International Journal of Software Innovation
Volume 11 • Issue 1

An Outlook Architecture:
Protocols and Challenges in IoT and Future Trends

Kajal Patel, Gujarat Technological University, India*
Mihir Mehta, Gujarat Technological University, India

ABSTRACT

The internet of things (IoT) has recently received much attention due to its revolutionary potential. The internet of things facilitates data interchange in a large number of possible applications, including smart transportation, smart health, smart buildings, and so on. As a result, these application domains can be grouped to form smart life. In response to the IoT's rapid growth, cybercriminals and security professionals are racing to keep up. Billions of connected devices can exchange sensitive information with each other. As a result, securing IoT and protecting users' privacy is a huge concern. A session for communication in a network is established by authenticating and validating the device's identity and checking whether it is a legal device. The IoT technology can be used for various applications only if challenges related to IoT security can be overcome.

KEYWORDS

Communication, Internet of Things, Protocols, Telecommunication, Wireless Sensor Networks (WSN)

INTRODUCTION

In the Internet-of-Things (IoT), various physical devices are connected to the Internet via wireless technologies. The Internet of Things (smart environment) has contributed significantly to the advancement of technology over the last few decades. Wireless Sensor Networks (WSN) are equipped with a digital skin that facilitates data collection by sensor nodes and connects the processed information over the Web to provide a virtual layer to IoT (Santhosh Krishna et al., 2017; Chang-le Zhong et al., 2017; Qian et al., 2018). A system of interactivity should be enabled by energy-constrained sensors, a unique identifier, a communication module, and a storage capacity. As a self-organizing, smart, and self-adaptive network world, it serves in security & emergencies (radiation level, liquid presence, perimeter access control), retail (smart shopping, supply chain control), agriculture (soil monitoring, greenhouse effect), water management (leakage, PH value, water level detection) and smart cities (health monitoring, smart parking), environment (air pollution, forest fire detection) (Jeffry Voas et al., 2018; Mamun et al., 2018).

Although in providing secure and private data transmission these devices can be accessed by hackers, there is a real challenge. Attacks such as offline cryptographic attacks, DoS, unauthorized usage, MITMs, replays, and other threats can all occur on a network (MardianabintiMohamad Noor

DOI: 10.4018/IJSI.315744

*Corresponding Author

et al., 2019). Therefore, it is crucial to provide a standard security solution for the integrity of data and privacy of the user that is adaptable to the dynamic nature of IoT (TarakNandy et al., 2019).

There are currently millions of objects in the IoT that need no human monitoring at the moment. Various vendors make these devices and they communicate with one another over the Internet (Hokeun Kim et al., 2017; Hirofumi Noguchi et al., 2019). It is a scenario where objects, animals, or humans are made smarter through their ability to communicate with each other over the Internet without involving humans or machines with each other.

OVERVIEW OF IOT

Through IoT, physical and cyber worlds are connected by things that participate and share information. In recent years, researchers and organizations have attempted to define IoT. According to (Zhou et al., 2019, IoT is:

The seamless integration of physical objects into information network and where actual things might take part in the economic process as active participants.

IoT is crucial for creating solutions for future problems, according to Kevin Ashton, the creator of the word IoT. He defines the Internet of Things as computers that sense the actual world on their own and for themselves, allowing information about things in the real world to be accessed over the Internet. According to a UN report, a modern concept of accessibility is beginning, in which internet users will number in the billions, and humans will become the minority in terms of data creation and consumption (Tahsien et al., 2020).

A further interesting definition of IoT comes from the ITU's Telecommunication Standardization Sector which adds virtual things to the definition and defines IoT as:

A global platform for the information society that enables advanced services through the interconnection of (physical and virtual) things based on existing and evolving interoperable information and communication technologies.

IBM approaches the IoT in different ways, broadening the idea of IoT to an interconnect system instead of linking specific things, resulting in a smart plant in which things are integrated with advanced devices (Ghani et al., 2019). However, these definitions have one thing in common: IoT refers to the system of interactions between physical objects and the cyber world.

Therefore, IoT is a technology that exists everywhere and enables things to interact with one another (things to things) or with each other (things to people). The Internet of Things could include anything around us or could be found at home such as, cameras, water irrigators, sensors, television, light bulbs, toaster, oven, washing machine, refrigerator home appliances, or perhaps on the streets, for example, Smart traffic signals which interact with smart vehicles providing direction in order to avoid traffic jams and open parking spots (Chikouche et al., 2019). Things like tiny sensors implanted in the body of the patient to monitor various health conditions could be used for remote healthcare monitoring or devices connected to the body like the CGM that monitors sugar levels, however, the application areas of IoT keep expanding (Chuang et al., 2018). The IoT is depicted in Figure 1, and its building blocks are seen in Figure 2.

IoT Characteristics

Here are some basic features of an IoT environment (Melki et al., 2020):

- **Connectivity:** Connectivity is a prominent and necessary characteristic in IoT. Networking allows the objects to communicate with each other and keep them accessible. It also contributes

Figure 1. Overview of IoT

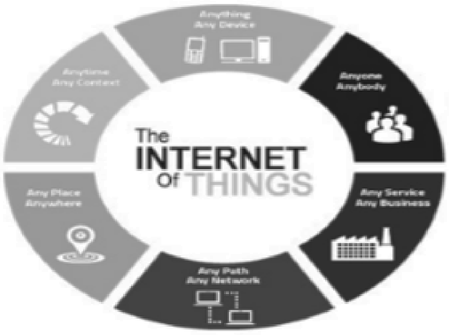
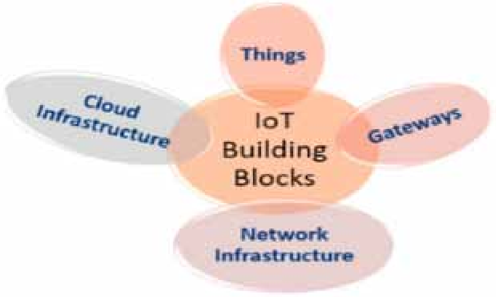


Figure 2. Building blocks of IoT



to compatibility, which is the process of transferring, consuming, and producing data without complexity or conflicts.

- **Heterogeneity:** IoT devices operate on many kinds of platforms and interact with devices in other networks. Because of the heterogeneity of IoT, there is no common security mechanism and handling it properly is difficult. (Panda et al., 2020).
- **Dynamic Environment:** Gathering data from the IoT infrastructure is a vital process, which is accomplished through the use of dynamic changes that occur (disconnected/connected/waking up/sleeping), context (temperature, location, and speed), and the number of its devices (Alladi et al., 2020). As a result, in order for IoT systems to be more efficient and reliable, they must be flexible and scalable.
- **Self-organized Network:** Since IoT networks are dynamic, it is impossible to organize them statistically over the long run. Adaptability is crucial as its environment changes constantly. In the case of mobile devices, it must be taken into account whether they may connect to the network or disconnect from it at any given point in time (Kou et al., 2019).
- **Resources Constraint:** The majority of IoT devices suffer from battery and memory limitations. Algorithms Legacy, as well as security services, should be as lightweight as possible so that IoT devices can operate more efficiently (Liang et al., 2019).
- **Sensing and Intelligence:** Sensor technologies are primarily responsible for IoT environments that capture, measure, and generate information about our complex physical world as well as the ability to connect with it in a brilliant manner on the basis of a combination of computation and algorithms (Hoque et al., 2019).

Iot Applications

It is possible to improve the quality of people's lives and activities using the Internet of Things (IoT) (Chin et al., 2017). Figure 3 depicts one of the IoT architectures typical of the IoT.

Smart Home

Includes a variety of devices (e.g., fire detector, smart lock, baby monitor) that communicate wirelessly at home. A home gateway allows remote access to smart devices at home.

Smart Healthcare

The system collects, transmits, and stores physiological information about patients. Medical sensors, for example, can collect the heart rate of the patient and send it to the server of the hospital for diagnosis and monitoring.

Smart Transportation

Several smart vehicles are available, which can communicate between themselves (vehicle-to-vehicle), (vehicle-to-infrastructure) to the outside stations, and (vehicle-to-pedestrian) to pedestrians over wireless networks. Using a smart car will help you drive safely, efficiently, and efficiently management of traffic status.

Smart Agriculture

Provides micro-climate conditions, soil moisture, irrigation, humidity, and remote control of temperature to give better quality and avoid financial losses. Sensors could be linked to wildlife in an intelligent farming system to track their behaviour and health.

Smart Industry

Industrial IoT (IIoT) is a type of IoT that uses machine-to-machine tools to simplify production processes with minimal human intervention. Industrial IoT aims to provide more reliable and efficient final products by better controlling the manufacturing process, data, and issues.

Smart Retail

Tracks products in warehouses or while traveling. It is possible to track the status of a retail item using sensors. Various smart shopping systems offer intelligent services and will increase the number of customers.

Smart Grid

Monitoring and managing the consumption of electricity is a popular aspect of the Internet of Things. Energy savings are provided, as well as the reduction of power grids problems and failures. Table 1 presents a potential attacks analysis posed by vulnerabilities as well as threats in the environment of IoT.

IoT Architecture Layers

The objects in the system should be linked to one another, which is a major factor of an IoT. System architecture for IoT should support IoT operations, bridging the physical and virtual worlds. Architecture for IoT involves a variety of factors, including processes, communication, network, etc. The operability, scalability, and extensibility of equipment must be taken into consideration when designing IoT architecture. Considering moving objects and the need for real-time interactions, the IoT Architecture should be adaptable so that devices can communicate with one another adaptively and interact with one another. Moreover, IoT should possess heterogeneity and decentralization (Alraja et al., 2019).

Figure 3. IoT System Architecture

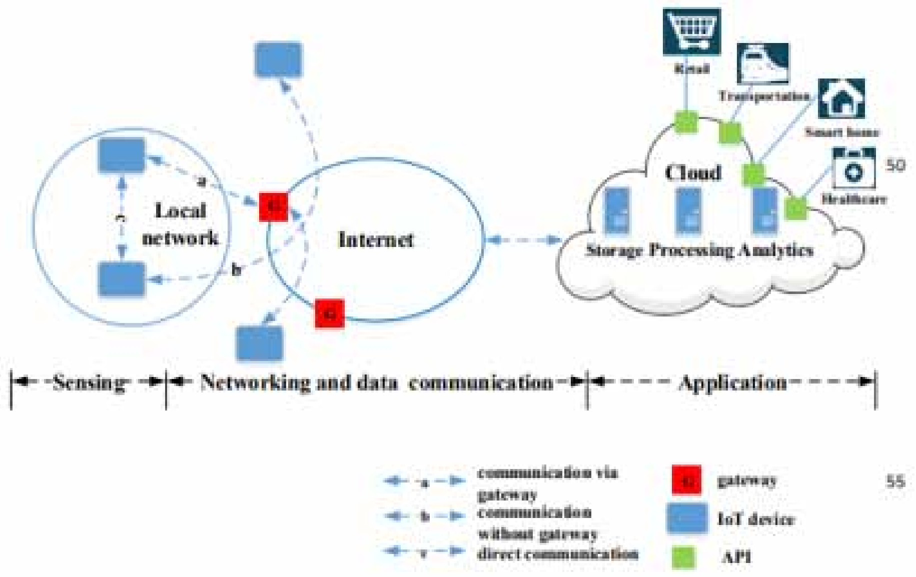


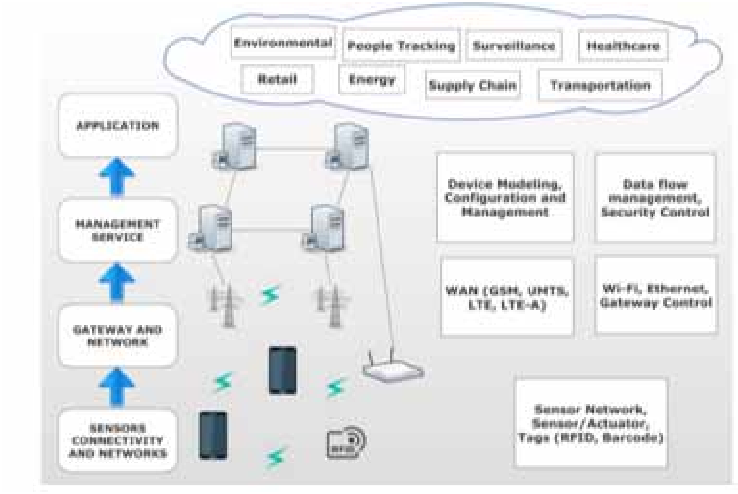
Table 1. Analysis of potential threats to the IoT smart application environment

Group	Features	Benefits	Threats	Vulnerability	Attacks	Confidentiality	Integrity	Authentication	Availability	Non-repudiation
Smart City	Waste Management, Water, Street Lighting and e-governance	Economic development, Faster delivery of service, Better city planning	Smart City DoS, Information manipulating	Fake detection of seismic, Fake detection of floods	Sensors, Mobile application	±	±	±	±	-
Smart grid	Smart meters, Smart Energy	Energy independence, Reliability and Cost savings	Physical security, Customer security	trust between traditional power devices	End points on devices, malicious attacks	±	±	±	±	±
Healthcare	Smart health cards	enhances privacy details and security of patients	Unintentional actions, Insider misuse, loss and Theft	Hacking	cyber attack, Internal attack	±	±	±	-	-
Smart Transportation	Public Transportation, Parking, Traffic control	Easy usage	Smart City DoS	Security plagued	Cyber-attacks	-	-	±	±	±

IoT does not have a standard architecture, though there are a few tentative designs that have three to five layers. In the early days of IoT, most architectures consisted of three layers: application layer, Perception, and middleware as outlined in section 4.

Perception/Sensor Layer: An object in the IoT ecosystem needs to be identified uniquely, which is possible by obtaining information about the object. RFID tags or sensors contribute to this layer.

Figure 4. IoT Architecture


Environmental
People Tracking
Surveillance
Healthcare
Retail
Energy
Supply Chain
Transportation
APPLICATION
MANAGEMENT SERVICE
GATEWAY AND NETWORK
SENSORS CONNECTIVITY AND NETWORKS
Device Modeling, Configuration and Management
Data flow management, Security Control
WAN (GSM, UMTS, LTE, LTE-A)
Wi-Fi, Ethernet, Gateway Control
Sensor Network, Sensor/Actuator, Tags (RFID, Barcode)
RFID

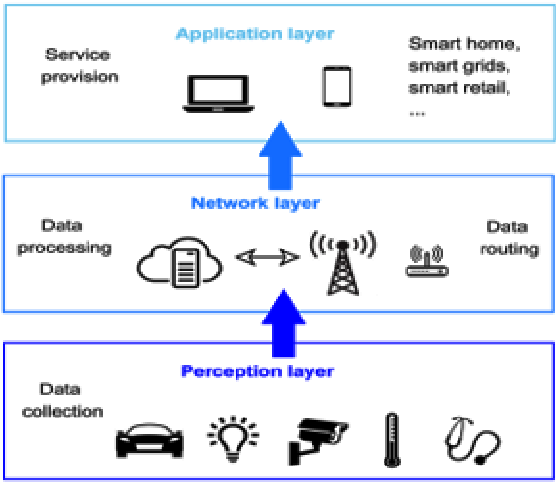
They also transmit and receive information from the device, which is then processed by the upper layers. (Sheron et al., 2020).

Middleware layer: Provides network support and IoT protocol stacks. As in other architectures, this layer consists of two parts: a processing layer for processing data collected by sensors. Another is the transport layer, which is made up of technology like Wi-Fi and Bluetooth. They transmit and receive data from the perception layer. Objects are also assigned IPv6 addressing (Wang et al., 2018).

Application Layer: Here, applications such as health care and smart cities are implemented. This layer could be revealed in two components in some architecture. Firstly, there is the business layer, which provides app management and handles privacy and guarantee. Second, there is an application layer, which differentiates the applications (Esfahani et al., 2017).

IoT architecture in three-layer structure (as shown in Figure 5).

Figure 5. Three Layer Architecture



IoT Challenges

The challenges that IoT faces, such as security, energy supply and many others are diverse and fall into different categories (Khalid et al., 2020):

1. **Authenticating devices:** Devices using sensors and similar objects must follow policies and proxy rules that confirm the sensor has the right to publish its data. Currently, if trust is required for the things, a costly remedy has been used (Lee et al., 2019).
2. **Identification of IoT environment:** Authentication must happen at every layer of IoT. IoT presents a major challenge because it will have a broad range of applications and can be designed in a vast several ways. In a distributed environment, as is the case with IoT, this is more challenging. In a closed environment, this challenge remains the same. Each parameter specifies the key goal of the identifier, like privacy, governance and security. As a result, a global identification reference is needed (Panda et al., 2020).
3. **Data management:** Managing the data is one of the most important problem. The most effective choices for protecting data are cryptographic mechanisms and network protocols, however, these tools are not always possible to implement. As a result, distinct policies should be in place to manage the data, irrespective of the nature of information, but several existing techniques will have to be altered to achieve this (Chuang et al., 2018).
4. **Continuous operation:** IoT applications can be compared to computers since computers are controlled by humans. However, intelligent objects need to be capable of configuring themselves by themselves, adapting to any situation, and also acting independently. Hence, they need sensors to make decisions (Kalyani et al., 2020).
5. **Detection:** Within the context of IoT, the population of things grows in lockstep with the human population, as each person carries multiple devices. These devices should be detected and it should also be known what is happening with them (Kumari et al., 2018).

IOT ARCHITECTURE FOR PRIVACY AND SECURITY

For securing the applications of IoT, we must address security and privacy issues at every layer of the architecture of IoT. All of these problems must be considered and addressed at the very beginning of the project design phase. The architecture of Internet of Things raises the need for appropriate security checks over and after the initial deployment of an overall IoT network (Fan et al., 2020). This section discusses the security issues related to the various layers of the IoT architecture.

Security Problems in Perception Layer

In the layers of perception, the RFID, WSN as well as other kinds of detecting and detection methods are the basic technologies utilized. This layer faces the following types of threats (Wang et al., 2017):

- **Capturing of node:** The nodes at the gateway of the network seem to be more probably to be exploited, which could lead to the sensitive data leakage, risking the entire network's security.
- **Malicious Data and Fake Node:** The opponent incorporates an affected node to the old model, which allows them to spread malicious code and information across the network and infect the entire system.
- **DoS Attack:** DDoS and DoS attacks are the most frequent and serious network attacks. Attacks like these lead to resource depletion on networks and service outages.
- **Replay Attack:** This attack aims to undermine the security and integrity of the system by replaying an earlier message.

Security Problems in Network Layer

Threats to privacy, authenticity, and accessibility must be addressed at the network layer. At this layer, attacks such as network intrusion, DoS/DDoS, man-in-the-middle, and eavesdropping are frequent (Almulhim et al., 2019; Bendavid et al., 2018; Fang et al., 2020):

- **Heterogeneity:** Diverse protocols and technologies make network and security coordination difficult. The system becomes vulnerable as a consequence.
- **Scalability Issues:** The Internet of Things (IoT) includes a wider range of equipment, and also more appliances could join or withdraw at any time at distinct intervals, posing problems such as identity verification, transmission delay, and so on. Depleting resources is also a problem.
- **Data Disclosure:** Adversaries may obtain sensitive information through social engineering. With such a large amount of data being generated, by utilizing certain data extraction techniques, it is simple to retrieve network information.

Security Problems in Application Layer

Various security standards are needed for different applications, making it difficult to secure applications. Here are a few security and privacy concerns (Hong et al., 2020; Soewito et al., 2021): Table 2 illustrates the IoT architecture and Security requirements:

- **Identification of node and Mutual authentication:** Every application has its user set with varying permissions degrees. Consequently, effective authentication schemes must be used to prevent any illegal entry.
- **Information Privacy:** Each communication should be protected by user privacy. Data processing techniques can be vulnerable at times, resulting in data loss and, in the long run, causing significant damage to the system.
- **Managing data:** Massive data collection maximizes the data management complexity and raises the risk of data loss.

Table 2. Summary of the three-layer IoT architecture security conditions

Layer	Security Requirements
Perception	Encryption that isn't too heavy
	Authentication
	Agreement of Key
	Confidentiality
Network	Security the Communication
	Security of router
	Attack Detection
	Key Management
	Authentication
Application	Protection of privacy
	Information Security Management
	Authentication

- **Application-Specific Vulnerabilities:** Some security flaws may be chosen to leave behind as looking to develop systems for an application that are uncertain to the client. In the future, these vulnerabilities may be exploited by an adversary.

WHY AUTHENTICATION?

Confidentiality, Integrity, and Authentication (CIA) are the three most important aspects of any security framework. With the use of encryption, privacy protects data being sent from one party to another. Defending against modification attacks is provided by integrity and verifies that received data is as it is and not changed by an adversary. This can be achieved with message digests and MACs. Authentication verifies the device's identity, i.e., whether the assumed group is guaranteeing that obtained information is not tampered with by an adversary, utilizing features like token, device identity, and so on. In addition to these three concepts, authentication is essential for providing security, as if an unauthorized device is involved in the exchange of communication, it can provide an opportunity to the attackers for easy access to the network and to perform various cyberattacks. For providing a secure IoT solution, it is fundamental to develop an unambiguous and strong authentication method first (Hirofumi Noguchi et al., 2019.).

MOTIVATION

Currently, the Internet of Things is a rapidly developing technology. IoT applications can be found in various fields – Defense, Manufacture, Smart City, Automobile, Health, Agriculture and so on. Automating, monitoring, and controlling various applications can be done via the internet. There will be close to 200 million web-connected devices by 2020, in accordance with a recent report. IoT is an open architecture, which is well known. It is therefore of the utmost importance to provide security to IoT applications today. As discussed in section 1.3, there are various ways to attack IoT. It can be dangerous for the whole network if a single weak link is detected. Thus, IoT benefits society only if it is properly secured and includes the following pillars: Security, Authentication, and especially unambiguous Authentication.

DIFFERENT AUTHENTICATION METHODS

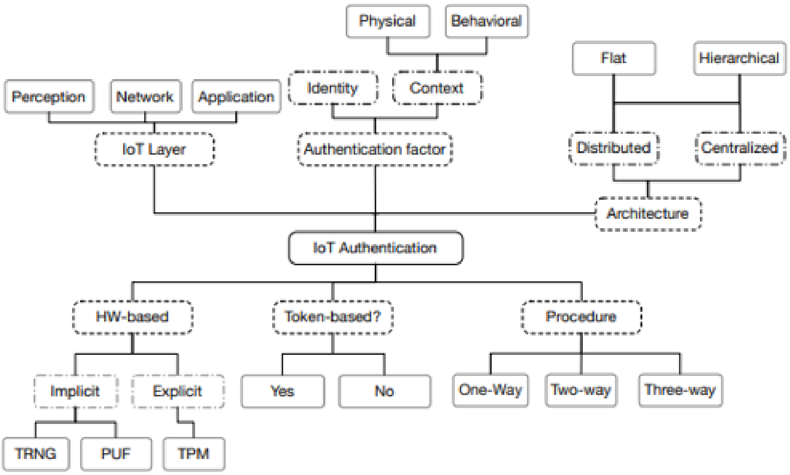
An authentication service verifies that a device or user in the network is who they claim to be. As suspicious equipment that is not legitimate equipment; it is a very important security pillar; it also poses a significant risk to the network and can be vulnerable to attack (Mohammad Wazid et al., 2017). Figure 6 illustrates these criteria.

Identity Based Authentication

One party presents information to another for authentication in this type of authentication algorithm. Various cryptographic algorithms can be combined with this schema, including asymmetric, symmetric, and hashing algorithms. Most of these schemas require a smart card, password, or secret key.

An identity-based cross-domain authentication scheme for the IoT was presented by the authors in (Jia et al., 2020). This framework replaces the traditional certificate of authority with the Blockchain as a decentralized trust pillar and the IB self-authentication algorithm with the traditional PKI authentication algorithm. A decentralized authentication scheme is presented in this paper, which allows the security domain to maintain its independence and initiative. Authentification using Radiofrequency has been presented in (Prosanta Gope et al., 2018) utilizing the Radiofrequency parameter. This method protects against spoofing. It is vulnerable to Interception attacks, MITM attacks. The author in (Yan et al., 2019) presented fine-grained access control, a Function-based Access Control scheme in the Internet

Figure 6. IoT Authentication Schemes



of Things (IoT-FBAC), which uses an Identity-based Encryption (IBE) scheme as a defense against unauthorized access. While the FBAC scheme uses IoT, the operation costs are constant. According to security analysis, IoT-FBAC is a secure procedure, which can prevent over-privileged access. A lightweight identity-based scheme of remote user authentication and key exchange was introduced in (Shafiq et al., 2020) in order to secure internet-connected devices. XOR operations, hash operations and Lightweight elliptic curve cryptography (ECC) are used in the suggested method. Using PyCrypto and Ubuntu, they have examined the effectiveness of their scheme compared with other schemes. Their evaluation indicates that the storage and communication costs of their scheme are trivial. In (Hussain et al., 2021) suggests an identity-based generalized proxy signcryption (IBGPS) scheme for the IIoT that is both lightweight and provably secure. The proposed IBGPS scheme was provably secure in terms of indistinguishability against adaptive chosen ciphertext attack ($IND - IBGPS - CCA$) and existential unforgeable against a possible adaptive chosen message attack ($EUF - IBGPS - CMA$) under Hyperelliptic Curve Decisional Diffie-Hellman problem (HEDHP) and Hyperelliptic Curve Discrete Logarithm problem (HECDLP) in the random oracle model. In (Jiang et al., 2018) presented a methodology for ensuring both of the privacy and confidentiality of a communications network, which is, safeguarding information privacy while preserving user anonymity. The system is based on anonymous identity-based encryption (IBE), ensuring users' security. The scheme was implemented in Java with Java pairing-based cryptography library (JPBC).

Token Based Authentication

As part of this authentication method, a server generates a token, such as in the OAuth2 protocol, which is used in verifying a device or user's identity. This authentication method is based on the token-based OAuth2 protocol.

A token-based security protocol with a tradeoff between energy efficiency and security for IoT devices has been introduced in (Rao et al., 2021). It is essential for IoT systems to support different and large-scale systems, so the protocol is based on the OAuth 2.0 framework. From hardware components to the protocol, the dynamic energy-quality tradeoff is facilitated. An analysis and simulation has been performed on the protocol to assess its security. An authentication algorithm of M2M communication based on the MQTT communication protocol is introduced by the authors in (Dikii et al., 2020), which enables verification of the authenticity of a device without directly transmitting the password. The most widespread method of data security on MQTT is the creation of a secure connection via the TLS protocol.

Physical Unclonable Function

There are several challenges to the Internet of Things, such as energy efficiency, limited computing capability, and limited storage capacity. Consequently, conventional cryptography techniques cannot be used on IoT devices due to a shortage of resources. Cryptographic assets are not stored on PUFs, so the devices provide reliable authentication. The PUF receives an input stream (Challenge) and outputs a stream of bits (Response). This Challenge-Response model is used in PUF authentication. As a result, the component might be guaranteed and validated based on the response to the issue, which the server provides as input.

According to (Zhang et al., 2019), a PUF-based key-sharing method is presented that uses the same shared key to unlock all devices, making it applicable to IoT key-sharing protocols. CRO-based PUF structures offer improved hardware efficiency and reliability. Based on Physical Unclonable Functions (PUF) the researchers in (Bendavid et al., 2018) have created a lightweight Radio Frequency Identification (RFID) mutual authentication protocol that enables tracking and cloning of tags using a shared reader by protection against clone attacks.

Context Based Authentication

In order to improve the verification process, collected features can be recombined with other devices and sent to them to be processed in order to determine the location and the time the message originated. These features can make the authentication process more secure.

IoT security was evaluated using a contextual ontology in (Nazir et al., 2021), which included concepts representing device security and information of the IoTSec ontology. It was developed using NeOn methodology and some of the best practices for sharing, referencing, and reusing ontologies. Authentication with two factors is presented in (Muhammad Naveed Aman et al., 2017). Smart cards and passwords and are among the factors considered. Authors developed identity-based authentication for the Internet of Things (IOT). Identity capture is possible here as well.

Procedure Based Authentication

One-way authentication and two-way authentication are popular examples of authentication (Mutually authentication). Only one party will be able to authenticate themselves; The other, on the other hand, will remain unverified. Each party authenticates the other through two-way authentication. Also known as mutual authentication.

Based on Private Cryptography, the author proposed a biometric attributes-based method of user identification and key agreement in (Jyoti Deogirikar et al., 2017). A multifactor authentication system is described here. UserId and password are used. User identification is achieved using biometrics. Multifactor authentication, including digital signatures, device capabilities, and other factors, are described in (Chang-le Zhong et al., 2017).

PUF Based Authentication

The paper examines the vulnerable key agreement scheme of a recently proposed PUF-based protocol (Tewari et al., 2017) aimed at the Internet of Things (IoT) using the Yao-Dolev security model. In addition to addressing these issues, the authors presented an alternative scheme that can provide a more efficient key exchange as well as a communication phase between two IoT devices. Paper (Sharma et al., 2018) presented a mutual authentication scheme based on the use of Physically Unclonable Functions (PUFs), special integrated circuits with unlovability, uniqueness, and tamper-evident properties. The suggested scheme takes into account the computational capabilities and storage abilities of the devices typically incorporated into CE systems in a low-overhead method while combating several known attacks. Various IOT authentication algorithms are listed below the diagram according to different categories.

Mutual Based Authentication

A new protocol for mutual authentication for IoT systems based on Physical Unclonable Functions (PUFs) is presented in the paper (Barbareschi et al., 2019). This document presents two protocols that can be used in two different scenarios: one for communicating between an IoT device and server, and the other for establishing a session between two IoT devices. The protocols have been thoroughly examined in terms of their security and performance, which shows that they are not only highly resistant to potential attacks, but also very efficient in terms of communication, energy, memory and computation. A lightweight mutual authentication protocol based on a unique public-key encryption scheme is presented in the paper (Sadhukhan et al., 2021). By balancing efficiency and communications costs, the proposed protocol retains security. In (Huang et al., 2020), a lightweight mutual authentication scheme was presented for actual physical objects in an IoT environment. Payload-based encryption schemes encrypt the payload and verify the identities of participants through a four-way handshake. Client-server interaction models are used to communicate between objects in the real world. Utilizing the lightweight features of Constrained Application Protocol (CoAP), they provide an energy-efficient method for clients to observe resources residing on the server. For resource monitoring, they utilized Advanced Encryption Standard (AES). In Table 3, various authentication methodologies are compared.

RESEARCH GAP

- For obtaining authentication in device of IOT, the existing algorithms for Authentication for the network of IOT uses a key based approach of authentication. In such methods; the values of the key should be stored in the memory of the device. So, to the attack of key stolen, they are vulnerable. Furthermore, the values of the key can be originated by acting attack of side-channel. So, there is a requirement to propose a method in which the value of the key should not be motionless. Based on the application session time and criticality, it should be altered regularly.
- The devices of IOT are kept into open place namely industry factory and military field. Due to their deployment at open place, they are inclined to various cloning and physical attacks. Such that, there is a requirement to model an algorithm which does not only provides security opposing Identity based threats namely Replay attack, MITM attack and Key stolen attack, also but it should offer security against various physical attack like modifying the location spoofing attack, device cloning attack and distance attack. Sometimes, the approaches of identity based authentication also guides towards identification of uncertain device. Consequently, a novel technique is needed for providing exact authentication of a device in a heterogeneous as well as open system of IOT. To improve the schema of authentication this technique can use devices physical behavior features.
- To authenticate the device of IoT, the existing authentication methods for the system of IoT are based on a single shared password or key. But these methods are susceptible to the several security threats such as, Side channel attack, MITM attack, Device cloning attack and Key stolen attack. If the value of the password or key does not upgraded over the time period, then it controls against the Dictionary attack. Thus, if the third party has the key or password access, he/she can create a similar device which is fake. Due to that, the modelled authentication approach should be active in nature, in which the value of the key should be modified based on the time period of the session “One Session, One Cipher”. The advantage of such method will be that if adversary gets shared the password or key then anyone can’t get into the system and the system security cannot be damaged. Then, we can provide safety in opposition to few security that is well-known threat-MITM attack, Dictionary attack.

Table 3. Analysis of IoT Authentication Schemes

S. No	Author	Advantage	Disadvantage
1	(Jia et al., 2020)	low cost, fast response, and anti-attack function	scalability was not strong
2	(ProsantaGope., 2018)	secure against all the imperative security threats computationally efficient	suitable to resource limited IoT devices
3	(Yan et al., 2019)	prevent over-privilege access	Computational overhead is little high
4	(Shafiq et al., 2020)	Less storage and communication cost.	Does not achieves Mutual authentication
5	(Hussain et al., 2021)	Better efficiency in computation and communication costs	Vulnerable to impersonation
6	(Jiang et al., 2018)	improves the efficiency of anonymous communication system	No performance measurement is provided
7	(Rao et al., 2021)	Compatibility problems are solved	Computational overhead is little high
8	(Dikii et al., 2020)	Faster device communication	Device synchronization over time.
9	(Zhang et al., 2019)	high security and low cost	No performance measurement is provided
10	(Bendavid et al., 2018)	Secure against replay and many logged-in device's attacks	vulnerable to a desynchronization attack
11	(Nazir et al., 2021)	secure communication between IoT nodes	Chance to reveal identity of the data owner.
12	(Muhammad et al., 2017)	lower computational overhead and energy consumption	higher computational complexity
13	(Jyoti Deogirikar et al., 2017)	High efficiency	High computational time
14	(Chang-le et al., 2017)	Reduces the computational cost	Does not achieves Mutual authentication
15	(Tewari et al., 2017)	Low computational cost	certificate maintenance is complex
16	(Sharma et al., 2018)	Secure against replay and many logged-in device's attacks	Does not achieves Mutual authentication
17	(Barbareschi et al., 2019)	Reduces the computational cost	Performance analysis is not considered.
18	(Sadhukhan et al., 2021)	overcomes the security flaws transmission and communication cost is decreased	high computation overhead
19	(Huang et al., 2020)	Quick wrong password detection	Privacy-preserving is not considered

- For the process of decision making, we know that majority of IoT devices are situated at the positions which are very much complex. If an opponent obtains that device access, anyone can change its location and then the device will transfer malfunctioned or fake data to the center of control and command base. Because in the system, the damage can happens. If an intruder spoofed with location of that sensor device now, device will transfer false information to the command center and command center will take decision based on these false information. It can leads to accident and congestion also. In this type of situation, a conventional password-based or secret-key based authentication approach, which considers a shared secret key/ password is the only authentication factor, is not good solution for solving the security related problems. It will provide device authentication in ambiguous way. Also it opens a door for various Physical attack- Device stolen attack and changing distance attack. So, we should also consider context parameter for device authentication. It will tighten security and enhance authentication process.

OPEN ISSUES

Towards securing the devices of IoT, important efforts of research have been done, and there are still many problems ahead. To define the applicability in the IoT context, taking into account the requirements of fundamental protection of many devices of IoT, majority of the existing cryptographic methods have some problems that are presently available, and hence needs further analysis and study (Sharma et al., 2020).

This is due to majority of the suites of cryptography were modelled for systems with enough resources, namely processor and speed memory. Still few new schemes were proposed for three layers of IoT, few are lightweight, required to be studied further and improved before they can be entirely applicable in the Internet of Things.

To their personal data that is sensitive the near-universal acceptance of IoT will largely depend upon people's confidence and trust of that the new technology will give some privacy and security level. To addressing the issues of privacy and security in the IoT, the existing solutions review in section five exhibits many significant research challenges belonging. We sketch some of the major challenges of open research that require to be addressed in this section in this research active area are as follows:

- Few schemes of authentication are modeled for particular scenarios of IoT which are not possible to protect over every viable threats associated with such ecosystems.
- The schedules of Authentication for applications of IoT must be efficient, lightweight and flexible, while guarantee that privacy and security are not committed.
- For each IoT application domain, there is a requirement to design suitable cryptographic schemes.
- Lightweight cryptography for the devices of resource constrained of IoT requires additional studies still.
- In order to ascertain the author claims about the schemes viability, there is a need to explore few solutions of existing lightweight authentication like the same in 179.
- To ensure privacy and security of Holistic approach in the devices of IoT is required, diverse the method in168 where safety is only assured when transmission is done in one direction.
- For securing the devices of IoT in quantum computing, there is requirement to examine the fate of existing schemes of lightweight cryptography, since it is hoped that quantum computers will split major of the existing public-key which is the standard cryptographic systems.
- For estimating the cryptographic schemes190 energy consumption, there is necessity to maintain a robust model.
- There is a requirement to enhance more resource and efficient reliable primitives of nano-electronic security. There is a requirement for effectual schemes of key management that can be utilized in various domains of application.
- Through experimental test beds simulations and schemes of Key management wanted to be checked. For example, the authors of 188, 173 and 165 did not verify their claims using experimental simulations or testbeds.
- For the IoT resource constrained devices, few existing schemes of key management are not appropriate. For example, assuming the resources and type of the machine utilized in the testbed

of the experiment in 166, it can be finalized that the proposed scheme is not appropriate for strictly constrained IoT devices, hence there is a offer for more lightweight schemes research.

- There is a requirement for efficient schemes of key revocation that can be employed to cancel or annul keys when opponents compromised smart devices successfully.
- The schemes of key management in which the constrained nodes of resource delegate majority of the computation tasks to easy going remote party agent nodes, generally outside the network, require studies furthermore.

COMPARATIVE ANALYSIS OF SECURITY CHALLENGES BETWEEN TRADITIONAL NETWORK AND IOT

In the preceding two sections, security issues in the Internet of Things (IoT) layers and countermeasures are examined in depth. This section compares and contrasts the security difficulties that IoT and traditional networks face, as seen in the following (Lin et al., 2017).

Resources

Typically, a typical network consists of a personal computer, servers, and smart phone with sufficient resources, whereas an IoT system consists of WSN and FRID nodes with insufficient resources. Users can employ a union of lightweight and complicated algorithms to maximise security in a casual network while using less processing capacity. Only lightweight algorithms can be used in Internet of Things to preserve the balance in the middle of security and processing capacity.

Communication Ways

Wireless media is utilised to connect the nodes of the Internet of Things, resulting in a security compromise. Communication on the internet is typically done over a more secure wire or wireless communications, which is also faster. In the mobile internet, wireless connections are built on top of complicated secure protocols, which are practically hard to implement in IoT nodes due to low resources.

Risk Factor

The hazard in IoT systems is higher than in traditional networks since a huge number of IoT applications are used in daily life, and if influence over these systems is lost, a significant security threat may be generated. In a casual network, on the other hand, if users do not disclose their classified information voluntarily, there is no way for a bad person to obtain it for his criminal purposes.

Data Formats

Even while different devices connect to the internet, their data formats are nearly same due to the abstraction of operating systems such as Windows or UNIX, however in IoT, there is no operating system, only a basic integrated programme for the chip. Because of the many nodes in the IoT ecosystem, there is a wide range of chip technology, resulting in a wide range of data formats.

ADVANTAGES OF CONTEXT AND DYNAMIC KEY PARAMETER FOR IOT AUTHENTICATION

- **Context Parameter:** During login time contextual variable such as location communication is inspected, in advance the request message can be recognize by the intruder. Then after, there is no need to validate additional elements even during authentication period unless it is absolutely necessary. It will aid in improving the protection system's presentation in terms of response time.
- **Dynamic Key Parameter:** Since we all know, if the twin key is utilize for authentication for an extended period of time, it gives an adversary the way to promote a Key Steal and Surveillance

attack. As a result, it is preferable to customize and upgrade key values on a session-by-session basis. So, even if an attacker gains access to the key, she or he will be unable to capture the public key for upcoming expansions. As a result, it will guard against key theft and surveillance attacks. The model utilize for the result can be showed in table 4.

Table 5 illustrates the Existing Approaches of Context based / Dynamic Key based Authentication methods.

CONCLUSION

The Internet of Things (IoT) approach brings all commonplace devices and services together on a single network platform. Everything in the Internet of Things has a unique identifier and may be accessed over the network. It is also the activity of embedding intelligence into physical objects. Integrated intelligence in objects will enhance a wide spectrum of Internet of Things systems, helping to optimise environmental efficiency and improve human living standard. There is a requirement for a unified design, security, privacy and protocols in such situations. This paper contains a detailed

Table 4. Parameters/ Methods can be used for Problem Statement Solution

Sr. No.	Parameter/ Method	Advantages
1	Context Information (Physical/ Behavioral)	- Verification depending on context - Protection for spoofing attacks on position. (Useful in domains like the industry and military, where the position of a device is likewise a major review along with its heritage.).
2	Dynamic Key (Random Number/ Physical Property based/ Vault based)	- Verification Employing Dynamic Keys - Protection from Key Theft and Surveillance Attacks - Utilizing one of the options mentioned in Method/ Parameter, a private and dynamic public key would be produced.

Table 5. Findings from Existing Approaches of Context based / Dynamic Key based Authentication methods

S.No.	Author	Proposed Technique	Finding
1	Lin Wang et al. (2020)	Dynamic Key Generation techniques based on Physical Properties of device	- In wireless transmission, the production of private keys utilizing physical layer characteristics such as RSSI and Channel State Information. - Although physical parameters do not vary regularly, the key would not be upgraded in every round.
2	Lukas Nemec et al.(2019)	Dynamic approach for Key Re-establishment into WSN	- RSS is a key component of radio channel attributes. - If the principal of Spatial de-correlation is violated mean Adversary is present in nearby distance of transmitting device, then adversary will also get same RSSI value and he/ she can get the same key.
3	Alan J. Michales et al. (2019)	PRNG based Key Derivation Functions for Dynamic Key Generation	-Linear Feedback Register circuit is used for PRNG. -Linear and Deterministic in nature. Does not provide good randomness.
4	MortizLoske et al. (2019)	Context based Authentication	-Physical/ Behavioral context parameters are suggested for IoT Authentication. -RSSI & Device operation capability do not provide unambiguous results for device Authentication.

overview of most Internet of Things topics, including privacy, security, protocols and architecture, among others. For the convenience of future scholars, we too have discussed briefly the major current research papers linked with the principles stated as well as open problems.

FUTURE DIRECTION

In this portion, we go over our proposed future IoT network in brief and share some insights. The work introduced in this study will be utilised as a foundation for the development of context aware dynamic key mechanisms for the Internet of Things in a variety of disciplines in the upcoming.

In the context-aware systems field, there are numerous future studies opportunities. Areas like modelling, distribution, acquisition, context discovery and reasoning, selection of sensors in privacy, context sharing, sensing-as-a-service model and security examined as initial unexplored areas:

- **Context discovery:** Context can be utilised to supplement sensor data in a variety of ways. Analyzing sensor data and spontaneously categorizing it in the IoT, where application domains differ greatly, is a difficult issue. The growth of linked data and semantic technology in recent years has shown the way forward.
- **Acquisition, modelling, reasoning and distribution:** Because of the IoT's inexperience, it's complex to know when and where to use every strategy. Various strategies can be incorporated to the remedies without a lot of effort if standard requirements are defined and followed.
- **Selection of sensors in sensing-as-a-service model:** It is necessary to clarify and implement quality standards.
- **Security, privacy and trust:** Privacy and security must be safeguarded on multiple levels. In the Internet of Things, user acceptance is crucial. As a result, in order to earn users' trust, privacy and security safeguarding concerns must be carefully handled.
- **Context sharing:** It's critical to share context data between different types of middleware solutions and multiple samples of the same middleware solution.
- **Context reasoning:** ANN-based techniques and Un-supervised learning are used to construct efficient algorithms at the context processing level.
- **Uncertainty management:** To address the ambiguity factor in this context-aware approach, new uncertainty management methods utilizing Hidden Markov Models (HMM) were developed.

FUNDING

Not applicable.

ACKNOWLEDGMENT

We declare that this manuscript is original, has not been published before and is not currently being considered for publication elsewhere.

CONFLICTS OF INTEREST

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

We declare that this manuscript is original, has not been published before and is not currently being considered for publication elsewhere.

REFERENCES

Alladi, T., & Chamola, V. (2020). HARCI: A two-way authentication protocol for three entity healthcare IoT networks. *IEEE Journal on Selected Areas in Communications*, *39*(2), 361–369.

Almulhim, M., Islam, N., & Zaman, N. (2019). A lightweight and secure authentication scheme for IoT based e-health applications. *International Journal of Computer Science and Network Security*, *19*(1), 107–120.

Alraja, M. N., Farooque, M. M. J., & Khashab, B. (2019). The effect of security, privacy, familiarity, and trust on users' attitudes toward the use of the IoT-based healthcare: The mediation role of risk perception. *IEEE Access: Practical Innovations, Open Solutions*, *7*, 111341–111354.

Aman. (2017). Two factor Authentication for IOT with Location Information. IEEE Internet of Things Journal.

Barbareschi, M., De Benedictis, A., La Montagna, E., Mazzeo, A., & Mazzocca, N. (2019). A PUF-based mutual authentication scheme for Cloud-Edges IoT systems. *Future Generation Computer Systems*, *101*, 246–261.

Bendavid, Y., Bagheri, N., Safkhani, M., & Rostampour, S. (2018). Iot device security: Challenging "a lightweight rfid mutual authentication protocol based on physical unclonable function". *Sensors (Basel)*, *18*(12), 4444.

Bendavid, Y., Bagheri, N., Safkhani, M., & Rostampour, S. (2018). Iot device security: Challenging "a lightweight rfid mutual authentication protocol based on physical enclosable function". *Sensors (Basel)*, *18*(12), 4444.

Chikouche, N., Cayrel, P. L., & Boidje, B. O. (2019). A privacy-preserving code-based authentication protocol for Internet of Things. *The Journal of Supercomputing*, *75*(12), 8231–8261.

Chin, W. L., Li, W., & Chen, H. H. (2017). Energy big data security threats in IoT-based smart grid communications. *IEEE Communications Magazine*, *55*(10), 70–75.

Chuang, Y. H., Lo, N. W., Yang, C. Y., & Tang, S. W. (2018). A lightweight continuous authentication protocol for the Internet of Things. *Sensors (Basel)*, *18*(4), 1104.

Chuang, Y. H., Lo, N. W., Yang, C. Y., & Tang, S. W. (2018). A lightweight continuous authentication protocol for the Internet of Things. *Sensors (Basel)*, *18*(4), 1104.

Deogirikar & Vidhate. (2017). *Security Attacks in IoT: A Survey*. Presented at IEEE International conference on I-SMAC.

Dikii, D. (2020). Authentication algorithm for Internet of things networks based on MQTT Protocol. *Serbian Journal of Electrical Engineering*, *17*(3), 389–403.

Esfahani, A., Mantas, G., Matischek, R., Saghezchi, F. B., Rodriguez, J., Bicaku, A., & Bastos, J. et al. (2017). A lightweight authentication mechanism for M2M communications in industrial IoT environment. *IEEE Internet of Things Journal*, *6*(1), 288–296.

Fan, K., Luo, Q., Zhang, K., & Yang, Y. (2020). Cloud-based lightweight secure RFID mutual authentication protocol in IoT. *Information Sciences*, *527*, 329–340.

Fang, D., Qian, Y., & Hu, R. Q. (2020). A flexible and efficient authentication and secure data transmission scheme for IoT applications. *IEEE Internet of Things Journal*, *7*(4), 3474–3484.

Ghani, A., Mansoor, K., Mehmood, S., Chaudhry, S. A., & Rahman, A. U., & NajmusSaqib, M. (2019). Security and key management in IoT-based wireless sensor networks: An authentication protocol using symmetric key. *International Journal of Communication Systems*, *32*(16), e4139.

Gope. (2018). Lightweight and Privacy-Preserving Two-Factor Authentication Scheme for IoT Devices. IEEE Internet of Things Journal.

Hong, S. (2020). P2P networking based internet of things (IoT) sensor node authentication by Blockchain. *Peer-to-Peer Networking and Applications*, *13*(2), 579–589.

Hoque, M. A., & Davidson, C. (2019). Design and implementation of an IoT-based smart home security system. *International Journal of Networked and Distributed Computing*, *7*(2), 85–92.

Huang, Z., & Wang, Q. (2020). A PUF-based unified identity verification framework for secure IoT hardware via device authentication. *World Wide Web (Bussum)*, *23*(2), 1057–1088.

Hussain, S., Ullah, I., Khattak, H., Khan, M. A., Chen, C. M., & Kumari, S. (2021). A lightweight and provable secure identity-based generalized proxy signcryption(IBGPS) scheme for Industrial Internet of Things (IIoT). *Journal of Information Security and Applications*, *58*, 102625.

Jia, X., Hu, N., Su, S., Yin, S., Zhao, Y., Cheng, X., & Zhang, C. (2020). IRBA: An identity-based cross-domain authentication scheme for the internet of things. *Electronics (Basel)*, *9*(4), 634.

Jiang, L., Li, T., Li, X., Atiquzzaman, M., Ahmad, H., & Wang, X. (2018). Anonymous communication via anonymous identity-based encryption and its application in IoT. *Wireless Communications and Mobile Computing*.

Kalyani, G., & Chaudhari, S. (2020). An efficient approach for enhancing security in Internet of Things using the optimum authentication key. *International Journal of Computers and Applications*, *42*(3), 306–314.

Khalid, U., Asim, M., Baker, T., Hung, P. C., Tariq, M. A., & Rafferty, L. (2020). A decentralized lightweight blockchain-based authentication mechanism for IoT systems. *Cluster Computing*, 1–21.

Kim, H., & Lee, E. A. (2017). Authentication and Authorization for the Internet of Things. *IEEE Computers & Society*.

Kou, L., Shi, Y., Zhang, L., Liu, D., & Yang, Q. (2019). A lightweight three-factor user authentication protocol for the information perception of IoT. *CMC-Computers. Materials & Continua*, *58*(2), 545–565.

Kumari, S., Karuppiah, M., Das, A. K., Li, X., Wu, F., & Kumar, N. (2018). A secure authentication scheme based on elliptic curve cryptography for IoT and cloud servers. *The Journal of Supercomputing*, *74*(12), 6428–6453.

Lee, J., Yu, S., Park, K., Park, Y., & Park, Y. (2019). Secure three-factor authentication protocol for multi-gateway IoT environments. *Sensors (Basel)*, *19*(10), 2358.

Liang, W., Xie, S., Long, J., Li, K. C., Zhang, D., & Li, K. (2019). A double PUF-based RFID identity authentication protocol in service-centric internet of things environments. *Information Sciences*, *503*, 129–147.

Lin, S. C., Wen, C. Y., & Sethares, W. A. (2017). Two-tier device-based authentication protocol against PUEA attacks for IoT applications. *IEEE Transactions on Signal and Information Processing Over Networks*, *4*(1), 33–47.

Mamun, M. S. I., Ghorbani, A. A., Miyaji, A., & Nguyen, U. T. (2018). SupAUTH: A new approach to supply chain authentication for the IoT. *Computational Intelligence*, *34*(2), 582–602. doi:10.1111/coin.12164

Melki, R., Noura, H. N., & Chehab, A. (2020). Lightweight multi-factor mutual authentication protocol for IoT devices. *International Journal of Information Security*, *19*(6), 679–694.

Nandy, Ghani, & Bhattacharya. (2019). Review on Security of Internet of Things Authentication Mechanism. *IEEE Access*, *7*, 151054-151089.

Nazir, A., Sholla, S., & Bashir, A. (2021). An Ontology based Approach for Context-Aware Security in the Internet of Things (IoT). *International Journal of Wireless and Microwave Technologies*, *11*(1), 28–46.

Noguchi, Kataoka, & Yamato. (2019). Device Identification Based on Communication Analysis for the Internet of Things. *IEEE Access*.

Noguchi, Kataoka, & Yamato. (2019). Device Identification Based on Communication Analysis for the Internet of Things. *IEEE Access*.

Noor & Hassan. (2019). Current research on Internet of Things (IoT) security: A survey. *Computer Networks*, 283–294.

Panda, P. K., & Chattopadhyay, S. (2020). A secure mutual authentication protocol for IoT environment. *Journal of Reliable Intelligent Environments*, *6*(2), 79–94.

Panda, P. K., & Chattopadhyay, S. (2020). A secure mutual authentication protocol for IoT environment. *Journal of Reliable Intelligent Environments*, *6*(2), 79–94.

Qian, Y., Jiang, Y., Chen, J., Zhang, Y., Song, J., Zhou, M., & Pustišek, M. (2018). Towards decentralized IoT security enhancement: A blockchain approach. *Computers & Electrical Engineering*, *72*, 266–273. doi:10.1016/j.compeleceng.2018.08.021

Rao, B. B., &Waoo, A. A. (2021). Design a novel approach for token based authentication in iot networks. *Ilkogretim Online, 20*(4).

Sadhukhan, D., Ray, S., Biswas, G. P., Khan, M. K., & Dasgupta, M. (2021). A lightweight remote user authentication scheme for IoT communication using elliptic curve cryptography. *The Journal of Supercomputing*, *77*(2), 1114–1151.

Santhosh Krishna, B. V., & Gnanasekaran, T. (2017). A Systematic Study of Security Issues in Internet-of-Things (IoT). Presented at *IEEE International conference on I-SMAC*.

Shafiq, A., Ayub, M. F., Mahmood, K., Sadiq, M., Kumari, S., & Chen, C. M. (2020). An identity-based anonymous three-party authenticated protocol for IoT infrastructure. *Journal of Sensors*.

Sharma, G., & Kalra, S. (2018). A lightweight multi-factor secure smart card based remote user authentication scheme for cloud-IoT applications. *Journal of Information Security and Applications*, *42*, 95-106.

Sharma, G., & Kalra, S. (2020). Advanced lightweight multi-factor remote user authentication scheme for cloud-IoT applications. *Journal of Ambient Intelligence and Humanized Computing*, *11*(4), 1771–1794.

Sheron, P. F., Sridhar, K. P., Baskar, S., & Shakeel, P. M. (2020). A decentralized scalable security framework for end-to-end authentication of future IoT communication. *Transactions on Emerging Telecommunications Technologies*, *31*(12), e3815.

Soewito, B., & Marcellinus, Y. (2021). IoT security system with modified Zero Knowledge Proof algorithm for authentication. *Egyptian Informatics Journal*, *22*(3), 269–276.

Tahsien, S. M., Karimipour, H., & Spachos, P. (2020). Machine learning based solutions for security of Internet of Things (IoT): A survey. *Journal of Network and Computer Applications*, *161*, 102630.

Tewari, A., & Gupta, B. B. (2017). A lightweight mutual authentication protocol based on elliptic curve cryptography for IoT devices. *International Journal of Advanced Intelligence Paradigms*, *9*(2-3), 111–121.

Voas, J., & Agresti, B. (2018). T: A Closer Look at the IOT “things”, published in *IEEE. Computers & Society*, *20*(30), 6–15.

Wang, K. H., Chen, C. M., Fang, W., & Wu, T. Y. (2017). A secure authentication scheme for internet of things. *Pervasive and Mobile Computing*, *42*, 15–26.

Wang, K. H., Chen, C. M., Fang, W., & Wu, T. Y. (2018). On the security of a new ultra-lightweight authentication protocol in IoT environment for RFID tags. *The Journal of Supercomputing*, *74*(1), 65–70.

Wazid, M. (2017). Design of Secure User Authenticated Key Management Protocol for Generic IoT Networks. IEEE Internet of Things Journal.

Yan, H., Wang, Y., Jia, C., Li, J., Xiang, Y., & Pedrycz, W. (2019). IoT-FBAC: Function-based access control scheme using identity-based encryption in IoT. *Future Generation Computer Systems*, *95*, 344–353.

Zhang, J., & Qu, G. (2019). Physical unclonable function-based key sharing via machine learning for IoT security. *IEEE Transactions on Industrial Electronics*, *67*(8), 7025–7033.

Zhong, C., Zhu, Z., & Huang, R. (2017). Study on the IOT Architecture and Access Technology. *IEEE 16th International Symposium on Distributed Computing and Applications to Business, Engineering and Science*.

Zhong, Zhu, & Huang. (2017). C: Study on the IOT Architecture and Access Technology. *IEEE 16th International Symposium on Distributed Computing and Applications to Business, Engineering and Science.*

Zhou, L., Li, X., Yeh, K. H., Su, C., & Chiu, W. (2019). Lightweight IoT-based authentication scheme in cloud computing circumstance. *Future Generation Computer Systems*, *91*, 244–251.

Mihir Mehta is a Research Scholar, Computer Engineering in Gujarat Technological University, Ahmedabad.