BULGARIAN ACADEMY OF SCIENCES

CYBERNETICS AND INFORMATION TECHNOLOGIES • Volume **21**, No 3
Sofia • 2021 Print ISSN: 1311-9702; Online ISSN: 1314-4081
DOI: 10.2478/cait-2021-0029

A Review on Privacy Requirements and Application Layer Security in Internet of Things (IoT)

K. Swapna Sudha, N. Jeyanthi

School of Information Technology and Engineering, VIT, Vellore Campus, Vellore 632 014, Tamilnadu, India
E-mails: swapanak41@gmail.com njeyanthi@vit.ac.in

***Abstract**: Internet of Things (IoT) is the predominant emerging technology that targets on facilitating interconnection of internet-enabled resources. IoT applications concentrate on automating different tasks that facilitate physical objects to act autonomously without any human interventions. The emerging and current IoT applications are determined to be highly significant for improving the degree of efficiency, comfort and automation for its users. Any kind of security breach on the system will directly influences the life of the humans In this paper, a comprehensive review on Privacy requirements and application layer Security in Internet of Things (IoT) is presented for exploring the possible security issues in IoT that could be launched over the individual layers of IoT architecture. This review explores different challenges of classical security solutions that are related to authentication, key management and cryptographic solutions.It also presents the details of existing access control and device authentication schemes with their pros and cons.*

***Keywords**: Internet of Things (IoT), Security threats, Access control, Smart authentication, IoT applications, Cyber-attacks.*

1. Introduction

The predominant technology of Internet of Things (IoT) was fundamentally anticipated in the year 1999 for the purpose of apprehending the data exchanging and inter communication among the physical devices [1]. The immense utilization of IoT in the real time world also invited a number of different security vulnerabilities and issues, thereby making the security solutions more imperative in this context [2]. The term “Internet of Things” (IoT) was first coined by Kevin Ashton. In the recent days, a exclusive change in the pattern of the users has been visualized due to the heterogeneous characteristics of smart devices used in the IoT applications [3]. For instance, business process management, industrial manufacturing process, smart living, e-Education, food monitoring, e-Education, smart manufacturing, smart health, quick transport, smart cities, smart agriculature, water shimmering and smart home management [4]. Fig. 1 presents the complete view of the possible applications that could be delivered through the utilization IoT devices.

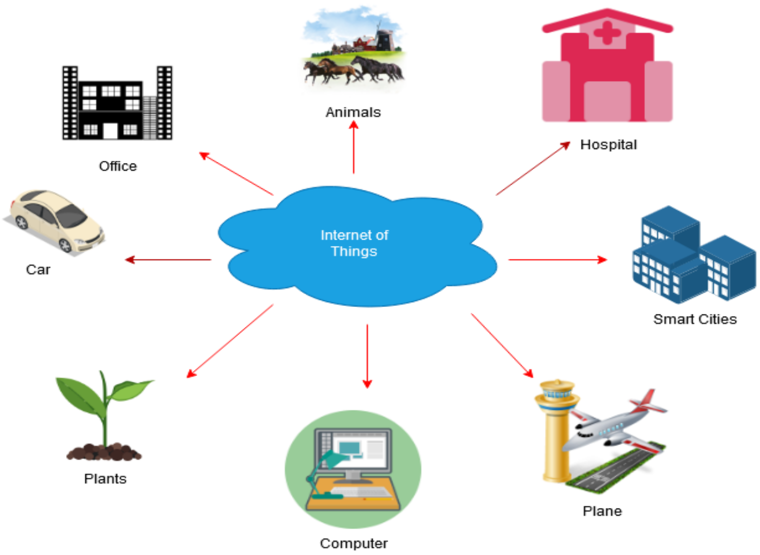

Fig. 1. Core applications of IoT

These IoT applications enable the technology, electronic equipments, phone like emebbed products, vehicles and other possible electronic devices to be monitored and controlled through the Internet based on actuators and sensor nodes that are wired or wirelessly connected [5]. Any person at any instant of time has the possibility of connecting with physical objects at distance locations or remote places through the path or the network [6]. IoT refers to the connectivity of the computers and different types of physical devices that need to cooperate with minimum degree of human interface in order to exchange data with the complementary devices connected on the Internet [7]. The popular definition of IoT propounded in 2012 by the International Telecommunications Union (ITU) stated that, “It is a global infrastructure developed for the information society in order to attain advanced services through virtual or physical things based on the existing and emerging communication technologies and interoperable information” [8]. Another definition given by Internet Architecture Board (IAB) stated that, Internet of Things is considered as a potential trend in which considerable number of embedded equipments that implements communication services that are provisioned by the internet protocols [9]. In IoT applications, smart equipments are considered to be deployed throughout the surroundings which are not operated directly by the humans [10]. These smart devices exist in the vehicles, buildings, and the suitable places of IoT environment implementation. The other significant definitions of IoT are explained as follows. Malaniet al. [11] defined IoT as a suitable environment that permits physical equipments and people to be connected in any place at any time without any intermediate devices through any service and internet. Li et al. [12] commented that the interconnections among the actuating and sensing devices aims at facilitating an indispensable potential that aids in sharing potential information in the heterogeneous platforms based on the utilization of a generic model, which is designed with traditional operating characteristic that enables the operations of innovative applications. Atzori and other authors also defined IoT as the significant interactive communication environment that helps in collaborating among different IoT smart objects based on the interface made possible between mobile phones, sensors, Radio-Frequency IDentification (RFID), and actuators in order to establish a common goal. In earlier days, IoT is considered as the communication of machine-to-machine, which refers to the interaction of two machines without the habitual participation of human through wireless and wired communication [14]. This IoT environment is determined to use two peer points for the objective of information exchange in the system. It provides an ad hoc scenario that transfers information among several physical objects which has the capability of self mentored, self-formed through the incorporation of Radio frequency identification, Zig Bee, Wireless sensor network, etc., for achieving effective communication [15].

The remaining sections of the paper are organized as follows. Section 2 presents the comprehensive functional model of IoTSecurity Architectrure with the major security challenges and requirements of IoT. Section 3 demonstrates the three different categories of the existing authentical protocols proposed for implemeting security in IoT environments. In addition, Section 4 details on the different IoT authentication approaches proposed for establishing security in IoT.

2. Basic architecture of IoT

The IoT architecture is defined as the network constructed through the interconnection of different devices associated with the retial, business and home environments in order to achieve potential and relaible communication [16]. This IoT architecture comprises of four significant layers that includes, i) Perception Layer, ii) Network Layer, iii) Support Layer, iv) Application Layer, and v) Business Layer [17] portrayed in Fig. 2.

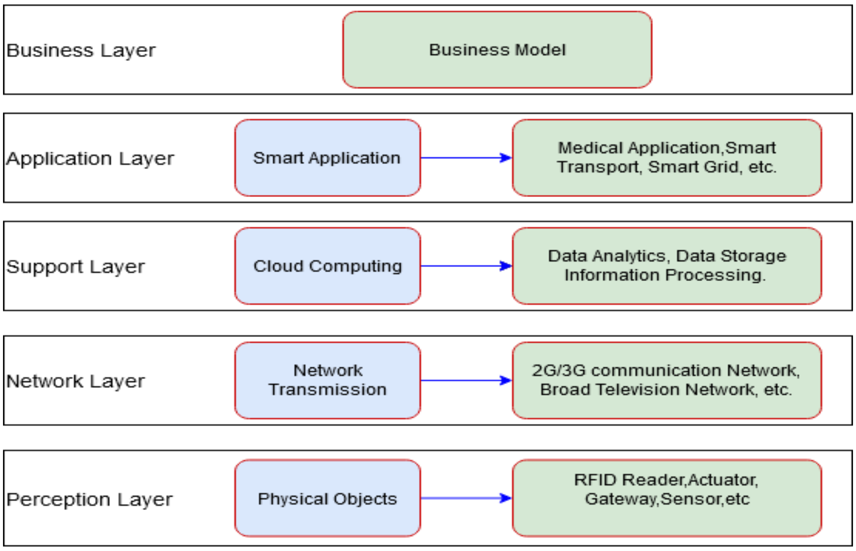
Business Layer
Business Model
Application Layer
Smart Application
Medical Application,Smart Transport, Smart Grid, etc.
Support Layer
Cloud Computing
Data Analytics, Data Storage Information Processing.
Network Layer
Network Transmission
2G/3G communication Network, Broad Television Network, etc.
Perception Layer
Physical Objects
RFID Reader,Actuator, Gateway,Sensor,etc

Fig. 2. The primitive architecture of IoT

i) Perception Layer. This perception layer comprises of different categories of data sensors such as barcodes, RFID and different other sensor equipments that can be used for constructing a network for communication [18]. This layer derives the major characteristics and potentialities of the tagging, nano and intelligent embedded technology [19]. The core objective of the layer concentrates on the process of identifying unique objects that aids in sensing information from the real world with the help of the monitoring sensors. It is responsible for collecting data through the incorporation of diversified equipments such as RFID tags, smart cards and sensor networks. It also possess the feature of broad sensing that could be achieved with the RFID system for deriving information from the monitoring equipments any where and any time [20]. In addition, each and every electronic tags possess a unique identifier named the Electronic Product Code (EPC), which is considered as the unique searchable ID allocated for each physical target. Moreover, comprehensive view of the attacks at the perception layers are now included through Table 1.

Table. 1. Comprehensive view of the Perception Layer Protocols

Issues or attacks	Explanation	Countermeasures
Unauthorized access to tags	Access to tags by someone without authentication	Secure data exchange protocol
Tag Cloning	Intercepting dataflow between tags	OTP synchronization tag and back end
Eavesdropping	Interrupting the packages of data exchange over HTTP	RFI private authentication protocol, RWP, AFMAP
Spoofing	Broadcasting fake information by creating the illusion of valid IP	Message authentication Filtering, SSL authentication
RF Jamming	Preventing the data exchange by jamming frequencies	Using narrow bandwidth and dynamic reconfiguration

ii) Network Layer. The network layer completely concentrates on the process of collecting information from the perception layer to any specific system that are capable for information processing with the help of mobile network, Internet and the other existing communication networks [21]. This information processing networks comprises of closed IP data networks, fixed telephone networks, 2G/3G communications networks, broad television networks, optical fiber communication networks and WSNs. The layer is liable for any kind of information transfer happening between the information processing system and the sensor equipments [22]. Moreover, comprehensive view of the attacks at the network layers are now included through Table 2.

In addition to the aforementioned attacks, middleware security issues such as Node tampering, DoS attack, Jamming, Non-permission to access, Session attacks, Malcious intruders, and Data attacks, etc., are also considered to hurdle the performance of the network layer in IoT.

Table 2. Comprehensive view of the attacks at the network layers

Issues or attacks	Explanation	Countermeasures
Sybil Attack	Creating multiple identities for a single node resulting in fake information	Douceur's Approach (Trusted certification)
Sinkhole Attack (Message digest Algorithm)	Making a particular node look powerful and rerouting data flow towards it	Message digest algorithm
Sleep (Deprivation Attack)	Keeping nodes awake resulting in battery drain	Random vote, Round Robin Scheme
Denial of Service Attack	Making massive non-legitimate requests to create a service unavailable to the general user	Load balancing
Malicious code injection	Compromising node by Injecting malicious program	Signature and anomaly-based approach
Man-in-the-Middle Attack	The attacker modifies the information between two Parties without their knowledge	Mutual Authentication and Tamper Detection

iii) Support Layer. The support layer includes different information processing systems that automate events through the derivation of data processing results and links associated with the database. It is responsible for providing storing potentialities to the data that are collected from the sensor equipments [23]. It is highly service-oriented and plays an indispensable role in facilitating significant services among the connected services. It is very close to the applications and it is the preferable area for the researchers to insert them into the layer of the application.

iv) Application Layer. The application layer completely focusses on the process of delivering potential services to the end customers. For example, it is capable for providing acceleration to the vehicles and provide accurate location of the vehicle at any point of time [24]. This application layer also includes the wide use of protocols such as MQTT (Message Queue Telemetry Transport), AMQP (Advanced Message Queuing Protocol), DDS (Data Distribution Service), Application layer incorporates CoAP (Constrained Application Protocol) and XMPP (Extensible Messaging and Presence Protocol) protocols for attaining its objective [25]. The possible application domains that could be benifitted by the application layer are Quick-witted HealthCare intelligence, Smart Factory, Intelligent Transport, Smart Grid and Smart Home, etc. Table 3 presents the comprehensive view of the attacks that could be possibly launched in the application layer.

Table 3. Comprehensive view of the attacks at the application layer

Issues or attacks	Explanation	Countermeasures
HTTP Flood Attack	These attacks generally targeting on HTTP are volumetric in nature as they frequently utilize a botnet for launching an attack	Source authentication, mutual authentication and homomorphic encryption schemes
DNS Flood	The malicious attacker attempts to overhear a specific DNS server or servers with the objective to control their activity and overpowering server assets in the network	Authetication of the source node and the intermediate nodes that forwards the packet in the network
Identity Theft Attack	The identity theft attack targets either the IoT user or IoT devices for the purpose of extracting information associated with the device IP, device identifier, version of device firmware and the credentials of devices	Provision of physical security, two party and three paty authentication
Attacks over Wi-Fi/Ethernet IEEE802.11	The attacker concentrates on launching attack over all IoT devices that are equipped with WiFi hardware and internal bluetooth associated with the IP and device identifier	Periodic analysis of IoT devices, frequent change in IoT device credentials and continuous monitoring
Man in the Middle Attacks	The attacker initially captures the first message and triggers the group discussion pretending as if the attacker is a significant part of the legal cooperation process	Probe packet exploration, Pseudonym-based certificates, trusted party authentication and source authentication
Botnet/ Thingbots	This botnet is a system of malicious node that work as a framework for gaining control over the network and dessiminating malware in a remote manner	Two party authentication, Pseudonym-based certificates and antijamming injection strategies
Denial of Service	The attackers gets the control of the data traffic stream through infrastructure or device connection	Pseudonym-based certificates, trusted party authentication and source authentication
Malware Attacks	It is launched by the malware which is specially injected with suspicious and malicious instructions for destroying or gaining control over the device	Continous monitoring, exploration of packet fields propgated into the network, mutual authentication

v) Business layer. Business layer also termed as the management layer is capable of handling complete set of segments for services that could be provided by the IoT. It included different flowcharts, models and individual graphs through the amount of data aggregated from the application layer. It has also potential in making potential analytics and effective decisions for the purpose of big data investigation [26].

2.1. Security challenges of IoT

The IoT domain faces different security challenges such as, i) Interoperability, ii) Durability, iii) Resource constraints, iv) Data volumes, v) Privacy protection,

vi) Scalability and vii) Autonomic control during the process of their implementation in the application environment [27].

i) Interoperability. Interoperability is a significant issue when not having the adequate knowledge of the system technical specifications which is completely utilized for interconnecting the systems or components with one another in the network systems of IoT [28].

ii) Durability. The IoT devices are existing on the side of the end users and they are generally deployed in extreme situations and environments such as shipping, under sea water, and harbour management systems [29]. They are highly capable in defending against the absolute temperature, humidity, and vibration. In this context, the networks should maintain connectivity and this must be carried on properly without any kind of interruptions.

iii) Resource constraints. The resource constraints in the IoT domain is a major issue and emerging as a complicated one, since resource is inadequate in some of the components such as CPU, Storage capacity, bandwidth and power required for establishing the security system setup [30]. The aforementioned resource constraints are also responsible for implementing different categories of encrypting algorithms with the objective of enhancing the security measures in the field of IoT.

iv) Data volumes. IoT systems can occupy large amounts of data for the purpose of utilizing the communication channels to provide different types of applications [31].

v) Privacy protection. IoT systems consist of numerous number of RFID systems, thereby the need arises to provide different types of authentication mechanisms [32]. At this juncture, the internal objects are given access to the communication channels and they can take the data for modification of the sensed data.

vi) Scalability. IoT emerges as the predominant model in the present days, since new systems are added frequently into the IoT network, such that current networking of the IoT domain has the capability of processing the new networks [33].

vii) Autonomic control. In the autonomic computing of IoT, the systems are responsible for concluding decisions automatically based with the intelligence and optimizing the status according to the conditions [34]. However, different types of mechanisms have been propounded for controlling the management, configuring, protecting, and optimizing the system automatically, such that it gets adapted in different forms of the implementation environment.

2.2. Security requirements of IoT

The basic security requirements necessitated in the architecture of IoT is portrayed as follows.

Confidentiality. Data confidentiality requires the protection of data using specific encryption techniques and mechanisms to prevent data disclosure and any unauthorized access to IoT equipment and devices [35]. This service is designed to protect sensitive information from the unauthorised users and restricts them from entering the networks.

Authenticity and Authorization. It enables the system to keep the IoT Network safe by providing access only to the authorised users to gain control over the protected resources [36]. The resources may include networks, data bases, computer systems, and other network-based services. Primarily it is used to validate the user identity and also used to determine the levels of client privileges on the different types of resources in the IoT Network.

Integrity. Data integrity refers to safe guarding valuable and sensitive information from the cyber criminals. Several things affect data integrity, for example, server downtime. The Cyclic Redundancy Check (CRC) is a way to ensure data integrity and detect message encryption errors by adding a fixed-length value to detect network errors in IoT [37]. The system should improve mainly the trustworthiness of data over the network, and it also maintains accuracy and consistency.

Availability. Data availability is crucial in IoT and provides guarantees to the users to have access to the security and reliability of available data. An IoT system needs to provide a backup of vital information to prevent data loss. Some attacks cause harm related to data availability, such as Denial-of-Service (DoS) and Distributed-Denial of Services (DDoS) attacks [38]. The IoT Network should be made available in all the times irrespective of the system failures or any hardware or software failures. The bandwidth should be provided by predicting the bottlenecks.

2.3. Overview of security attacks

The attackers in the IoT environment are capable to accesses the possible vulnerabilities in order to exploit each and every layer in the architecture. The security attacks focus on the process of gaining access over the aspects of authentication, confidentiality, integrity, and other security services [39]. The systems weaknesses act as the loophole for compromising security at each of the specific layers. The several types of attacks that could be launched over the IoT architecture are:

i. Spoofing/Altering/Replay Routing,

ii. Denial of Service (DoS): Distributed Denial of Service (DDoS) and Ordinary DoS,

iii. Sybil attack,

iv. Low-end and High-end device class attacks based on device property,

v. Passive and Active attacks based on access level,

vi. Internal and external attacks based on adversary location,

vii. Physical and Logical attacks based on strategy,

viii. Interruption based on Information Damage Level,

ix. Eavesdropping, Alteration, Fabrication, Message Replay, Man-in-the-middle,

x. Host-based: User-compromise, Software-compromise, Hardware-compromise,

xi. Deviation from protocol and Protocol disruption.

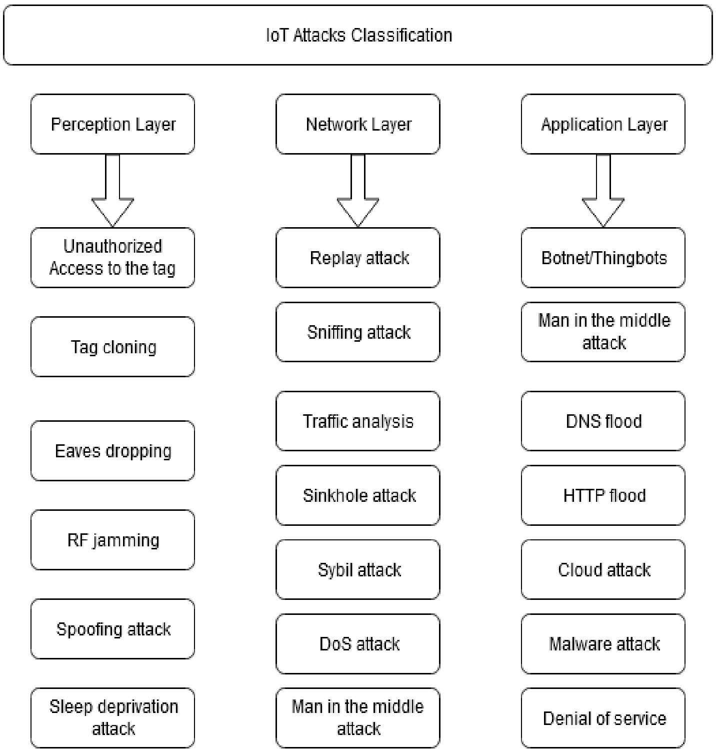

Fig. 3. Different kinds of IoT attacks launched over the IoT architecture

The subsequent section details some of the common security issues that need to be handled in the layers of IoT. It also presents the diversified number of application layer protocols developed for IoT with a comprehensive picture of the countermeasures designed for handling them.

2.4. Security issues in application layer

The application layer of IoT incorporates different significant devices that plays an anchor role in predominant decision making processes. However, the significant devices of the application layer are more vulnerable leading to a number of security issues in the IoT architecture [40]. Further, the attackers in the application layer are likely to destroy the privacy through a known vulnerability (SQL injection, cross site scripting and buffer overflow, unauthorized access of permission and error configuarion (simple and guessable password) .The various kinds of attacks that are launched over the Application layer and are considered as the threat to the IoT environment are detailed as follows:

- **HTTP Flood Attack.** It is a kind of Distributed Denial of Service (DDoS) attack in which the attacker exploits the legitimate POST or HTTP GET applications for attacking a specific application or the web server. This attacks that generally targets on HTTP are volumetric in nature, since they frequently utilize a botnet for launching an attack. For instance, a collection of Internet-related PCs that forms a zombie armed force can launch a HTTP flood attack in which each individual entity is capable for assuming pernicious control for maximum probability of exploitation with the aid of Trojan Horse like malware. On the other hand, the HTTP floods never utilize the reflection systems, spoofing and deformed packets in its form of refine layer attack However, it completely relies on least amplitude of transmission compared to diversified attacks that bring down the performance of the server.

- **DNS Flood.** It is also a type of Distributed Denial of Service (DDoS) attack in which the attacker targets on one or more Domain Name System (DNS) servers that exist in a particular zone for preventing the user from determining the location of asset records in that specified zones and sub-zones [41]. In this DNS attack, the malicious attacker attempts to overhear a specific DNS server or servers with the objective to control their activity, hindering the capacity of the servers and overpowering server assets in the network.
- **Identity Theft Attack.** It is the most common attack that can be launched to each and every smart device user due to his/her negligence or careless behaviour during the physical safekeeping of the interconnected those smart devices integrated in the IoT environment [42]. The major target of the identity theft attack is either the IoT user or IoT devices for the purpose of extracting information associated with the device IP, device identifier, version of device firmware and the credentials of devices. This attack may be launched over the information such that includes the details of the user account and user-related smart application that are generally exchanged among the entities interacting in IoT. Further, this identity theft attack belongs to the common cyber attack, which is launched over the intelligent IoT application devices, mobile devices and smart devices. This attack could further emerge into its aggressive form for bypassing user authentication, stealing of user-related bank accounts and permanent blocking of user devices.
- **Attacks over Wi-Fi/Ethernet IEEE802.11.** This type of attack completely concentrates on launching attack over any IoT devices that are equipped with WiFi hardware and internal bluetooth associated with the IP and device identifier. This attack is generally launched in the network, since WPA or WPA2 are the standard security schemes that are considered to be highly susceptible to cyber attacks.
- **Man in the Middle Attacks.** It is a specific type of attack in which the interceptor or the aggressor attempts to interfere in the process of information interchange which is facilitated between the gadgets and any two trusted frameworks. In this attack, the attacker initially captures the first message and triggers the group discussion pretending as if the attacker is a significant part of the legal cooperation process [43]. This man in the middle attack mainly targets on the integrity of the communication parties and actual communication setup established between them. It is generally launched over smart vehicles and smart TVs that are empowered with web availability in order to work on with some specific working frameworks.
- **Botnet/Thingbots.** It is a specific kind of attack launched by the botnet, which is a system of malicious nodes that are integrated together as a framework for gaining control over the network and disseminating malware in a remote manner [44]. The botnets are generally command and control servers that are controlled by the botnet administrators for exploiting private data, misusing internet data and managing the account information. On the other hand, Thingbots consist of a diversified number

of gadgets that are interconnected with one another. The interconnected entities that are controlled by the thingbots are portable workstations, tablets, PCs and cell phones.

- **Denial of Service.** It is the most common attack that is launched in the IoT application, since most of the IoT devices being vulnerable to the attackers are low-end devices. In this DoS attack, the attackers gets the control of the data traffic stream through infrastructure or device connection. In this DoS attack, huge volume of network packets are generated for targeting the nodes that are existing in the application that causes real time service interrupt.
- **Malware Attacks.** This significant attack is traditionally launched by the malware, which is specially injected with suspicious and malicious instructions in order to destroy the device or gain control over the device [45]. This malware attack is launched through a USB device, since some of the manufactures who manufacture the components of IoT inherently facilitate USB hubs. This kind of malware attack has the potential of directly injecting malicious code into the machine either directly or indirectly inserted by the web server, since the application and devices can send and receive commands through the web server. This malware attack is frequently launched in smart refrigerators, smart TVs that operate on some specific operating systems. In addition, this malware attacks pose threats over the availabaility of the resources and services that could be potentially facilitated by the IoT authentication environment.

3. Standard protocols of the IoT architecture

The potential performance of the IoT architecture depends on the protocols such as HTTP, XMPP, MQTT, DDS, Advanced Message Queuing Protocol (AMQP) and Constrained Application Protocol (CoAP) in the application layer [46].

i) Hypertext Transfer Protocol (HTTP). HTTP forms the foundation of the data communication facilities of the world wide web, since it is an application protocol which pertains to the charateristics of hypermedia information systems' collaborative and distributed properties [47]. It has been developed within the Internet protocol suite framework. The definition of HTTP protocol inherits the merits of the reliable and commonly used transport layer protocol named TCP. However, HTTP also possesses the option of utilizing the benefits of the unreliable User Datagram Protocol (UDP), for instance in the development of the Simple Service Discovery Protocol (SSDP). The resources are localized and identified in the network through the use of specialized Uniform Resource Identifier (URI) and uniform resource locators (URLs).

ii) EXtensible Messaging and Presence Protocol (XMPP). EXtensible Messaging and Presence Protocol (XMPP) is a instant message standard that supports voice, telepresence, video calling and multi-party chatting [48]. This XMPP protocol has been developed by Jabber open source community for supporting spam free, secure, open and decentralized message exhanges among the nodes under interaction. It permits users to interact with one another by sending and receveing instant infomarion on the Internet, independent to the utilized operating system. It permits the applications of instant messages to attain compatibility, end-to-end encryption, hop-by-hop communication, privacy estimation, access control and authentication. The potential and diversified features of XMPP makes it highly suitable and preferable by majority of the instant messaging applications that are highly correlating within the scope of IoT. It is considered to secure and permit the use of new applications that could be deployed over the top of the core protocols. It aids in connecting a server to the client through the inclusion of XML stream of stanzas. XML stream of stanzas highlights a piece of code which is partitioned into the components of message, presence and information query. Message stanzs is responsibe for determining identifiers, destination addresses and source addresses assoacited with the entities of XMPP which is associated with the method of push that aids in data retrieval. This message stanza fills the gap between the body fields and the subject with the message contents and title. The existence of verse notifies and expresses the status of the customers who are authorized in a specific instant of time.

iii) Message Queue Telemetry Protocols (MQTT). MQTT protocol is termed as the transportation of MQ Telemetry. This MQTT is designed and developed as the lightweight and straight forward messaging protocol for subscribing and publishing messages shared with high latency, low bandwidth, restricted devices and unreliable networks [49]. The design principles of MQTT mainly targets on minimizing the processing, the requirements of device resources, and network bandwidth, that tries to guarantee delivery and attain reliability.

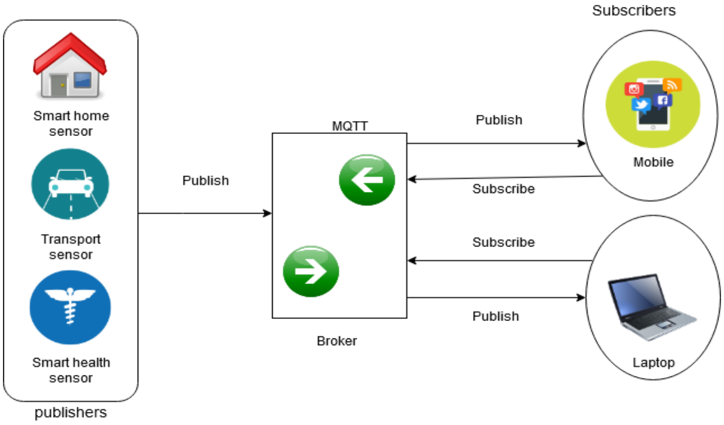

Fig. 4. Operation of MQTT protocol in the smart applications

Fig. 4 presents the operation of MQTT protocol in the IoT architecture. The MQTT protocol utilizes four major components such as broker, topic, publisher and subscriber. Broker is the first component that plays the role of a server for accomplishing the task of data monitoring between the sensors and remote devices. It facilitates the devices to interact automatically with the other restricted nodes based on potential Quality of Services (QoS). The Topic component of MQTT permits the tools and sensors for generating information based on some specific application under monitoring. The component of publisher is responsible for facilitating the devices to publish messages in the IoT environment. Finally, the subsribers are capable of receiving and sending the messages depending on the requirement generated by the clients [50]. Further, publisher is used for sensing the data to the broker such that it accepts different ways to receive data from the broker.

iv) Data Distcribution Service (DDS) Protocol. Data Distcribution Service (DDS) protocol is a data centric and PKI-oriented certificate authentication protocol developed through the publish, subscribe and brokerless properties. It is more significant and reliable protocol developed for attaining maximized QoS well adopted for IoT object and mobile-to-mobile communication. This DDS protocol developed by Object Management Group (OMG) supports mulicasting and token strategy induced by the resistive properties of secure DSA and RSA algorithms. It uses as device to device relational data model that helps in direct data transmission to the node that uses the communication of the bus. The architecture of DDS protocol is double layered with Data-Local Reconstruction Layer (DLRL) and Data-Subscribe Publish-Subscribe (DCPS) for disseminating tha data to the subscribers on demand. Between the two layers of DDS, DLRL is considered to the optional interfacing layer to DCPS. DDS protocol enables to configure reliability, multicasting, QoS control and pervasive redundancy and handles the issue of data management and data distribution. It is also a QoS-based standard and data centric protocol specially developed for middlware platform in order to facilitate applications that communicate with one another by information publication that subscribes potential services.

v) Advanced Message Queuing Protocol (AMQP). This AMQP protocol has evolved by John O'Hara as a software layer protocol well suited for message-assisted middleware scenario. It is the open standard used for exchanging messages among organizations and applications [51]. It is responsible for interconnecting systems, captures business processes based on the required information, and propagates the instructions that facilitate their objectives in a reliable forward direction. This protocol derives the benefits of warranty primitive messages such as exactly as soon as shipping, at least one and at-most-one for facilitating reliable verbal exchanges. It comprises of fast as well as hard components that are responsible for saving and routing the message internal to a broker carrier with a collection of policies that integrates the cooperating components in a reliable manner. This protocol facilitates the option of engaging and talking to the leader through the utilization of patron programs that are inherent with the AMQP model. This AMQP protocol includes three additives such as exchange, message queues and binding for linking into the processing chains that enable the server to construct the required potentiality. Exchange additive is responsible for receiving messages from the publisher-based programs in order to route them towards message queues. The message queue is responsible for storing the messages unless they are completely processed through the utilized client software. In addition, binding primitive bundles the connection between the message queue and its corresponding change in state.

vi) Constrained Application Protocol (CoAP). CoAP is a specialized internet application protocol defined in the RFC standard 7252 for restricted devices [52]. This protocol permits the cooperation of restricted devices named nodes for utilizing similar type of protocols used for communicating with the broader Internet. It is designed for the devices to utilize them when they are operating on the same network. This CoAP protocol utilized UDP protocol for its lightweight implementation as presented in Fig. 5. It also inherits the Restful architecture, which is very similar in characteristics to the HTTP protocol. This protocol is specifically designed for IoT systems that majorly concentrate on the HTTP protocols.

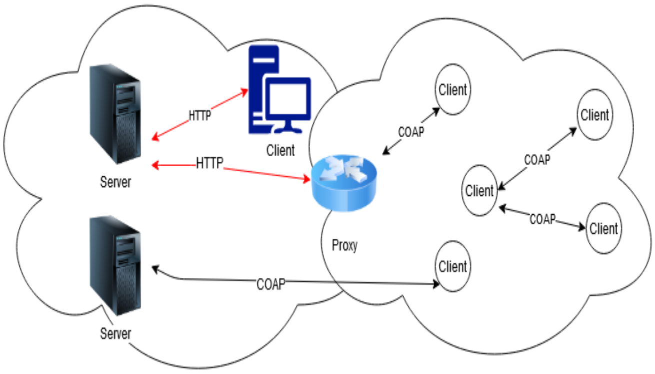

Fig. 5. Operation of CoAP

This CoAP protocol supports low power computation and tiny devices to improve their communication potentialities that enhance the degree of RESTful interactions [53]. This CoAP protocol consists of two significant sub-layers such as messaging sub-layer and the request/response sub-layer. The former layer is responsible for facilitating reliable communication and detecting duplications on the UDP transport layer that uses the features of exponential backoff. This adoption in CoAP is included as it does not support a built-in error recovery mechanism. The latter layer termed as the request/response sub-layer has been developed for handling REST communications. In addition, CoAP inherits four message categories that are designated as confirmable, non-confirmable, reset, and acknowledgement. However, CoAP protocol's reliability is completely established through the hybridization of confirmable and non-confirmable messages.

Table 4. Comprehensive view of the protocols developed for IoT environment

Protocols	Year	Architecture	Abstraction	Header size	QoS	Transport protocol	Security
HTTP	1997	Master/Slave	Request/Response	Not defined	No	TCP	TLS/SSL
XMPP	1999	Master/Slave	Request/Response or Publish/Subscribe	Not defined	No	TCP/IP	TLS & SASL
MQTT	1999	Master/Broke	Publish/Subscribe	2 Bytes	Yes	TCP	SSl/TLS
DDS	2001	No Broke	Real Time Data CentricPublish/Subscribe	Not defined	Yes	TCP/UDP	No security
AMQP	2003	Master/Broke or Master/Slave	Request/Response OrPublish/Subscribe	8 Bytes	Yes	SCTP, TCP	SASL, SSl/TLS
CoAP	2010	Master/Slave OrMaster/Broke	Request/Response OrPublish/Subscribe	4 Bytes	Yes	SCTP, UDP	IPSec, DTLS

4. IoT authentication approaches for establishing security in IoT

This section depicts the hierarchy of IoT authentication approaches propounded using different conditions chosen based on main characteristics and similarities of the schemes [54]. Further, authentication can be implemented at the individual three layers of IoT architecture that enforces diversity with respect to the authentication techniques. The comprehensive view of the key distribution schemes are presented in Fig. 5.

4.1. Factor of authentication

i) Identity-based authentication. It is the information presented by a subject to another entity in order to achieve its authentication by itself. The identity-based authentication schemes can be single or the hybridization of asymmetric, symmetric and hash cryptographic algorithms.

ii) Context-based authentication. It is the authentication scheme that relies completely on physical and behavioural information [55]. The physical biometric information depends on the traits of an individual such as retinal scans, hand geometry and fingerprints. On the other hand, behavioural information pertains to the behavioural traits of an individual person such as voice identifier, gait analysis, and keystroke analysis.

iii) Token-based authentication. This authentication scheme completely depends on the device or the user authority determined based on the utilized token of authentication generally constructed by servers associated with open ID and OAuth2 protocol [56].

iv) Non-Token based authentication. It includes the utilization of credential such as username and password which is generated every time when there is chance of exchanging data in the network.

Moreover, the authentication architectures independent of their distributed or centralized characteristics, are categorized into flat and hierarchical architecture [80]. The authentication is considered to be flat, when procedure of authentication is not including any hierarchical process. On the other hand, the architecture is considered to be hierarchical, when it is capable of handling the procedure of authentication by utilizing a multi-level arhictecture.

4.2. IoT layers used in implementing authentication process

The layers over which the procedures of authentication is implemented are perception layer, network layer and application layer [59]. The perception layer is responsible for collecting, processing and digitizing the information that is determined by the data perceived from the edge nodes existing in the IoT platform [60]. The network layer is useful for receiving the data perceived from the perception layer and the strategy of processing it [86]. In addition, the application layer is responsible for data reception from the network layer for providing service request from the users [61].

4.3. Authentication schemes for smart home applications

A Smart home authentication scheme-based on strong password was proposed by Vaidya et al. [63] for facilitating efficient and robust secure access in the environment of digitial home network. This strong password-based authentication scheme was proposed with the modules of lightweight computation that inherits the potentiality of hash-chaining approach and hashed one-time password integrated with the technology of low cost smart card. This authentication scheme was proposed for satisfying diversified number of security essentialities that incorporated stolen smart card attack. It was enhanced with the significance of forward secrecy and functional requirements that does not require time synchronization and verification table. The formal verification proved that this authentication scheme is capable enough in ensuring superior robustness with predominant security charateristcis compared to the state of art representative schemes in the literature. An smart home authentication scheme that used smart card with one-time password was proposed by Jeong, Chung and Choo [65] for attaining maximized security in the IoT environment. This one-time password approach examined the smart cards, certificates, password and biometric traits considered for user authentication before they are employed in the home devices that may posses low performance and efficiency. This authentication approach completely utilized the merits of one-time password protocol for satisfying the security essentials of the home networks, such that it could be converted in a well adaptable ideal solution. It incorporated the merits of one-way hash function as they necessitated only low computation that inherited only a simple degree of operations during authentication. It was considered to permit the users with the real time privileges that provides good implementation and superior control over the home networks. A remote smart home authentication scheme was proposed by Wazid et al. [67] for achieving predominant verification of users under the impact of resource constrained smart devices. It was proposed with the merits of symmetric one-way hash functions, bitwise XOR operations and one-way hash functions for authenticating the resource constrained smart devices used by the smart home users. The security investigation of this authentication conducted with the renown Real-Or-Random (ROR) model confirmed its predominance over the existing works of the literature. The formal and informal security verification of this user authentication scheme done using AVIPSA tool and broadly-accepted Automated Validation of Internet Security Protocols confirmed their superiority in user authencation on par with the existing protocols considered for authentication.

Further, an user authentication scheme with strong security was proposed by Santoso and Vun [68] for attaining maximized interaction with high consideration emphasized on the user comfort associated with system operation. This secure scheme inherited the merits of asymmetric Elliptic Curve Cryptography (ECC) to initate authentications in the event of system operation. This smart home authenctication is implemented with the classical wifi network, which is completely integrated with the AllJoyn framework. This ECC-based user authentication approach utilized the systems’ center node for initiating the process of system configuration. It was responsible for authenticating different parties of communication in the IoT environment and also established as a suitable medium for system control, access and user setup through the execution of suitable application program that runs of Android based mobile devices. Another ECC-based anonymous authentication was proposed by Shuai et al. [70] for verifying the credentials of the smart card users. This anonymous approach completely prevents the utilization of verification table that are used for the purpose of authentication. It was propounded with random number methodology which is capable in preventing the issue of clock synchronization. It is also considered to be highly resistive against replay attack. The formal verification and heurictic investigation of this anonymous approach conducted rigorously proved to prevent most possible attack of an IoT environment with necessitated security properties. It was confirmed to facilitate a suitable tradeoff between efficiency and security, compared to the most of the existing authentication schemes implemented in the most realistic scenarios. A lightweight anonymous secure framework was proposed by Shayan, Naser and Hossein [72] for securing smart home environments that are highly vulnerable to attacks imposed over user devices. This secure framework facilitated the devices (data and identity) with unlinkability, anonymity and key aggrement. The computation overhead of this secure framework was considered to be signficantly improved compared to the user secure framework. This secure framework was also identified to be highly fault tolerant as the system operation does not terminate, even when the smart home owners device is either compromised or attacked.

Furthermore, a three-level Kerberos authentication approach was proposed by Gaikwad, Gabhane and Golait [73] was implementing effective and efficient user authentication in smart home systems. This Kerberos-based authentication approach was propounded with the merits of low cost and ecofriendlyness. This authentication scheme was enhanced for easing out the task of home automation by making the user to potentially monitor and control the home devices from any remote place through the Internet. It inherited the modules of GPRS, embedded systems and RF for making the system more robust and efficient. The formal and informal analysis of this Kerberos-based authentication approach was confirmed to be more secure than the currently avalilable smart home systems. Then, a signcryption based user authentication scheme was proposed by Ashibani and Mahmoud [75] for satisfying the requirements of confidentiality and integrity under user credential verification process. This signcryption based user authentication scheme integrated the benefits of signature and encryption schemes. It was proposed as an identity-based signcryption technique that provides maximized security and fault tolerance during the process of authentication. This significant scheme was confirmed to facilitate better confidentiality and integrity with increased capability to resist possible attacks that are possible during the process of communication.

In addition, ECC-based authentication scheme with robust session key was proposed by Naoui, Elhdhili and Saidane [78] for remote smart card user verification. It was developed as a lightweight approach for adapting to be capable in handling the restricted resources of the constrained smart devices with the help of the gateway that supports the generation of session key which need to be transmitted to the sensor device. The formal analysis of this ECC-based authentication scheme conducted using Scyther tool proved its resistance to mobile devices stolen attack, denial of service attack, impersonation attack and privileged-insider attack. Then, an integrated transaction history and context awareness-based user authentication scheme was proposed by Fakroon et al. [79] for achieving maximized resistance to attacks that are possible in smart home environment. This integrated authentication strategy offered two significant merits, in which one prevented the management of any verification table and another concentrated on resolving the issue of clock synchronization. It was considered to reduce computational cost and communication overhead compared to the related schemes in the literature. This authentication methodology was identified to be robust during the conduction of informal analysis and formal analysis attained through the Burrows-Abadi-Needham (BAN) logic. The model verification of this authentication scheme was performed using AVIPSA tool and the internet security protocols also proved their predominance in satisfying the security requirements of the smart home environment.

In order to evaluate the effectiveness of the proposed authentication algorithms, the following evaluation parameters [72-81] defined below can be used.

Communication overhead. The number of packets (bytes) used for establishing and attaining the communication between different entities of IoT environment in the presence of possibly launched attack.

Computation cost. It is the cumulative amount of time incurred for encrypting and decrypting the data in the process of data aggregation if IoT is applied.

Data aggregation decryption cost. It is the amount of time incurred for decrypting the data during the application of privacy preserving fully homomorphic encryption scheme in the event of data aggregation in IoT.

Blind signature generation cost. It is the amount of time incurred for the generation of blind generation during the implementation of authentication schemes in IoT.

Attack detected. It represents the binary value that describes whether the attack has been detected (1) or not (0).

Detection counter. It defines the number of sensors within the network that detected an attack (excluding the attacked sensor).

Min detection time. It is defined as the minimum detection time until the first sensor detected an attack within the network.

MW detection time. It is defined as the mean way detection time until at least half of the sensors connected to the sensor under attack detected the attack.

Max detection time. It is defined as the maximum detection time until the last sensor detected an attack within the network.

Isolated attack factor. This factor is considered as the binary value describing whether the attack has been correctly isolated (1) or not (0).

The time incurred for mitigating attack. It is considered as the estimated time required for detecting and isolating the possible attacks in IoT environment.

5. Conclusion

This paper depicts the detailed view of security challenges that are possible in different layers of IoT. It presents the investigation of diversified number of authentication protocols and authentication schemes that contribute to identifying potential requirements and open challenges that can be taken into consideration by the developers and researchers during the development of new authentication approaches specifically targeting on IoT networks and their applications. This review has highlighted diversified kinds of attacks that are possible in the perception layer, network layer and application layer of IoT environment. This review has presented different authentication schemes that are proposed for user device verification with their merits. The shortcomings in the literature that could be considered for future research are listed as follows.

a) The majority of the existing schemes have not included the merits of hash tree, even though the computation complexity could be significantly handled during the process of authentication.

b) Most of the state of art user authentication schemes proposed for smart home environment has not utilized the merits of chaotic map (when biometric traits considered as images are used). which is considered to be one of the potential image encryption schemes that introduces maximized randomness in the data being shared during authentication.

c) The existing schemes fail to use the currently popular fully homomorphic encryption in the user authentication environment.

d) The current scheme in the literature has not derived the benefits of verifiable computation techniques that could contribute to robust user device authentication process with added lightweight capability.

e) The user authentication schemes available in the literature are considered to still have a room of improvement in terms of communication overhead and computation overhead involved during the authentication process.

The aforementioned limitations of the literature may be considered for the formulation of any new smart home authentication schemes in order to achieve predominance in the process of implementation.

References

1. Neshenko, N., E. Bou-Harb, J. Crichigno, G. Kaddoum, N. Ghani. Demystifying IoT Security: An Exhaustive Survey on IoT Vulnerabilities and a First Empirical Look on Internet-Scale IoT Exploitations. – IEEE Communications Surveys & Tutorials, Vol. **21**, Third Quarter 2019, No 3, pp. 2702-2733.
2. Shin, D., K. Yun, J. Kim, P. V. Astillo, J. Kim, I. You. A Security Protocol for Route Optimization in DMM-Based Smart Home IoT Networks. – IEEE Access, Vol. **7**, 2019, pp. 142531-142550.
3. Meneghello, F., M. Calore, D. Zucchetto, M. Polese, A. Zanella. IoT: Internet of Threats? A Survey of Practical Security Vulnerabilities in Real IoT Devices. – IEEE Internet of Things Journal, Vol. **6**, October 2019, No 5, pp. 8182-8201.
4. Hassija, V., V. Chamola, V. Saxena, D. Jain, P. Goyal, B. Sikdar. A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures. – IEEE Access, Vol. **7**, 2019, pp. 82721-82743.
5. Choi, C., J. Choi. Ontology-Based Security Context Reasoning for Power IoT-Cloud Security Service. – IEEE Access, Vol. **7**, 2019, pp. 110510-110517.

6. Samaila, M. G., J. B. F. Sequeiros, T. Simões, M. M. Freire, P. R. M. Inácio. IoT-HarPSecA: A Framework and Roadmap for Secure Design and Development of Devices and Applications in the IoT Space. – IEEE Access, Vol. **8**, 2020, pp. 16462-16494.
7. Frustaci, M., P. Pace, G. Aloi, G. Fortino. Evaluating Critical Security Issues of the IoT World: Present and Future Challenges. – IEEE Internet of Things Journal, Vol. **5**, August 2018, No 4, pp. 2483-2495.
8. Ingham, M., J. Marchang, D. Bhowmik. IoT Security Vulnerabilities and Predictive Signal Jamming Attack Analysis in LoRaWAN. – IET Information Security, Vol. **14**, 2020, No 4, pp. 368-379.
9. Wang, D., B. Bai, K. Lei, W. Zhao, Y. Yang, Z. Han. Enhancing Information Security via Physical Layer Approaches in Heterogeneous IoT with Multiple Access Mobile Edge Computing in Smart City. – IEEE Access, Vol. **7**, 2019, pp. 54508-54521.
10. Lounis, K., M. Zulkernine. Attacks and Defenses in Short-Range Wireless Technologies for IoT. – IEEE Access, Vol. **8**, 2020, pp. 88892-88932.
11. Malani, S., J. Srinivas, A. K. Das, K. Srinathan, M. Jo. Certificate-Based Anonymous Device Access Control Scheme for IoT Environment. – IEEE Internet of Things Journal, Vol. **6**, December 2019, No 6, pp. 9762-9773.
12. Li, X., Q. Wang, X. Lan, X. Chen, N. Zhang, D. Chen. Enhancing Cloud-Based IoT Security through Trustworthy Cloud Service: An Integration of Security and Reputation Approach. – IEEE Access, Vol. **7**, 2019, pp. 9368-9383.
13. Asplund, M., S. Nadjm-Tehrani. Attitudes and Perceptions of IoT Security in Critical Societal Services. – IEEE Access, Vol. **4**, 2016, pp. 2130-2138.
14. Wazid, M., A. K. Das, V. Odelu, N. Kumar, M. Conti, M. Jo. Design of Secure User Authenticated Key Management Protocol for Generic IoT Networks. – IEEE Internet of Things Journal, Vol. **5**, February 2018, No 1, pp. 269-282.
15. Farris, T. T., Y. Khettab, J. Song. A Survey on Emerging SDN and NFV Security Mechanisms for IoT Systems. – IEEE Communications Surveys & Tutorials, Vol. **21**, First Quarter 2019, No 1, pp. 812-837.
16. Zarca, M., J. B. Bernabe, A. Skarmeta, J. M. Alcaraz Calero. Virtual IoT HoneyNets to Mitigate Cyberattacks in SDN/NFV-Enabled IoT Networks. – IEEE Journal on Selected Areas in Communications, Vol. **38**, June 2020, No 6, pp. 1262-1277.
17. Yi, M., X. Xu, L. Xu. An Intelligent Communication Warning Vulnerability Detection Algorithm Based on IoT Technology. – IEEE Access, Vol. **7**, 2019, pp. 164803-164814.
18. Zhou, W., Y. Jia, A. Peng, Y. Zhang, P. Liu. The Effect of IoT New Features on Security and Privacy: New Threats, Existing Solutions, and Challenges Yet to Be Solved. – IEEE Internet of Things Journal, Vol. **6**, April 2019, No 2, pp. 1606-1616.
19. Shin, D., V. Sharma, J. Kim, S. Kwon, I. You. Secure and Efficient Protocol for Route Optimization in PMIPv6-Based Smart Home IoT Networks. – IEEE Access, Vol. **5**, 2017, pp. 11100-11117.
20. Sathyadevan, S., K. Achuthan, R. Doss, L. Pan. Protean Authentication Scheme – A Time-Bound Dynamic KeyGen Authentication Technique for IoT Edge Nodes in Outdoor Deployments. – IEEE Access, Vol. **7**, 2019, pp. 92419-92435.
21. Mukherjee. Physical-Layer Security in the Internet of Things: Sensing and Communication Confidentiality Under Resource Constraints. – Proceedings of the IEEE, Vol. **103**, October 2015, No 10, pp. 1747-1761.
22. Amato, F., V. Casola, G. Cozzolino, A. De Benedictis, F. Moscato. Exploiting Workflow Languages and Semantics for Validation of Security Policies in IoT Composite Services. – IEEE Internet of Things Journal, Vol. **7**, May 2020, No 5, pp. 4655-4665.
23. Oh, M., S. Lee, Y. Kang, D. Choi. Wireless Transceiver Aided Run-Time Secret Key Extraction for IoT Device Security. – IEEE Transactions on Consumer Electronics, Vol. **66**, February 2020, No 1, pp. 11-21.
24. Mandal, S., B. Bera, A. K. Sutrala, A. K. Das, K. R. Choo, Y. Park. Certificateless-Signcryption-Based Three-Factor User Access Control Scheme for IoT Environment. – IEEE Internet of Things Journal, Vol. **7**, April 2020, No 4, pp. 3184-3197.

25. Tedeschi, P., S. Sciancalepore, A. Eliyan, R. Di Pietro. LiKe: Lightweight Certificateless Key Agreement for Secure IoT Communications. – IEEE Internet of Things Journal, Vol. **7**, January 2020, No 1, pp. 621-638.
26. Ahanger, T. A., A. Aljumah. Internet of Things: A Comprehensive Study of Security Issues and Defense Mechanisms. – IEEE Access, Vol. **7**, 2019, pp. 11020-11028.
27. Li, C., Z. Qin, E. Novak, Q. Li. Securing SDN Infrastructure of IoT-Fog Networks from MitM Attacks. – IEEE Internet of Things Journal, Vol. **4**, October 2017, No 5, pp. 1156-1164.
28. Thangavelu, V., D. M. Divakaran, R. Sairam, S. S. Bhunia, M. Gurusamy. DEFT: A Distributed IoT Fingerprinting Technique. – IEEE Internet of Things Journal, Vol. **6**, February 2019, No 1, pp. 940-952.
29. Zhao, B., P. Zhao, P. Fan. ePUF: A Lightweight Double Identity Verification in IoT. – Tsinghua Science and Technology, Vol. **25**, October 2020, No 5, pp. 625-635.
30. Verma, L. P., M. Kumar. An IoT Based Congestion Control Algorithm. – Internet of Things, Vol. **9**, 2020, No 1, pp. 100-157.
31. Alshahrani, M., I. Traore, I. Woungang. Anonymous Mutual IoT Interdevice Authentication and Key Agreement Scheme Based on the ZigBee Technique. – Internet of Things, Vol. **7**, 2019, No 2, 100061.
32. Fakroon, M., M. Alshahrani, F. Gebali, I. Traore. Secure Remote Anonymous User Authentication Scheme for Smart Home Environment. – Internet of Things, Vol. **9**, 2020, No 1, 100158.
33. Rizvi, S., R. Orr, A. Cox, P. Ashokkumar, M. R. Rizvi. Identifying the Attack Surface for IoT Network. – Internet of Things, Vol. **9**, 2020, No 1, 100162.
34. Enokido, T., M. Takizawa. The Redundant Energy Consumption Laxity Based Algorithm to Perform Computation Processes for IoT Services. – Internet of Things, Vol. **9**, 2020, No 1, 100165.
35. Ghosh, A., A. Raha, A. Mukherjee. Energy-Efficient IoT-Health Monitoring System Using Approximate Computing. – Internet of Things, Vol. **9**, 2020, No 2, 100166.
36. Fallis, E., P. Spachos, S. Gregori. A Power-Efficient Audio Acquisition System for Smart City Applications. – Internet of Things, Vol. **9**, 2020, No 1, 100155.
37. Karanja, E. M., S. Masupe, M. G. Jeffrey. Analysis of Internet of Things Malware Using Image Texture Features and Machine Learning Techniques. – Internet of Things, Vol. **9**, 2020, No 2, 100153.
38. Shukla, R. M., S. Sengupta. COP: An Integrated Communication, Optimization, and Prediction Unit for Smart Plug-in Electric Vehicle Charging. – Internet of Things, Vol. **9**, 2020, 100148.
39. Aftab, N., S. A. Zaidi, D. McLernon. Scalability Analysis of Multiple Lora Gateways Using Stochastic Geometry. – Internet of Things, Vol. **9**, 2020, No 1, 100132.
40. Nizzi, F., T. Pecorella, F. Esposito, L. Pierucci, R. Fantacci. IoT Security via Address Shuffling: The Easy Way. – IEEE Internet of Things Journal, Vol. **6**, April 2019, No 2, pp. 3764-3774.
41. Liu, Y., Y. Kuang, Y. Xiao, G. Xu. SDN-Based Data Transfer Security for Internet of Things. – IEEE Internet of Things Journal, Vol. **5**, February 2018, No 1, pp. 257-268.
42. Das, K., M. Wazid, A. R. Yannam, J. J. P. C. Rodrigues, Y. Park. Provably Secure ECC-Based Device Access Control and Key Agreement Protocol for IoT Environment. – IEEE Access, Vol. **7**, 2019, pp. 55382-55397.
43. Hao, P., X. Wang, W. Shen. A Collaborative PHY-Aided Technique for End-to-End IoT Device Authentication. – IEEE Access, Vol. **6**, 2018, pp. 42279-42293.
44. Badii, C., P. Bellini, A. Difino, P. Nesi. Smart City IoT Platform Respecting GDPR Privacy and Security Aspects. – IEEE Access, Vol. **8**, 2020, pp. 23601-23623.
45. Chaabouni, N., M. Mosbah, A. Zemmari, C. Sauvignac, P. Faruki. Network Intrusion Detection for IoT Security Based on Learning Techniques. – IEEE Communications Surveys & Tutorials, Vol. **21**, Third Quarter 2019, No 3, pp. 2671-2701.
46. Hwang, J., A. Aziz, N. Sung, A. Ahmad, F. Le Gall, J. Song. AUTOCON-IoT: Automated and Scalable Online Conformance Testing for IoT Applications. – IEEE Access, Vol. **8**, 2020, pp. 43111-43121.

47. Hafeez, M. Antikainen, A. Y. Ding, S. Tarkoma. IoT-KEEPER: Detecting Malicious IoT Network Activity Using Online Traffic Analysis at the Edge. – IEEE Transactions on Network and Service Management, Vol. **17**, March 2020, No 1, pp. 45-59.

48. Xu, Q., P. Ren, H. Song, Q. Du. Security Enhancement for IoT Communications Exposed to Eavesdroppers with Uncertain Locations. – IEEE Access, Vol. **4**, 2016, pp. 2840-2853.

49. De Hoz Diego, J. D., J. Saldana, J. Fernández-Navajas, J. Ruiz-Mas. IoTsafe, Decoupling Security from Applications for a Safer IoT. – IEEE Access, Vol. **7**, 2019, pp. 29942-29962.

50. Mohsenian-Rad, A. Leon-Garcia. Distributed Internet-Based Load Altering Attacks Against Smart Power Grids. – IEEE Transactions on Smart Grid, Vol. **2**, December 2011, No 4, pp. 667-674.

51. Samarah, S., M. G. Al Zamil, A. F. Aleroud, M. Rawashdeh, M. F. Alhamid, A. Alamri. An Efficient Activity Recognition Framework: Toward Privacy-Sensitive Health Data Sensing. – IEEE Access, Vol. **5**, 2017, pp. 3848-3859.

52. Mosenia, S. Sur-Kolay, A. Raghunathan, N. K. Jha. DISASTER: Dedicated Intelligent Security Attacks on Sensor-Triggered Emergency Responses. – IEEE Transactions on Multi-Scale Computing Systems, Vol. **3**, 1 October-December 2017, No 4, pp. 255-268.

53. Saxena, N., B. J. Choi, R. Lu. Authentication and Authorization Scheme for Various User Roles and Devices in Smart Grid. – IEEE Transactions on Information Forensics and Security, Vol. **11**, May 2016, No 5, pp. 907-921.

54. Gupta, M., M. Abdelsalam, S. Khorsandroo, S. Mittal. Security and Privacy in Smart Farming: Challenges and Opportunities. – IEEE Access, Vol. **8**, 2020, pp. 34564-34584.

55. Koroniotis, N., N. Moustafa, E. Sitnikova. Forensics and Deep Learning Mechanisms for Botnets in Internet of Things: A Survey of Challenges and Solutions. – IEEE Access, Vol. **7**, 2019, pp. 61764-61785.

56. Kong, H., L. Lu, J. Yu, Y. Chen, F. Tang. Continuous Authentication through Finger Gesture Interaction for Smart Homes Using WiFi. – IEEE Transactions on Mobile Computing. DOI: 10.1109/TMC.2020.2994955.

57. Hossain, M., R. Hasan. P-HIP: A Lightweight and Privacy-Aware Host Identity Protocol for Internet of Things. – IEEE Internet of Things Journal. DOI: 10.1109/JIOT.2020.3009024.

58. Bin, Q., C. Ziwen, X. Yong, H. Liang, S. Sheng. Rogue Base Stations Detection for Advanced Metering Infrastructure Based on Signal Strength Clustering. – IEEE Access. DOI: 10.1109/ACCESS.2019.2934222.

59. Zhou, Y., Y. Liu, S. Hu. Smart Home Cyberattack Detection Framework for Sponsor Incentive Attacks. – IEEE Transactions on Smart Grid, Vol. **10**, March 2019, No 2, pp. 1916-1927.

60. Kumar, A. Braeken, A. Gurtov, J. Iinatti, P. H. Ha. Anonymous Secure Framework in Connected Smart Home Environments. – IEEE Transactions on Information Forensics and Security, Vol. **12**, April 2017, No 4, pp. 968-979.

61. Ivanova-Rohling, V. N., N. Rohling. Evaluating Machine Learning Approaches for Discovering Optimal Sets of Projection Operators for Quantum State Tomography of Qubit Systems. – Cybernetics and Information Technologies, Vol. **20**, 2020, No 6, pp. 61-73.

62. Mocrii, D., Y. Chen, P. Musilek. IoT-Based Smart Homes: A Review of System Architecture, Software, Communications, Privacy and Security. – Internet of Things, Vol. **1-2**, 2018, No 2, pp. 81-98.

63. Vaidya, B., J. H. Park, S. Yeo, J. J. Rodrigues. Robust One-Time Password Authentication Scheme Using Smart Card for Home Network Environment. – Computer Communications, Vol. **34**, 2011, No 3, pp. 326-336.

64. Prabadevi, N. Jeyanthi. TSCBA-A Mitigation System for ARP Cache Poisoning Attacks. – Cybernetics and Information Technologies, Vol. **18**, 2018, No 4, pp. 75-93.

65. Jeong, J., M. Y. Chung, H. Choo. Integrated OTP-Based User Authentication Scheme Using Smart Cards in Home Networks. – In: Proc. of 41st Annual Hawaii International Conference on System Sciences (HICSS'08), Waikoloa, HI, 2008, pp. 294-294.

66. Brindha, K., N. Jeyanthi. Secured Document Sharing Using Visual Cryptography in Cloud Data Storage. – Cybernetics and Information Technologies, Vol. **15**, 2015, No 4, pp.111-123.

67. Wazid, M., A. K. Das, V. Odelu, N. Kumar, W. Susilo. Secure Remote User Authenticated Key Establishment Protocol for Smart Home Environment. – IEEE Transactions on Dependable and Secure Computing, Vol. **17**, 1 March-April 2020, No 2, pp. 391-406.

68. Santoso, F. K., N. C. H. Vun. Securing IoT for Smart Home System. – In: Proc. of International Symposium on Consumer Electronics (ISCE'15), Madrid, 2015, pp. 1-2.

69. Srivastava, M., J. Siddiqui, M. A. Ali. A Review of Hashing Based Image Copy Detection Techniques. – Cybernetics and Information Technologies, Vol. **19**, 2019, No 2, pp. 1-27.

70. Shuai, M., N. Yu, H. Wang, L. Xiong. Anonymous Authentication Scheme for Smart Home Environment with Provable Security. – Computers & Security, Vol. **86**, 2019, No 3, pp. 132-146.

71. Prabadevi, B., N. Jeyanthi. Security Solution for ARP Cache Poisoning Attacks in Large Data Center Networks. – Cybernetics and Information Technologies, Vol. **17**, 2017, No 4, pp. 69-86.

72. Shayan, M., M. Naser, G. Hossein. IoT-Based Anonymous Authentication Protocol Using Biometrics in Smart Homes. – In: Proc. of 16th International ISC (Iranian Society of Cryptology) Conference on Information Security and Cryptology (ISCISC'19), Mashhad, Iran, 2019, pp. 114-121.

73. Gaikwad, P. P., J. P. Gabhane, S. S. Golait. 3-Level Secure Kerberos Authentication for Smart Home Systems Using IoT. – In: Proc. of 1st International Conference on Next Generation Computing Technologies (NGCT'15), Dehradun, 2015, pp. 262-268.

74. Usha, S., S. Kuppuswami, M. Karthik. A New Enhanced Authentication Mechanism Using Session Key Agreement Protocol. – Cybernetics and Information Technologies, Vol. **18**, 2018, No 4, pp. 61-74.

75. Ashibani, Y., Q. H. Mahmoud. An Efficient and Secure Scheme for Smart Home Communication Using Identity-Based Signcryption. – In: Proc. of IEEE 36th International Performance Computing and Communications Conference (IPCCC'17), San Diego, CA, 2017, pp. 1-7.

76. Gumusbas, D., T. Yildirim. Offline Signature Identification and Verification Based on Capsule Representations. **–** Cybernetics and Information Technologies, Vol. **20**, 2020, No 5, pp. 60-67.

77. Pencheva, E. N., I. I. Atanasov, V. G. Vladislavov. Mission Critical Messaging Using Multi-Access Edge Computing. – Cybernetics and Information Technologies, Vol. **19**, 2019, No 4, pp. 73-89.

78. Naoui, S., M. H. Elhdhili, L. A. Saidane. Novel Smart Home Authentication Protocol LRP-SHAP. – In: Proc. of IEEE Wireless Communications and Networking Conference (WCNC'19), Marrakesh, Morocco, 2019, pp. 1-6.

79. Fakroon, M., M. Alshahrani, F. Gebali, I. Traore. Secure Remote Anonymous User Authentication Scheme for Smart Home Environment. – Internet of Things, Vol. **9**, 2020, No 3, 100158.

80. Gayathiri, P., B. Poorna. Effective Gene Patterned Association Rule Hiding Algorithm for Privacy Preserving Data Mining on Transactional Database. – Cybernetics and Information Technologies, Vol. **17**, 2017, No 3, pp. 92-108.

81. Patil, D. R., J. B. Patil. Malicious URLs Detection Using Decision Tree Classifiers and Majority Voting Technique. – Cybernetics and Information Technologies, Vol. **18**, 2018, No 1, pp. 11-29.

Received: 27.01.2021; Second Version: 26.05.2021; Accepted: 15.06.2021