. Technol., Electron. Mobile Commun. Conf. (IEMCON), 2018.

[89] Y. Du, M. Fang, J. Yi, J. Cheng, and D. Tao, "Towards query efficient black-box attacks: An input-free perspective," presented at the 11th ACM Workshop Artif. Intell. Secur. (AISec), 2018.

[90] X. Liang, M. Barua, R. Lu, X. Lin, and X. S. Shen, "HealthShare: Achieving secure and privacy-preserving health information sharing through health social networks," *Comput. Commun.*, vol. 35, no. 15, pp. 1910–1920, Sep. 2012. doi: 10.1016/j.comcom.2012.01.009.

[91] L. Duan, Y. Zhang, S. Chen, S. Wang, B. Cheng, and J. Chen, "Realizing IoT service's policy privacy over publish/subscribe-based middleware," *SpringerPlus*, vol. 5, no. 1, p. 1615, 2016. doi: 10.1186/s40064-016-3250-x.

[92] J. Shen, T. Zhou, F. Wei, X. Sun, and Y. Xiang, "Privacy-preserving and lightweight key agreement protocol for V2G in the social Internet of Things," *IEEE Internet Things J.*, vol. 5, no. 4, pp. 2526–2536, Aug. 2018. doi: 10.1109/jiot.2017.2775248.

[93] D. Wang, J. Ming, T. Chen, X. Zhang, and C. Wang, "Cracking IoT device user account via brute-force attack to SMS authentication code," presented at the 1st Workshop Radical Experiential Secur., Incheon, Republic of Korea, 2018.

[94] J.-S. Cho, Y.-S. Jeong, and S. Park, "Consideration on the brute-force attack cost and retrieval cost: A hash-based radio-frequency identification (RFID) tag mutual authentication protocol," *Comput. Math. Appl.*, vol. 69, no. 1, pp. 58–65, 2012.

[95] D. Bisson. *5 Social Engineering Attacks to Watch Out For, The State Of Security News. Trends. Insights*. Accessed: Jul. 16, 2019. [Online]. Available: https://www.tripwire.com/state-of-security/security-awareness/5-social-engineering-attacks-to-watch-out-for/

[96] M. Harwood, *Internet Security: How to Defend Against Attackers on the Web*. Burlington, MA, USA: Jones & Bartlett, 2015.

[97] Web Application Security Center. *Social Engineering Attack Lifecycle*. Accessed: May 4, 2019. [Online]. Available: https://incapsula.com

[98] T. S. Messerges, E. A. Dabbish, and R. H. Sloan, "Examining smart-card security under the threat of power analysis attacks," *IEEE Trans. Comput.*, vol. 51, no. 5, pp. 541–552, May 2002.

[99] N. Nissim, R. Yahalom, and Y. Elovici, "USB-based attacks," *Comput. Secur.*, vol. 70, pp. 675–688, Sep. 2017. doi: 10.1016/j.cose.2017.'08.002.

[100] T. H. Lin, C. C. Lee, and C. H. Chang, "WSN integrated authentication schemes based on Internet of Things," *J. Internet Technol.*, vol. 19, no. 4, pp. 1043–1053, Jul. 2018.

[101] G. Ma, X. Li, Q. Q. Pei, and Z. Li, "A secure routing protocol based on RPL for Internet of Things," in *Proc. Int. Conf. Netw. Netw. Appl.*, New York, NY, USA, Dec. 2017, pp. 209–213.

[102] S. R. Rajeswari and V. Seenivasagam, "Comparative study on various authentication protocols in wireless sensor networks," *Sci. World J.*, vol. 2016, Jan. 2016, Art. no. 6854303.

[103] P. Amish and V. B. Vaghela, "Detection and prevention of wormhole attack in wireless sensor network using AOMDV protocol," *Procedia Comput. Sci.*, vol. 79, pp. 700–707, 2016. doi: 10.1016/j.procs.2016.03.092.

[104] V. Bansal and K. K. Saluja, "Anomaly based detection of black hole attack on leach protocol in WSN," presented at the IEEE Int. Conf. Wireless Commun., Signal Process. Netw., New York, NY, USA, 2016.

[105] H. Kaur and A. Singh, "Identification and mitigation of black hole attack in wireless sensor networks," presented at the Int. Conf. Micro-Electron. Telecommun. Eng., New York, NY, USA, 2016.

[106] I. Memon, L. Chen, Q. A. Arain, H. Memon, and G. C. Chen, "Pseudonym changing strategy with multiple mix zones for trajectory privacy protection in road networks," *Int. J. Commun. Syst.*, vol. 31, no. 1, Jan. 2018, Art no. e3437. doi: 10.1002/dac.3437.

[107] M. Motamedi and N. Yazdani, "Detection of black hole attack in wireless sensor network using UAV," presented at the 7th Conf. Inf. Knowl. Technol., New York, NY, USA, 2015.

[108] M. M. Fouda, Z. M. Fadlullah, N. Kato, R. Lu, and X. Shen, "A lightweight message authentication scheme for smart grid communications," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 675–685, Dec. 2011. doi: 10.1109/TSG.2011.2160661.

[109] M. Hossain and R. Hasan, "Boot-IoT: A privacy-aware authentication scheme for secure bootstrapping of IoT nodes," presented at the IEEE Int. Congr. Internet Things (ICIOT), 2017.

[110] A. Tewari and B. B. Gupta, "Cryptanalysis of a novel ultra-lightweight mutual authentication protocol for IoT devices using RFID tags," *J. Supercomput.*, vol. 73, no. 3, pp. 1085–1102, Mar. 2017. doi: 10.1007/s11227-016-1849-x.

[111] Information Society Technology. *Automated Validation of Internet Security Protocols and Applications*. Accessed: Apr. 18, 2019. [Online]. Available: http://www.avispa-project.org

[112] M. Burrows, M. Abadi, and R. Needham, "A logic of authentication," *ACM Trans. Comput. Syst.*, vol. 8, no. 1, pp. 18–36, 1990. doi: 10.1109/TSG.2011.2160661.

[113] D. He, N. Kumar, and N. Chilamkurti, "A secure temporal-credential-based mutual authentication and key agreement scheme with pseudo identity for wireless sensor networks," *Inf. Sci.*, vol. 321, pp. 263–277, Nov. 2015. doi: 10.1016/j.ins.2015.02.010.

[114] M. N. Abadi and A. D. Gordon, "A calculus for cryptographic protocols: The Spi calculus," *Inf. Comput.*, vol. 148, no. 1, pp. 1–70, Jan. 1999. doi: 10.1006/inco.1998.2740.

[115] B. Blanchet, V. Cheval, X. Allamigeon, and B. Smyth. (2010). *ProVerif: Cryptographic Protocol Verifier in the Formal Model*. [Online]. Available: http://prosecco.gforge.inria.fr/personal/bblanche/proverif

[116] M. Abdalla, P.-A. Fouque, and D. Pointcheval, "Password-based authenticated key exchange in the three-party setting," in *Public Key Cryptography—PKC*. Berlin, Heidelberg: Springer, 2005, pp. 65–84.

[117] K. Xue, P. Hong, and C. Ma, "A lightweight dynamic pseudonym identity based authentication and key agreement protocol without verification tables for multi-server architecture," *J. Comput. Syst. Sci.*, vol. 80, no. 1, pp. 195–206, 2014.

[118] M.-C. Chuang and M. C. Chen, "An anonymous multi-server authenticated key agreement scheme based on trust computing using smart cards and biometrics," *Expert Syst. Appl.*, vol. 41, no. 4, pp. 1411–1418, Mar. 2014.

[119] D. He, N. Kumar, J.-H. Lee, and R. S. Sherratt, "Enhanced three-factor security protocol for consumer USB mass storage devices," *IEEE Trans. Consum. Electron.*, vol. 60, no. 1, pp. 30–37, Feb. 2014.

[120] 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. doi: 10.1016/j.ins.2015.02.010.

[121] R. Amin and G. Biswas, "A secure light weight scheme for user authentication and key agreement in multi-gateway based wireless sensor networks," *Ad Hoc Netw.*, vol. 36, pp. 58–80, Jan. 2016.

[122] S. D. Kaul and A. K. Awasthi, "Security enhancement of an improved remote user authentication scheme with key agreement," *Wireless Pers. Commun.*, vol. 89, no. 2, pp. 621–637, Jul. 2016.

[123] W.-B. Hsieh and J.-S. Leu, "A robust user authentication scheme using dynamic identity in wireless sensor networks," *Wireless Pers. Commun.*, vol. 77, no. 2, pp. 979–989, Jul. 2014.

[124] Y.-H. An, "Security improvements of dynamic ID-based remote user authentication scheme with session key agreement," in *Proc. 15th Int. Conf. Adv. Commun. Technol. (ICACT)*, Jan. 2013, pp. 1072–1076.

[125] J.-S. Chou, C.-H. Huang, Y.-S. Huang, and Y. Chen, "Efficient two-pass anonymous identity authentication using smart card," *IACR Cryptol. ePrint Arch.*, vol. 2013, p. 402, Mar. 2013.

[126] Y.-F. Chang, W.-L. Tai, and H.-C. Chang, "Untraceable dynamic-identity-based remote user authentication scheme with verifiable password update," *Int. J. Commun. Syst.*, vol. 27, no. 11, pp. 3430–3440, Nov. 2014.

[127] S. Kumari, M. K. Khan, and X. Li, "An improved remote user authentication scheme with key agreement," *Comput. Electr. Eng.*, vol. 40, no. 6, pp. 1997–2012, Aug. 2014.

[128] 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.

[129] H. L. Yeh, T. H. Chen, P. C. Liu, T. H. Kim, and H. W. Wei, "A secured authentication protocol for wireless sensor networks using elliptic curves cryptography," *Sensors*, vol. 11, no. 5, pp. 4767–4779, 2011. doi: 10.3390/s110504767.

[130] M. Turkanovic and M. Holbl, "An improved dynamic password-based user authentication scheme for hierarchical wireless sensor networks," *Elektronika Elektrotechnika*, vol. 19, no. 6, pp. 109–116, 2013.
[131] W. R. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "Energy-efficient communication protocol for wireless microsensor networks," in *Proc. 33rd Annu. Hawaii Int. Conf. Syst. Sci.*, vol. 2, Jan. 2000, p. 10.
[132] H.-C. Jang, H.-C. Lee, and J.-X. Huang, "Optimal energy consumption for wireless sensor networks," in *Proc. 9th Joint Int. Conf. Inf. Sci. (JCIS)*, Oct. 2006, pp. 1–4.
[133] F. Wu, L. Xu, S. Kumari, X. Li, A. K. Das, M. K. Khan, M. Karuppiah, and R. Baliyan, "A novel and provably secure authentication and key agreement scheme with user anonymity for global mobility networks," *Secur. Commun. Netw.*, vol. 9, no. 16, pp. 3527–3542, Nov. 2016.
[134] W. Shi and P. Gong, "A new user authentication protocol for wireless sensor networks using elliptic curves cryptography," *Int. J. Distrib. Sensor Netw.*, vol. 9, no. 4, 2013, Art. no. 730831.
[135] Y. Choi, D. Lee, J. Kim, J. Jung, J. Nam, and D. Won, "Security enhanced user authentication protocol for wireless sensor networks using elliptic curves cryptography," *Sensors*, vol. 14, no. 6, pp. 10081–10106, 2014.
[136] J. Yang, J. Park, H. Lee, K. Ren, and K. Kim, "Mutual authentication protocol for low-cost RFID," in *Proc. WRLC*, 2005, pp. 17–24.
[137] S. Kaur and P. Khandnor, "A survey on two-factor user authentication schemes in wireless sensor networks," presented at the IEEE Int. Advance Comput. Conf., New York, NY, USA, 2015.

TARAK NANDY (M'19) was born in Kolkata, West Bengal, India, in 1986. He received the B.Tech. and M.Tech. degrees in computer science and engineering from the Maulana Abul Kalam Azad University of Technology (formerly West Bengal University of Technology), Kolkata, India, in 2012. He is currently pursuing the Ph.D. degree in computer science with the University of Malaya, Kuala Lumpur, Malaysia.

From 2012 to 2014, he was an Assistant professor in computer science and engineering with the Narula Institute of Technology, Kolkata. He pursued research in ISI, Kolkata. Since 2014, he has been an Associate Professor with the Information Technology Department, Maldives Business School, Male', Maldives. He is the author of many articles. His research interests include the IoT, authentication, security, cluster and classification, wireless networks, vehicular networks, machine learning, and deep learning.

MOHD YAMANI IDNA BIN IDRIS received the Ph.D. degree in electrical engineering. He has vast experience in research. He is currently an Associate Professor with the Faculty of Computer Science and Information Technology, University of Malaya. His expertise is in the area of security systems, sensor networks, and signal/image processing.

RAFIDAH MD NOOR received the BIT degree from University Utara Malaysia, in 1998, the M.Sc. degree in computer science from Universiti Teknologi Malaysia, in 2000, and the Ph.D. degree in computing from Lancaster University, U.K., in 2010. She is currently an Associate Professor with the Department of Computer System and Technology, Faculty of Computer Science and Information Technology, University of Malaya, and the Director of the Centre of Mobile Cloud Computing Research, which focuses on high impact research. She has performed nearly RM 665 606.00 for High-Impact Research, Ministry of Education Grant, and other research grants from the University of Malaya and public sectors. She has supervised more than 30 postgraduate students within five years. She has published more than 50 journals in Science Citation Index Expanded Non-Science Citation Index, proceeding articles published in international/national conferences, and a few book chapters. Her research is related to a field of transportation systems in computer science research domain, including vehicular networks, wireless networks, network mobility, quality of service, and the Internet of Things.

MISS LAIHA MAT KIAH received the B.Sc. degree (Hons.) in computer science from the University of Malaya, in 1997, and the M.Sc. and Ph.D. degrees from Royal Holloway, University of London, U.K., in 1998 and 2007, respectively. She joined the Faculty of Computer Science and Information Technology, University of Malaya, Malaysia, as a Tutor, in 1997. She was appointed as a Lecturer, in 2001. She is currently a Full Professor with the Department of Computer System and Technology, Faculty of Computer Science and Information Technology, University of Malaya. Since 2008, she has been actively doing research, particularly in the security area of computing and networking. Her current research interests include cybersecurity, the IoT, and cryptography. Amongst of her research grants were a High-Impact Research Grant by the Ministry of Higher Education, Malaysia, in 2012, for a duration of four years, working on secure framework for electronic medical records, and an eScience Grant by the Ministry of Science, Technology and Innovation, in 2013, for a duration of three years, working on Secure Group Communication for Critical National Information Infrastructure (CNII).

LAU SIAN LUN received the B.Eng. degree (Hons.) in electronics and telecommunications from Universiti Malaysia Sarawak, Malaysia, the M.Sc. degree in electrical communication engineering from Universität Kassel, Germany, in 2004, and the Dr. Ing. degree from Universität Kassel, Germany, in 2011.

Since 2004, he has been a Full-Time Researcher with the University of Kassel. He has contributed and managed various German national as well as EU-funded projects, such as the EU FP6 MobiLife, the ITEA S4ALL, the BMBF MATRIX, and the EU FP7 SEAM4US. In February 2013, he returned to his home country and took up the Head of the Department position with the Department of Computing and Information Systems, Sunway University. He continues to be involved in active research and has published over 50 publications in conferences, workshops, book chapters, as well as journals. His research interests include ubiquitous computing, sustainable smart city, context-awareness, and applied machine learning.

NOR BADRUL ANNUAR JUMA'AT (SM'18) received the B.Comp.Sc. degree (Hons.) in management information system and the M.Comp.Sc. degree from the University of Malaya, Kuala Lumpur, Malaysia, and the Ph.D. degree from the University of Plymouth, U.K. His research interests include intrusion detection systems (intrusion detection systems, intrusion response systems, security event and incident management, digital forensics, network security), high-speed networks (switching, routing, IPv6, multicast), management information systems (E-thesis, library systems, online systems).

ISMAIL AHMEDY received the B.Sc. degree in computer science from University Teknologi Malaysia, in 2006, and the Ph.D. degree in wireless networks system specializing in wireless sensor networks in the routing system from the Universiti Teknologi Malaysia. After completing his study, he has been granted a full scholarship to pursue his studies in master's degree, where he receives the M.Sc. degree in computer science from The University of Queensland, Australia. He has been a Senior Lecturer with the Department of Computer System and Technology, Faculty of Computer Science and Information Technology, University of Malaya, since 2007. His current research interests are the Internet-of-Things, wireless sensor networks, optimization algorithm, and mobile computing.

NORJIHAN ABDUL GHANI received the BIT degree from Universiti Utara Malaysia, the MIT degree in information technology from Universiti Kebangsaan Malaysia, and the Ph.D. degree from Universiti Teknologi Malaysia. She teaches with the Department of Information Systems, University of Malaya. Her research interests include database (database security and privacy), digital image processing systems (image retrieval), data security (information security and privacy), information system security, authentication systems (access control), database security (access control), and data security (personal data collection).

SANANDA BHATTACHARYYA received the B.Tech. degree in information technology from MCKVIE, Kolkata, India, and the M.Tech. degree in computer science and engineering from the Narula Institute of Technology, Kolkata, India, in 2012.

She has served as an Assistant Professor with the Greater Kolkata College of Engineering and Management, Kolkata, India, in 2015. She is currently an Ad-Hoc Faculty with the Information Technology Department, Maldives Business School, Male', Maldives. Her areas of interests are in network security, cryptography, data security, and steganography.