Educational Administration: Theory and Practice
2024, 30(6), 1768-1779
ISSN: 2148-2403
https://kuey.net/

Research Article

A Study On Various Authentication Schemes In Iot To Provide Security

Mrs. Misbah Kousar[1]*, Dr. Sanjay Kumar[2], Dr. Mohammed Abdul Bari[3]

[1]*Ph.D Scholar in Kalinga University, Email: mkouar11@gmail.com
[2]Associate Professor, Kalinga University (CSE DEPT)
[3]Associate Professor – CSE-KMEC, Email: abdulbarimohammed11@gmail.com

***Corresponding Author:** Mrs. Misbah Kousar
*Ph.D Scholar in Kalinga University, Email: mkouar11@gmail.com

Citation: Mrs. Misbah Kousar et al. (2024), A Study On Various Authentication Schemes In Iot To Provide Security, *Educational Administration: Theory and Practice*, *30*(6), 1768-1779
Doi: 10.53555/kuey.v30i6.5586

ARTICLE INFO

ABSTRACT

The capacity to provide commonplace devices a means of identification and an additional channel for communication between themselves is what the Internet of Things (IoT) is all about. Smart homes, smart cities, wearables, e-health, and many more sectors span the vast expanse of the Internet of Things (IoT). The end result will be the interconnection of billions upon billions of devices. Automatic data collection, analysis, and decision-making will be possible with the help of these intelligent gadgets. In these situations, security is of the utmost importance, and authentication in particular is of great concern because to the potential harm that could be caused by an unauthenticated item in an IoT system. A comprehensive and current overview of the Internet of Things authentication sector is provided in this paper. Various authentication techniques have been suggested in the literature, and this document summarizes them all. As a first step for researchers and developers in this field, it compares and evaluates the proposed authentication methods using a multi-criteria categorization that we previously provided. It then shows the strengths and shortcomings of each protocol.

Keywords: Internet of Things; IoT; security; authentication

1. Introduction

The so-called Internet of Things (IoT) is a vast network of interconnected systems that links intelligent objects like sensors and actuators. The quantity of these devices is expanding at an exponential rate. Smart grids, smart transportation, smart homes, smart cities, smart agriculture, energy management, public health, and many more disciplines are embracing these technologies [1]. There are a lot of problems that arise from the requirements and limitations of the connected "things." For example, there is the problem of connecting billions of devices so that they can talk to each other. Another problem is security, since there is a need to protect IoT networks from attacks (according to a Gartner report, 20% of organizations have experienced at least one IoT attack in the last three years [2]) and from being used as an attack tool (e.g., Mirai botnet [3]). IoT devices have limited resources, which makes using conventional security and communication protocols ineffective or perhaps impossible. The widespread use of IoT devices in vital applications is increasing the severity of security breaches to the point where they pose a real threat to human life. As a result, concerns about IoT-related security are growing in severity. For example, in 2017, the US Food and Drug Administration (FDA) recalled half a million pacemakers due to a security flaw that may have allowed an attacker to take control of the device and regulate the patient's heart rate [4].
The applications that an IoT network supports determine its primary security requirements; these applications dictate whether authentication, confidentiality, or integrity is necessary. To be more specific, authentication is seen of as an essential component of the Internet of Things; having faith in the devices that make up an IoT network is vital to the network's efficiency. If even one compromised node becomes malicious, it might bring the entire system to its knees or even trigger catastrophic events. Traditional authentication systems are not suitable or viable for IoT devices due to their unique characteristics. The resource-constrained Internet of Things (IoT) nodes are not a good fit for cryptographic algorithms developed for powerful, high-processing, and/or memory-intensive devices. Because of this, several sparse authentication methods have evolved, some

of which are tailored to the Internet of Things (IoT) or the Wireless Sensor Network (WSN)—an environment that is well-suited to the IoT. This paper provides a high-level, layer-based overview of the security requirements and issues in an Internet of Things (IoT) setting. Additionally, it offers a current overview of the various authentication techniques used by the Internet of Things. As an expansion on earlier published research, it uses a multi-criteria classification to evaluate and analyze the current authentication systems, highlighting their benefits and drawbacks.

Here is the structure of the remaining portion of the paper: Section 2 introduces the generic architecture of the Internet of Things. The most pressing issues with Internet of Things (IoT) security, as well as the unique threats faced by each architectural layer, are covered in Section 3. In Section 4, we present a taxonomy of current authentication techniques. In Section 5, we utilise this taxonomy to examine the most well-known IoT authentication schemes. The study and its discussion of the survey's results are wrapped up in Section 6.

2. Generic Architecture of IOT

The Internet of Things (IoT) provides Machine-to-Machine (M2M) and Human-to-Machine (H2M) connectivity for diverse types of machines to support a variety of applications, such as identifying, locating, tracking, monitoring, and controlling, in contrast to the traditional Internet, which connects people to networks [5]. The necessity to address big data storage arises from the high traffic that results from connecting a large number of heterogeneous equipment. Consequently, the Internet Control Protocol/Internet Protocol (TCP/IP) architecture, which has been in use for a long time for network connectivity, is not suitable for the requirements of the Internet of Things (IoT) in terms of scalability, reliability, interoperability, quality of service, and security (e.g., information privacy, machine safety, data confidentiality, data encryption, and network security) [6]. Despite the many proposed IoT architectures, a reference architecture is still necessary [7]. As illustrated in Figure 1a, the three-layer architecture is the fundamental model suggested in the literature [8]. Three layers make it up: perception, network, and application.

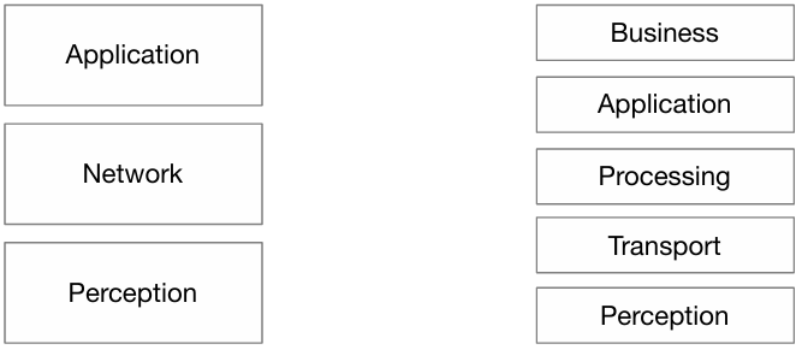
1. Perception layer: This layer uses end-nodes and various sensing technologies (e.g., RFID, GPS, NFC, etc.) to feel the environment and perceive physical qualities (e.g., temperature, humidity, speed, location, etc.).
2. The Network Layer: This layer is responsible for receiving data from the Perception Layer and sending it to the Application Layer using several network technologies, including as 3G, 4G, 5G, Wi-Fi, Bluetooth, Zig-Bee, etc. Data management, including storage and processing through middlewares like cloud computing, is also its responsibility.
3. Application layer: It is responsible for providing the user with services that are specific to the program. This layer's capacity to encompass several markets makes it crucial (e.g., smart metering, smart homes, health care, building automation, etc). [9].

One further layered design that has been suggested is the five-layer design (Figure 1b). Business, application, processing, transportation, and perception are the five levels, in that order, from highest to lowest. Perception, transport (the network layer), and application layers perform identically as they did in the original three-layer design. The remaining architectural components are:

1. The processing layer, often known as the middle-ware layer, is in charge of storing, analyzing, and processing data in relation to the computing outputs, among other things.
2. The business layer is responsible for the overall operation and behaviors of the IoT system. The data is sent from the application layer to the business layer, whose job it is to analyze the data using business models, graphs, and flowcharts. This helps with decision making on corporate plans and roadmaps.

The literature also contains descriptions of other types of architectures. To facilitate the incorporation of the Internet of Things (IoT) into business services, the authors of [10] adopted a five-layer SOA-based design. For example, cloud, fog, social IoT, and brain-based architectures were all evaluated as potential alternatives to a layered design.

We focus on the three-layer design for the remainder of the article.



(**a**) The-layer architecture (**b**) Five-layer architecture

Figure 1. IoT architecture models.

3. Security Issues in IoT

3.1 Security Services

Everyday people's reliance on connecting objects can pose serious security risks, as previously stated. Hackers have the ability to attack the smart features built into houses, cars, and energy grids in order to cause harm. In light of the proliferation of Internet of Things (IoT) applications handling sensitive data (personal, industrial, governmental, etc.), several hacking scenarios reported in recent years [11] demonstrate the severity of the damage that could ensue from a security breach. Security issues with the Internet of Things mostly revolve around the following: availability, privacy, authenticity, authorization, integrity, secrecy, non-repudiation, and authenticity [12].

- Authentication, which is making sure that something is who it says it is. In an Internet of Things setting, every node should be able to verify the identity of every other node in the system or in the specific area it communicates with.
- Authorization, is granting someone or something the green light to do or own something.
- Integrity is the process of ensuring that information remains consistent, accurate, and reliable over its entire life cycle. For example, in use scenarios involving smart health systems, it may result in the patient's death if fundamental information was altered or if incorrect information was introduced into the IoT.
- Protecting the information so that only authorized individuals can access it is known as confidentiality. Concerning privacy in the Internet of Things (IoT), there are two primary considerations: first, data management; and second, making sure the object receiving the data won't pass it to other things.
- Non-repudiation is the process of making sure that it is possible to prove that something happened (and by whom) so that it can't be disputed later. What this means is that the object cannot dispute the legitimacy of any data that has been transmitted.
- Availability is the process of making sure that the service that people require may be accessed whenever and wherever they need it. In the Internet of Things, this also encompasses the objects' accessibility.
- Privacy is about making sure that no one, including bad actors, may access sensitive data.

3.2 Security Challenges in IoT Layers

We examine the security issues, threats, and prerequisites at each level of the Internet of Things (IoT) architecture, starting with its most fundamental design (a three-layer architecture).

3.2.1. Perception Layer Security Issues and Requirements

Limited processing power and storage capacity are characteristics of the sensors that make up the perception layer [13]. Because of these restrictions, a number of security difficulties and assault dangers have increased. Damage to the perceptual layer has been detected in multiple instances:

1. Node Capture: Attackers can easily gain control of nodes, whether it’s the base node or the gateway. When an attacker manages to capture a node, they have access to sensitive information like cryptographic keys and protocol states. What’s worse is that they can use this information to create copies of themselves and disseminate them around the network, compromising its security [14].
2. DoS: The second kind of attack is known as a denial of service (DoS) attack, and it blocks legitimate users from accessing the system or network. One way to accomplish this would be to send a flood of spam requests to the system or network at once, which would cause it to crash and stop providing regular service [15].
3. Denial of Sleep Attack: An Internet of Things (IoT) network relies on sensing capabilities provided by a distributed network of nodes, each of which collects and transmits small amounts of data (e.g., temperature, humidity, vibration, etc.) at regular intervals before going to sleep for another period of time to prolong the nodes’ operational lifespan. By stopping the node from going to sleep after providing the required sensed data, a denial-of-sleep attack increases power consumption and, in turn, shortens the node’s service lifetime [16].
4. Distributed denial of service (DDoS) assault is a kind of DoS attack that targets multiple servers at once. The capacity to transmit gathered traffic to the victim server over the vast network of IoT nodes presents the greatest obstacle [17].
5. Fake node/sybil attack, which allows the attacker to use false nodes to deploy phony identities. It is possible for the entire system to provide inaccurate data or for neighboring nodes to get spam data and lose privacy if a sybil node is present [18]. The service could go down if the “legitimate” nodes were drained of their energy supply by data transmitted by the phony nodes.
6. Replay Attack: This type of attack involves the unauthorized storage and retransmission of information. Common targets for these kinds of attacks include authentication methods [19].
7. Routing Attacks: These attacks are the most basic kind at the network layer, but they can also happen at the perception layer during data forwarding. A routing loop, which an attacker can construct, can shorten or lengthen the routing path, which in turn increases the end-to-end time and the number of error messages [20].
8. A side-channel attack is a kind of attack that targets encryption devices. It takes advantage of information about the hardware, specifically the chips used to implement the crypto-system, such as the time it takes to execute, the amount of power consumed, the amount of power dissipated, and interference from

electromagnetic fields caused by electronic devices. By analyzing this data, one might potentially find the encryption secret keys [21].
9. Authenticating a large number of nodes in an IoT system is known as mass node authentication. This procedure necessitates a great deal of network connection to complete, which could impact the overall system performance.
In light of these dangers, it is essential to encrypt data in transit between nodes (end node, gateway, or server) and to provide node authentication to forestall fraudulent nodes and unauthorized access. Mature, lightweight security systems, incorporating both cryptographic algorithms and security protocols, are required because of the nodes' characteristics regarding power limitation and low storage capacity.
The following security measures are defined as a result of these possible assaults at the wireless or wired network layer: hopping from one hop to another, authenticating at each hop, managing keys, securing routes, and detecting intrusions [22].
It is the job of the application layer to provide services. It hosts a number of message carrying protocols, including message queuing telemetry transport (MQTT), COAP (Constrained Application Protocol), XMPP (Extensible Messaging and Presence Protocol), and many more [23]. This layer is the one the user is interacting with directly. Several application-layer security vulnerabilities have arisen as a result of the absence of IoT-specific international standards and the fact that "traditional" protocols have a hard time working within the IoT.
Making Data Verifiable and Accessible: Any one app could have a huge user base [24]. Verified users are essential for the system's availability, while imposters pose a serious threat. A wide range of permissions and access controls are required when dealing with a big number of people.
Because the IoT links devices made by different companies, several authentication methods are employed to safeguard identities and data. Integrating different approaches to ensure data privacy and identity is not an easy task.
The massive amount of data that needs to be managed is a direct result of the Internet of Things (IoT) connecting so many end devices. This data puts a heavy strain on the application's processing power, which in turn reduces the availability of the application's service(s).
To ensure the safety of application layers and the privacy of users' data, authentication is a must. Management of physical security information and resources should also be part of any strategy for overseeing information security. The Internet of Things (IoT) is structured with three layers, as shown in Table 1.

Table 1. IoT Architecture and security requirements.

Layer	Security Requirements
Perception	Lightweight Encryption
	Authentication
	Key Agreement
	Data Confidentiality
Network	Communication Security
	Routing Security
	Authentication
	Key Management
	Intrusion Detection
Application	Authentication
	Privacy protection
	Information Security Management

In Table 1, it is clear that authentication is a core security mechanism that should applied at different layers. An IoT use case might need an authentication between the end devices and an intermediate device (gateway). The gateway should authenticate itself while sending data to the cloud, and the application (mobile or web) should be authenticated to the cloud in order to collect data for analysis.

4. Taxonomy of IoT Authentication Schemes

This section presents a taxonomy of IoT authentication schemes using various criteria selected based on the similarities and the main characteristics of these schemes. As previously mentioned, the authentication can be

applied at each of the three layers of the IoT architecture, which makes the diversity of the authentication techniques.

1. Authentication factor

Identity: An information presented by one party to another to authenticate itself. Identity-based authentication schemes can use one (or a combination) of hash, symmetric or asymmetric cryptographic algorithms.
Context: which can be:
Physical: Biometric information based on physical characteristics of an individual, e.g., fingerprints, hand geometry, retinal scans, etc.
Behavioral: Biometric based on behavioral characteristics of an individual, e.g., keystroke dynamics (pattern of rhythm and timing created when a person types), gait analysis (method used to assess the way we walk or run), voice ID (voice authentication that uses voice-print), etc.

2. Use of tokens

Token-based Authentication: Authenticates a user/device based on an identification token (piece of data) created by a server such as OAuth2 protocol.
Non-Token based authentication: Involves the use of the credentials (username/password) every time there is a need to exchange data.

3. Authentication procedure

One-way authentication: In a scenario of two parties wishing to communicate with each other, only one party will authenticate itself to the other, while the other one remains unauthenticated.
Two-way authentication: It is also called mutual authentication, in which both entities authenticate each other.
Three-way authentication: Where a central authority authenticates the two parties and helps them to mutually authenticate themselves.

4. Authentication architecture

Distributed: Using a distributed straight authentication method between the communicating parties.
Centralized: Using a centralized server or a trusted third party to distribute and manage the credentials used for authentication.
Whether centralized or distributed, the authentication scheme architecture can be:
Hierarchical: Utilizing a multi-level architecture to handle the authentication procedure.
Flat: No hierarchical architecture is used to deal with the authentication procedure.

5. IoT layer: Indicates the layer at which the authentication procedure is applied.

Perception layer: Responsible for collecting, processing, and digitizing information perceived data by the end nodes in IoT platform.
Network layer: Responsible for receiving the perceived data from the perception layer and processing it.
Application layer: Responsible for receiving data from the network layer, and then providing services requested by users.

6. Hardware-based: The authentication process might require the use of physical characteristics of the hardware or the hardware itself.
Implicit hardware-based: Uses the physical characteristics of the hardware to enhance the authentication such as Physical Unclonable Function (PUF) or True Random Number Generator (TRNG).
Explicit hardware-based: Some authentication schemes are based on the use of a Trusted Platform Module (TPM), a chip (hardware) that stores and processes the keys used for hardware authentication.

5. Analysis of IoT Authentication Schemes

Authentication mechanisms for the Internet of Things (IoT)—including those for WSN—are reviewed in this section. The multi-criteria categorization given in Section 4 forms the basis of the analysis.
The surveyed research works are organized based on the IoT application domains.

a. Smart Grids:

Smart grid is taking the momentum over traditional power grids due to its efficiency and effectiveness, but security issues are still challenging in such field. In [26], the authors proposed an authentication scheme based on a Merkle-hash tree. Each home is equipped with a smart meter to collect the consumption of electricity for a time interval and sends the data via wireless communication to the Neighborhood Gateway (NG). The NG sends these data to the control center to collect the bill, which is sent back to the customer. The main contribution is the mutual authentication done between the smart meter and NG using a lightweight scheme that has an efficient computation and communication overhead.
While developing a smart grid, two main features should be taken into consideration: the data sent to the control unit or gateway should be sent from a valid smart meter, and there should not be a way of bring out the style of the customer by analyzing his consumption of electricity, thus breaking his privacy. In [27], the authors took the above features into consideration and developed an authentication scheme (called PASS) for smart

grids based on Hash-based Message Authentication Code (HMAC). Such approach also ensures the privacy of the customer.

To achieve a lightweight message authentication scheme for smart grid, the authors of [28] built an approach that allows smart meters to mutually authenticate to other system components and achieve message authentication. The authentication is done using a lightweight Diffie–Hellman and the data integrity is achieved using HMAC.

In [29], the authors proposed an authentication protocol for smart grids called Smart Grid Mutual Authentication (SGMA) and another scheme called Smart Grid Key Management (SGKM) for key management. The scheme benefits from the traditional protocols and enhances them to achieve mutual authentication and key management. It uses the Secure Remote Password (SRP) that depends on the password entered by the requester to generate a verification ID for further communications, but the enhanced version has less overhead with respect to the exchanged handshake messages and number of packets. Public Key Infrastructure (PKI) is used for key management but due to its overhead regarding the key regeneration, an enhanced version of ID-based Cryptography (EIBC) is used with PKI by replacing the public key with the identity of the requester.

In [30], the authors proposed a lightweight authentication protocol for smart grids. It consists of three tiers by using three different protocols for different purposes: Diffie–Hellman is used as key agreement protocol, with the use of RSA and AES for achieving the confidentiality, and HMAC for maintaining message integrity. To address some performance and security challenges such as the storage cost and the key management, the authors of [31] discussed one-time signature to be used for multicast authentication in smart grids. This reduces the amount of exchanged data. The main advantage of such scheme is keeping the identity of the smart meter hidden to the gateway and the control center until the time of generating the bills, thus ensuring privacy. Due to the limitation of one-time signature with respect to the size and the storage of the signature, a one-time signature-based multicast authentication in smart grid is proposed. Their scheme deployed a new one-time signature based on a nonlinear integer programming that reduces the computation cost.

b. RFID and NFC-Based Applications

Radio Frequency Identification (RFID) is a wireless technology that consists of tags that can be attached to any physical object or even humans; its main purpose is the identification or detection of the tagged objects. RFID can be deployed in various fields, e.g., supply chain, health care, climate sensing, etc.

In [32], the authors suggested a lightweight authentication protocol for RFID tags based on PUF. The protocol consists of three transactions: tag recognition, verification, and update. In the first transaction, the tag reader recognizes the tag. The second transaction is the verification, where the reader and the tag mutually verify the authenticity of each other. In the last transaction (Update), one should keep up the most recent used key for the next verification.

To protect the supply chain of connected devices, they enabled authentication and perceptibility of the IoT devices, through an RFID-based solution. The authentication process consists of two steps: checking the connectivity between the tag and the IoT device and then approving the perceptibility of the tag.

In an IoT-RFID based system, the RFID reader is connected to the Internet to form an IoT end device. On the other side, it is connected to the tagged items via RFID communication protocols. The tagged item is portable and moves from a reader to another, thus there is a need for verifying the identity of each other via authentication. Due to the absence of cryptographic features in RFID, the system is vulnerable to security threats such as impersonation or cloning attacks. they presented an authentication protocol to be used in IoT-RFID use case with the use of lightweight encryption algorithm.

To resist against cloning attacks to the RFID tag, the authors of [33] proposed an offline authentication for RFID-tags based on PUF. It combined both identification and digital signature security protocols. In the authentication, the tag generates a secret key by challenging the PUF and collecting the response. Such response with the helper data will create a certificate that will be stored inside the ROM of the tag. Next, the verifier authenticates the tag by checking the validity of the certificate.

To provide anonymous authentication for RFID systems, they presented a PUF-based authentication scheme for classic RFID tags. Then, they provided an enhanced scheme for noisy PUF environment. The main drawback of such scheme is not taking into consideration re-feeding the server with new Challenge–Response Pair (CRP) when the existing pool becomes empty.

A two-factor authentication scheme based on smartphone with Near Field Communication (NFC) feature as first factor and fingerprint of the user as the second factor is proposed. Both factors are used to authenticate user on smart library system. The library database then checks if the personal data embedded in the NFC tag and the fingerprint match then the user is authorized to access the internal library network to query for books and providing the user with the rack position (location) in which the book is located.

c. Vehicular Networks

Vehicular networks, also known as the Internet of Vehicles, are formed when cars nowadays are linked to either the Internet or the Internet of Things. Several services rely on this kind of connection, including electric vehicle charging, ridesharing, traffic reports, and more. Electric vehicles (EVs) are quickly gaining popularity, and one of the most difficult aspects of EV systems is authenticating vehicles. A two-factor authentication approach for EV was suggested by the authors of [35], however it has potential applications in other domains as well. An

innovative contextual feature is integrated into the scheme. It is dependent on the physical connectivity to validate the identity since the car is linked to the server through wireless connectivity and to the charger through a charging cable.

Prediction-Based Authentication (PBA), described in [36], is a broadcast authentication method that protects against denial-of-service (DoS) assaults and packet loss. Instead of keeping track of all the receiving signatures, the protocol uses self-generated Message Authentication Codes (MACs) and uses Merkle hash trees to verify urgent communications instantly. A Prediction-Based Authentication (PBA) as a VANET broadcast authentication technique offered. The suggested method efficiently and effectively authenticates messages between cars by using ECDSA signatures and TESLA, which stands for Time Efficient Stream Loss Tolerant Authentication.

One authentication method for protecting VANETs was suggested by the authors of [37] and is known as (ESPA). Communications between vehicles and infrastructure (V2I) and vehicles and each other (V2V) are protected by the protocol's usage of symmetric HMAC and asymmetric cryptography (PKI). The authors put out a novel group-authentication based approach for VANET authentication. In order to facilitate vehicle-to-vehicle communication, a session key is created and the vehicles are grouped.

In order to facilitate safe and privacy-preserving communications in VANETs, the authors of [38] suggested a threshold authentication system. In order to accomplish threshold authentication, efficient cancelation, anonymity, and traceability while cars are communicating, the protocol is defined by a group signature scheme. The authors of [39] employed public key infrastructure (PKI) to validate the vehicle's public key and a set of immutable characteristics. A method to authenticate the identity of a motorist in transit was suggested. User authentication and privacy protection are achieved through the use of elliptic-curve cryptography (ECC) and steganography techniques.

Because of roadside impediments and vehicle movement, connecting VANETs to IP networks using ARs was an issue in most cases, a feasibility of a multi-hop system for providing IP connectivity to VANET vehicles was proposed. For roaming purposes, the location and traffic data are maintained in a location server. This method allows ARs and roaming vehicles to authenticate each other.

d. Smart Homes

In [40], the authors introduced a new authentication scheme to authenticate the end devices deployed in smart homes, which is based on the combination of PUF and Physical Key Generation (PKG). The PUF provides the security of the system by generating a secure key based on the physical parameters of the end device (the design of PUF depends on common circuit fabrication features that give it the ability to create unique secret key). Machine-to-Machine (M2M) communication is taking a lead in the IoT development, but it also has security challenges.

The authors of [41] developed a PUF-based authentication scheme for IoT devices to provide mutual authentication between the end device and the gateway by using the CRP data stored inside the gateway. It also provides a way for user (smart phone or wearable device) to authenticate itself with the gateway in order to have the ability to communicate with the end devices using session key generated between them. Timestamp data are used by the user to ensure security against replay attacks.

The authors of [42] proposed a mutual authentication for IoT systems. The scheme is based on the lightweight features of Constrained Application Protocol (CoAP) as an application layer protocol for the communication between client and the server. The secure communication channel is provided by the advantage of Advanced Encryption Standard (AES) cipher. Both the client and the server challenge each other for mutual authentication by encrypting a payload from the message of size 256 bits, and then exchange payloads for verification. The authentication is done during the request-response interaction without the use of an extra layer (DTLS) which increases the communication and computation cost.

e. Wireless Sensor Networks

The capacity to integrate billions of sensors embedded in many domains (e.g., household appliances, cars, power grids, etc.) with the ability to link and sense is known as wireless sensor networks (WSN).

Optimization of Communication for Ad-hoc Reliable Industrial Networks (OCARI), an authentication mechanism at the media access control sub-layer was proposed. This protocol made use of a one-time shared session key. Devices with limited resources can benefit from this method. When it comes to key management protocols, the Blom key predistribution scheme and the polynomial schema are seen as suitable for some Internet of Things applications.

Mutual authentication is achieved by the use of BAN-logic, which is a logic of belief and action that guarantees one component of the communication believes that the authentication key is good. Each node in the system should be identified in the enrollment stage of the two-stage mutual authentication described by the authors of [43]. Then, in the authentication stage, the end device and the server exchange a series of handshake messages to generate a session key that will be used for future communication.

An authentication scheme based on lightweight Hash and XOR operations was developed to ensure mutual authentication between the user, the end node, and the gateway node (GWN) in a WSN. This scheme allows the remote user to connect to the end nodes in WSN systems without initially needing to be connected to the gateway.

Lightweight encryption techniques are necessary because of the resource-constrained characteristics of the sensor nodes in WSN systems. Consequently, a less burdensome alternative to the conventional RSA cypher, Elliptic Curve Cryptography (ECC) was suggested as a safe authentication mechanism for WSN. Furthermore, the authors implemented the scalable Attribute-Based Access Control (ABAC) authorization method for access control.
It was suggested in [44] that WSNs use an authentication method. There are two primary components to the system. The first is the setup process, when a user is provided with a public and private key pair utilizing a lightweight ECC-based protocol. Step two involves authentication, wherein nodes verify each other's identities using the public/private pair.

f. Mobile Network and Applications

To allow remote users to access Internet services any time, anywhere, the authors of [45] proposed a new scheme to provide a secure roaming for anonymous users benefiting from the group signature technique. They call it Conditional privacy-preserving authentication with access linkability (CPAL). In [46], the authors proposed two authentication schemes, the first one is based on pseudo-random authentication and the second is based on zero-knowledge authentication for providing authentication and location privacy-preserving scheme for LTE-A. The schemes enable all the entities in LTE-A networks to mutually authenticate each other and update their location without involving the subscriber server. They provided also a group-based authentication scheme for LTE networks by developing a group temporary key. It is based on both Elliptic Curve Diffie–Hellman (ECDH) that provides forward and backward secrecy, while using asymmetric key protocol to provide user's privacy. They also proposed SEGR for the authentication of a group of devices using both 3GPP or WIMAX systems. It is based on certificate-less aggregate signature which was proposed to remove the complication of certificate management in public key cryptography.

Due to challenging issues in developing a user-friendly authentication scheme for smart phone environment where touch screen is the most user-friendly input peripherals, the authors of [47] provided an authentication process for Android smartphone devices using dual-factor authentication called (Duth). The protocol is made up of a registration step in which the place and time of user entering patterns to the touch screen are stored and then the stored data are used as dual factors for authentication. This approach can improve security without adding any extra hardware.
The authors of [48] proposed a new authentication scheme for mobile phone users based on behavioural pattern. They started by collecting the behavior of mobile phone user regarding the applications used in a specific time and the duration of usage, and then they change these data to a unique pattern to be used as an authentication between the user and the mobile phone.The proposed scheme will be used as complementary to the existing authentication schemes provided by mobile phones (pin code, fingerprint, gestures, etc.).

g. Generic IoT Applications

The authors of [49] presented GLARM, a group-based lightweight authentication and key agreement scheme, to address the issue of resource-constrained devices requiring mutual authentication and secure key management in response to the overwhelming number of devices attempting to access the network. GLARM involves two main steps: first, identifying the devices to be authorized; and second, authenticating the group and agreeing on a key based on a combination of message authentication codes.
One such protocol for Internet of Things (IoT) systems is speaker-to-microphone (S2M). The distance authentication between wireless Internet of Things devices is accomplished by this method. In order to verify its efficacy in experiments, it is installed on both mobile phones and personal computers.
In [50], the author introduced a novel hardware-based method for authenticating Internet of Things (IoT) devices by means of their Physical Unclonable Functions (PUF). The author described the assaults on PUF that used machine learning, which resulted in the development of a software model of the PUF. In order to enroll devices, authenticate users, decrypt data, and generate digital signatures, they employed an elliptic curve based on PUF. The author used error correction codes to pinpoint the environmental fluctuations that the IoT devices will be operating in, as well as the impact of aging on PUF usage. They dealt with ML attacks by encrypting the produced key using a combination of PUF and ECC. To prevent modeling-based attacks, an authentication mechanism was suggested that uses PUF modeling to conceal the model using a symmetric encryption algorithm (AES). This prevents the storage or retrieval of whole Challenge-Response Pairs (CRPs) during authentication or verification.

In [51], the authors provided an authentication scheme to be used in cloud computing use cases. They divided the devices into two categories: registered and unregistered devices, and handled the authentication using two different approaches. The registered devices are authenticated using an authentication server. Firstly, the device is registered in the server, then a session key is generated by the server and sent encrypted using Advanced Encryption Standard (AES), to the device to be used for further communications. On the other hand, a cloud-based Software-as-a-Service (SaaS) using modified Diffie–Hellman (DH) algorithm is used to authenticate unregistered devices for accessing cloud services.
Using password or smart cards as the only way of authentication for remote users is vulnerable to security

attacks. Thus, the authors of [52] proposed a novel scheme by using a three-factor authentication. The fingerprint or iris-scan, the smart card, and a password to authenticate a user to remotely-based applications.

The authors of [53] presented a two-factor device authentication scheme. They used both the digital signature and a novel factor called the device capability. Device capability is similar to a functional operation solved by the device, which could be a mathematical challenge or even a cryptographic-based puzzle. Such scheme can be used to authenticate both the end-device and the server too. Using a secure TLS channel, the device sends a request for communication to the server, the server then sends a nonce encrypted with its private key and the timestamp to avoid replay attacks. The device then decrypts the signature, solves the nonce with functional operation, signs the result with its private key and sends it back to the server. The server then checks the valid signature and the result of the functional operation to authenticate the device.
The authors of [54] proposed a new authentication scheme for IoT system based on PUF. The scheme is based on generating a response of a challenge, then feeding the response to another PUF as a challenge. The two PUFs are connected using Linear Feedback Shift Register (LFSR). The main drawback of such design is its complexity, and the lack of security analysis. Machine learning attacks to create a model of PUF is not considered
The authors of [55] proposed a new authentication scheme for IoT systems based on blockchain called Bubbles-of-Trust. The idea is to divide the devices into virtual zones called bubbles in which they identify and trust each other (concept of grouping). Then, the communication (transaction) between different devices is controlled and validated by the public blockchain implemented using Ethereum.

6. Conclusion

Authentication within the Internet of Things (IoT) setting is categorized and reviewed in this article. Research and development teams working on novel authentication schemes for the Internet of Things (IoT) should keep in mind the many requirements and open concerns uncovered by analyzing a wide range of authentication protocols and schemes. The recommended protocols for sensor-based applications must be lightweight, striking a balance between power consumption and security, because sensors are end-devices with limited memory, processing power, battery life, etc. Consideration and analysis should be given to the robustness of authentication methods against potential attacks such as sybil, replay, man-in-the-middle, DoS, collision, chosen-plaintext, brute force, message forging, and node capture. Take Distributed Denial of Service assaults (the second assault on the Internet of Things in 2017 according to [6]) into careful consideration.
Smart grids and VANETs are two examples of Internet of Things (IoT) technologies that require careful consideration of location and identity privacy.It is important to minimize the amount of messages sent and received between authentication parties in order to reduce the communication overhead of authentication protocols. This is particularly true when working with devices that have limited power. Similarly, because the wireless communication protocols utilized have limited bandwidth, the message sizes should be kept to a minimum. Particularly for power-constrained and processing-limited IoT environments, low computation cost should be addressed while developing IoT authentication algorithms. The importance of using lightweight cryptographic algorithms and protocols in the development of authentication solutions is highlighted by this.
The ideal authentication strategy for the Internet of Things (IoT) would be scalable, meaning it could handle a high number of nodes and easily add more nodes without requiring any additional configuration or setup. All three tiers of an Internet of Things (IoT) architecture—the application, the network, and the perception layer—need an authentication service. In order to create effective IoT authentication techniques, it is necessary to think about the heterogeneity of devices in IoT networks.Because of its benefits over software security measures, hardware security employing "PUF" is currently trending. There needs to be a mix of software (less expensive) and hardware (more secure) solutions.

References

1. El-hajj, M.; Chamoun, M.; Fadlallah, A.; Serhrouchni, A. Analysis of authentication techniques in Internet of Things (IoT). In Proceedings of the 2017 1st Cyber Security in Networking Conference (CSNet), Rio de Janeiro, Brazil, 18–20 October 2017; pp. 1–3.
2. Maresch, D.; Gartner, J. Make disruptive technological change happen—The case of additive manufacturing. *Technol. Forecast. Soc. Chang*. 2018
3. Ahmed, M.E.; Kim, H. DDoS Attack Mitigation in Internet of Things Using Software Defined Networking. In Proceedings of the 2017 IEEE Third International Conference on Big Data Computing Service and Applications (BigDataService), San Francisco, CA, USA, 6–9 April 2017.
4. Hern, A. Hacking risk leads to recall of 500,000 pacemakers due to patient death fears. *The Guardian*, 31 August 2017.
5. Liu, R.; Wang, J. Internet of Things: Application and Prospect. In *MATEC Web of Conferences*; Zhao, L., Xavior, A., Cai, J., You, L., Eds.; EDP Sciences France: Les Ulis, France, 2017; Volume 100, p. 02034.
6. Shang, W.; Yu, Y.; Droms, R.; Zhang, L. *Challenges in IoT Networking via TCP/IP Architecture*; Technical Report 04, NDN, Technical Report NDN-0038; Named Data Networking. Available online: http://named-

data.net/techreports.html (accessed on 10 Augest 2018).
7. Weyrich, M.; Ebert, C. Reference Architectures for the Internet of Things. *IEEE Softw*. **2016**, *33*, 112–116. [CrossRef]
8. Mashal, I.; Alsaryrah, O.; Chung, T.Y.; Yang, C.Z.; Kuo, W.H.; Agrawal, D.P. Choices for interaction with things on Internet and underlying issues. *Ad Hoc Netw*. **2015**, *28*, 68–90. [CrossRef]
9. Nastase, L. Security in the Internet of Things: A Survey on Application Layer Protocols. In Proceedings of the 21st International Conference on Control Systems and Computer Science (CSCS), Bucharest, Romania, 29–31 May 2017; pp. 659–666.
10. Wang, F.; Hu, L.; Zhou, J.; Zhao, K. A data processing middleware based on SOA for the Internet of things. *J. Sens*. **2015**, *2015*, 827045. [CrossRef]
11. Hernandez, G.; Arias, O.; Buentello, D.; Jin, Y. *Smart Nest Thermostat: A Smart Spy in Your Home*; Black Hat USA: Las Vegas, NV, USA, 2014.
12. Mahmoud, R.; Yousuf, T.; Aloul, F.; Zualkernan, I. Internet of things (IoT) security: Current status, challenges and prospective measures. In Proceedings of the 2015 10th International Conference for Internet Technology and Secured Transactions (ICITST), London, UK, 14–16 December 2015.
13. Wen, Q.; Dong, X.; Zhang, R. Application of dynamic variable cipher security certificate in Internet of Things. In Proceedings of the 2012 IEEE 2nd International Conference on Cloud Computing and Intelligence Systems, Hangzhou, China, 30 October–1 November 2012.
14. Zhu, B.; Addada, V.G.K.; Setia, S.; Jajodia, S.; Roy, S. Efficient Distributed Detection of Node Replication Attacks in Sensor Networks. In Proceedings of the Twenty-Third Annual Computer Security Applications Conference (ACSAC 2007), Miami Beach, FL, USA, 10–14 December 2007.
15. Anirudh, M.; Thileeban, S.A.; Nallathambi, D.J. Use of honeypots for mitigating DoS attacks targeted on IoT networks. In Proceedings of the 2017 International Conference on Computer, Communication and Signal Processing (ICCCSP), Chennai, India, 10–11 January 2017.
16. Capossele, A.T.; Cervo, V.; Petrioli, C.; Spenza, D. Counteracting Denial-of-Sleep Attacks in Wake-Up-Radio-Based Sensing Systems. In Proceedings of the 2016 13th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON), London, UK, 27–30 June 2016.
17. Machaka, P.; Bagula, A.; Nelwamondo, F. Using exponentially weighted moving average algorithm to defend against DDoS attacks. In Proceedings of the 2016 Pattern Recognition Association of South Africa and Robotics and Mechatronics International Conference (PRASA-RobMech), Stellenbosch, South Africa, 30 November–2 December 2016.
18. Evangelista, D.; Mezghani, F.; Nogueira, M.; Santos, A. Evaluation of Sybil attack detection approaches in the Internet of Things content dissemination. In Proceedings of the 2016 Wireless Days (WD), Toulouse, France, 23–25 March 2016.
19. Na, S.; Hwang, D.; Shin, W.; Kim, K.H. Scenario and countermeasure for replay attack using join request messages in LoRaWAN. In Proceedings of the 2017 International Conference on Information Networking (ICOIN), Da Nang, Vietnam, 11–13 January 2017.
20. Airehrour, D.; Gutierrez, J.; Ray, S.K. A Lightweight Trust Design for IoT Routing. In Proceedings of the 2016 IEEE 14th Intl Conf on Dependable, Autonomic and Secure Computing, 14th Intl Conf on Pervasive Intelligence and Computing, 2nd Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress(DASC/PiCom/DataCom/CyberSciTech), Auckland, New Zealand, 8–12 August 2016.
21. Pammu, A.A.; Chong, K.S.; Ho, W.G.; Gwee, B.H. Interceptive side channel attack on AES-128 wireless communications for IoT applications. In Proceedings of the 2016 IEEE Asia Pacific Conference on Circuits and Systems (APCCAS), Jeju, Korea, 25–28 October 2016.
22. Mahmoud,R.;Yousuf, T.; Aloul, F.; Zualkernan, I. Internet of things (IoT) security: Current status, challenges and prospective measures. In Proceedings of the 2015 10th International Conference for Internet Technology and Secured Transactions (ICITST), London, UK, 14–16 December 2015.
23. Hedi, I.; Speh, I.; Sarabok, A. IoT network protocols comparison for the purpose of IoT constrained networks. In Proceedings of the 2017 40th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), Opatija, Croatia, 22–26 May 2017.
24. Manyika, J.; Chui, M.; Bisson, P.; Woetzel, J.; Dobbs, R.; Bughin, J.; Aharon, D. *Unlocking the Potential of the Internet of Things*; McKinsey Global Institute: New York, NY, USA, 2015.
25. Chae, C.J.; Choi, K.N.; Choi, K.; Yae, Y.H.; Shin, Y. The Extended Authentication Protocol using E-mail Authentication in OAuth 2.0 Protocol for Secure Granting of User Access. *J. Internet Comput. Serv*. **2015**, *16*, 21–28. [CrossRef]
26. Li, D.; Aung, Z.; Williams, J.R.; Sanchez, A. Efficient authentication scheme for data aggregation in smart grid with fault tolerance and fault diagnosis. In Proceedings of the 2012 IEEE PES Innovative Smart Grid Technologies (ISGT), Washington, DC, USA, 16–20 January 2012.
27. Fouda, M.M.; Fadlullah, Z.M.; Kato, N.; Lu, R.; Shen, X. Towards a light-weight message authentication mechanism tailored for Smart Grid communications. In Proceedings of the 2011 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), Shanghai, China, 10–15 April 2011.
28. Nicanfar, H.; Jokar, P.; Beznosov, K.; Leung, V.C.M. Efficient Authentication and Key Management Mechanisms for Smart Grid Communications. *IEEE Syst. J*. **2014**, *8*, 629–640. [CrossRef]

29. Wu, T. The Secure Remote Password Protocol. In Proceedings of the Network and Distributed System Security Symposium, San Diego, CA, USA, 11–13 March 1998; Volume 98, pp. 97–111.
30. Ji, C.; Kim, J.; Lee, J.Y.; Hong, M. Review of one-time signatures for multicast authentication in smart grid. In Proceedings of the 2015 12th International Conference & Expo on Emerging Technologies for a Smarter World (CEWIT), Melville, NY, USA, 19–20 October 2015.
31. Chim, T.W.; Yiu, S.M.; Li, V.O.; Hui, L.C.; Zhong, J. PRGA: Privacy-preserving recording & gateway-assisted authentication of power usage information for smart grid. *IEEE Trans. Dependable Secur. Comput.* **2015**, *12*, 85–97.
32. Li, Q.; Cao, G. Multicast Authentication in the Smart Grid With One-Time Signature. *IEEE Trans. Smart Grid* **2011**, *2*, 686–696. [CrossRef]
33. Yang, K.; Forte, D.; Tehranipoor, M.M. Protecting endpoint devices in IoT supply chain. In Proceedings of the 2015 IEEE/ACM International Conference on Computer-Aided Design (ICCAD), Austin, TX, USA, 2–6 November 2015.
34. Gope, P.; Lee, J.; Quek, T.Q.S. Lightweight and Practical Anonymous Authentication Protocol for RFID Systems Using Physically Unclonable Functions. *IEEE Trans. Inf. Forensics Secur.* **2018**, *13*, 2831–2843. [CrossRef]
35. Zhang, L.; Wu, Q.; Domingo-Ferrer, J.; Qin, B.; Hu, C. Distributed Aggregate Privacy-Preserving Authentication in VANETs. *IEEE Trans. Intell. Transp. Syst.* **2017**, *18*, 516–526. [CrossRef]
36. Lalli, M.; Graphy, G.S. Prediction based dual authentication model for VANET. In Proceedings of the 2017 International Conference on Computing Methodologies and Communication (ICCMC), Erode, India, 18–19 July 2017.
37. Waghmode, R.; Gonsalves, R.; Ambawade, D. Security enhancement in group based authentication for VANET. In Proceedings of the 2016 IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT), Bangalore, India, 20–21 May 2016.
38. Dolev, S.; Krzywiecki, Ł.; Panwar, N.; Segal, M. Vehicle authentication via monolithically certified public key and attributes. *Wirel. Netw.* **2015**, *22*, 879–896. [CrossRef]
39. Kumar, A.; Prakash, A.; Sharma, S.; Jyoti, K. Vehicle authentication and message hiding protocol for vehicle to vehicle communication. In Proceedings of the 2015 1st International Conference on Next Generation Computing Technologies (NGCT), Dehradun, India, 4–5 September 2015.
40. Huth, C.; Zibuschka, J.; Duplys, P.; Guneysu, T. Securing systems on the Internet of Things via physical properties of devices and communications. In Proceedings of the 2015 Annual IEEE Systems Conference (SysCon) Proceedings, Vancouver, BC, Canada, 13–16 April 2015.
41. Sun, X.; Men, S.; Zhao, C.; Zhou, Z. A security authentication scheme in machine-to-machine home network service. *Secur. Commun. Netw.* **2012**, *8*, 2678–2686. [CrossRef]
42. Jan, M.A.; Khan, F.; Alam, M.; Usman, M. A payload-based mutual authentication scheme for Internet of Things. *Future Gen. Comput. Syst.* **2019**, *92*, 1028–1039. [CrossRef]
43. Hammi, M.T.; Livolant, E.; Bellot, P.; Serhrouchni, A.; Minet, P. A Lightweight Mutual Authentication Protocol for the IoT. In *Mobile and Wireless Technologies 2017*; Springer: Singapore, 2017; pp. 3–12.
44. Fu, A.; Lan, S.; Huang, B.; Zhu, Z.; Zhang, Y. A Novel Group-Based Handover Authentication Scheme with Privacy Preservation for Mobile WiMAX Networks. *IEEE Commun. Lett.* **2012**, *16*, 1744–1747. [CrossRef]
45. Kumar, P.; Lee, S.G.; Lee, H.J. E-SAP: Efficient-Strong Authentication Protocol for Healthcare Applications Using Wireless Medical Sensor Networks. *Sensors* **2012**, *12*, 1625–1647. [CrossRef] [PubMed]
46. Haddad, Z.J.; Taha, S.; Saroit, I.A. Anonymous authentication and location privacy preserving schemes for LTE-A networks. *Egypt. Inform. J.* **2017**, *18*, 193–203. [CrossRef]
47. Lai, C.; Li, H.; Lu, R.; Shen, X.S. SE-AKA: A secure and efficient group authentication and key agreement protocol for LTE networks. *Comput. Netw.* **2013**, *57*, 3492–3510. [CrossRef]
48. Sbeyti, H.; El Hage, B.; Fadlallah, A. Mobile user signature extraction based on user behavioural pattern (MUSEP). *Int. J. Pervasive Comput. Commun.* **2016**, *12*, 421–446. [CrossRef]
49. Aman, M.N.; Chua, K.C.; Sikdar, B. Mutual Authentication in IoT Systems Using Physical Unclonable Functions. *IEEE Internet Things J.* **2017**, *4*, 1327–1340. [CrossRef]
50. Chen, D.; Zhang, N.; Qin, Z.; Mao, X.; Qin, Z.; Shen, X.; Li, X. S2M: A Lightweight Acoustic Fingerprints based Wireless Device Authentication Protocol. *IEEE Internet Things J.* **2016**, *4*, 88–100. [CrossRef]
51. Wallrabenstein, J.R. Practical and Secure IoT Device Authentication Using Physical Unclonable Functions. In Proceedings of the 2016 IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud), Vienna, Austria, 22–24 August 2016.
52. Lu, J.Z.; Chen, T.; Zhou, J.; Yang, J.; Jiang, J. An enhanced biometrics-based remote user authentication scheme using smart cards. In Proceedings of the 2013 6th International Congress on Image and Signal Processing (CISP), Hangzhou, China, 16–18 December 2013.
53. Pranata, I.; Athauda, R.I.; Skinner, G. Securing and Governing Access in Ad-Hoc Networks of Internet of Things. In Proceedings of the IASTED International Conference on Engineering and Applied Science, Colombo, Sri Lanka, 27–29 December 2012; pp. 84–90.
54. Srinivasu, B.; Vikramkumar, P.; Chattopadhyay, A.; Lam, K.Y. CoLPUF: A Novel Configurable LFSR-based PUF. In Proceedings of the 2018 IEEE Asia Pacific Conference on Circuits and Systems (APCCAS),

Chengdu, China, 26–30 October 2018; pp. 358–361.
55. Hammi, M.T.; Hammi, B.; Bellot, P.; Serhrouchni, A. Bubbles of Trust: A decentralized blockchain-based authentication system for IoT. *Comput. Secur.* **2018**, *78*, 126–142. [CrossRef]
56. Dr. Mohammed Abdul Bari,Arul Raj Natraj Rajgopal, Dr.P. Swetha ," Analysing AWSDevOps CI/CD Serverless Pipeline Lambda Function's Throughput in Relation to Other Solution", International Journal of Intelligent Systems and Applications in Engineering , JISAE, ISSN:2147-6799, Nov 2023, 12(4s), 519–526
57. Mr. Pathan Ahmed Khan, Dr. M.A Bari,: Impact Of Emergence With Robotics At Educational Institution And Emerging Challenges", International Journal of Multidisciplinary Engineering in Current Research(IJMEC), ISSN: 2456-4265, Volume 6, Issue 12, December 2021,Page 43-46
58. Shahanawaj Ahamad, Mohammed Abdul Bari, Big Data Processing Model for Smart City Design: A Systematic Review ", VOL 2021: ISSUE 08 IS SN : 0011-9342 ;Design Engineering (Toronto) Elsevier SCI Oct : 021