

Architectural Threats to Security and Privacy: A Challenge for Internet of Things (IoT) Applications

by Nur Agus Salim

Submission date: 17-Dec-2023 09:01PM (UTC-0500)

Submission ID: 2261504962



File name: electronics-12-00088.pdf (3.49M)

Word count: 10749

Character count: 80804

Review

Architectural Threats to Security and Privacy: A Challenge for Internet of Things (IoT) Applications

Yasser Khan ^{1,2}, Mazliham Bin Mohd Su'ud ^{1,*}, Muhammad Mansoor Alam ³ , Sayed Fayaz Ahmad ⁴, Nur Agus Salim ⁵  and Nasir Khan ⁶

- ¹ Research Management Center, Multimedia University, Cyberjaya 63100, Malaysia
 - ² Department of Electrical Engineering, Iqra National University, Peshawar 25100, Pakistan
 - ³ Faculty of Computing, Riphah International University, Islamabad 46000, Pakistan
 - ⁴ Department of Engineering Management, Institute of Business Management, Karachi 75190, Pakistan
 - ⁵ Elementary School Teacher Education, Universitas Widya Gama Mahakam Samarinda, Kota Samarinda 75243, Indonesia
 - ⁶ Department of Petroleum & Gas Engineering, University of Chakwal, Chakwal 48800, Pakistan
- * Correspondence: mazliham@mmu.edu.my

Abstract: The internet of things (IoT) is one of the growing platforms of the current era that has encircled a large population into its domain, and life appears to be useless without adopting this technology. A significant amount of data is generated from an immense number of smart devices and their allied applications that are constructively utilized to automate our daily life activities. This big data requires fast processing, storage, and safe passage through secure channels to safeguard it from any malicious attacks. In such a situation, security is considered crucial to protect the technological resources from unauthorized access or any interruption to disrupt the seamless and ubiquitous connectivity of the IoT from the perception layer to cloud computers. Motivated by this, this article demonstrates a general overview about the technology and layered architecture of the IoT followed by critical applications with a particular focus on key features of smart homes, smart agriculture, smart transportation, and smart healthcare. Next, security threats and vulnerabilities included with attacks on each layer of the IoT are explicitly elaborated. The classification of security challenges such as confidentiality, integrity, privacy, availability, authentication, non-repudiation, and key management is thoroughly reviewed. Finally, future research directions for security concerns are identified and presented.

Keywords: internet of things; IoT architecture; security challenges; privacy



Citation: Khan, Y.; Su'ud, M.B.M.; Alam, M.M.; Ahmad, S.F.; Salim, N.A.; Khan, N. Architectural Threats to Security and Privacy: A Challenge for Internet of Things (IoT) Applications. *Electronics* **2023**, *12*, 88. <https://doi.org/10.3390/electronics12010088>

Academic Editors: Yoshiyasu Takefuji, Subhas Mukhopadhyay and Enrico Vezzetti

Received: 6 November 2022
Accepted: 6 December 2022
Published: 26 December 2022



Copyright: © 2022 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

The internet of things (IoT) has emerged from conventional internet technology with immense capabilities to establish a strong interconnection between humans and machines and machines and machines by utilizing numerous sensing and actuating devices. The intelligence in the omnipotent technology of the IoT is made possible because of the integration of various cutting-edge contemporary technologies of data science, wireless sensory networks, edge and fog computing, and big data analytics. Moreover, notable progress in the wireless discipline of information and communication technology, electromechanical devices, and industrial types of equipment designs have greatly expanded the scope of the internet of things [1,2]. In addition, the management of IoT networks has become challenging as it grows exponentially. Different objects networked in the internet of things are automatically interacting with one another and are determined according to pre-design communication protocols without the involvement of human beings [3]. The IoT has a pivotal role in managing the day-to-day activities of humans. Thus, a significant amount of human effort and time is saved by the effective coordination of connected sensors and

actuators designed to perform specific tasks in a smart home. Similarly, the IoT has significantly provided a solution to assist physically disabled people without making much effort. The occupancy sensors are installed to detect the motion of humans that consequently turn on/off the lights and fan. The energy consumption bill is lowered through the implementation of the internet of things. People risk various natural calamities such as tsunamis, earthquakes, and floods and are timely evacuated by the early warning of integrated technology of the IoT through remotely installed sensing devices. Likewise, the IoT has automated many tasks of industries, healthcare, supply chain management, crop yield, and other business firms.

With the increased use of IoT devices in the home and commercial entities, there is a great risk of extracted data from smart gadgets being compromised. Intruders can illegally penetrate these networks and access data without being detected for a longer period. These hackers can bypass the security setup and gain access to the internet of things ecosystem without being identified, authenticated, and authorized. As these smart objects are interconnected and exchange information through open-channel internet connections, they allow attackers to carry out any malicious activities without informing anyone, as presented in Figure 1. Presently, the IoT environment is confronted with numerous security issues such as access control, privacy, verification, authorization, data management, and storage [4]. Smartphones are fulfilling human needs by providing global connectivity with the help of the digital environment; however, the security of information flow is never guaranteed. Attackers arrange to intercept users' signals, so the privacy of IoT users is critically breached. The confidence of the internet of things users can simply be ascertained in the adoption of technology by addressing the privacy and control of secure personal data [5]. In short, the enhancement of the IoT is subject to the resolution of security issues.

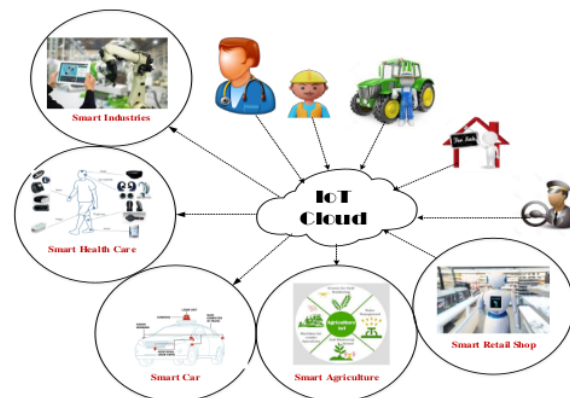


Figure 1. Smart Objects.

The overall connectivity of IoT objects with the internet has made them prone to malicious attacks. Mainly, traditional data dissemination schemes are responsible for these kinds of assaults. Temporary measures such as gossiping, gradient-based routing, directed diffusion, and one-phase pull diffusion are not adequate to secure the IoT from threats. Some loopholes such as data validation, verification of data packets, data maintenance, the latency of the network, and security requirements need to be addressed in prevailing dissemination schemes. Furthermore, the end-to-end security of the IoT is conditional on the safety of its elements and networks. As networking and other related objects are new to implementing the IoT, security is not given a high priority during the design of products [6]. IoT security and privacy challenges can be overcome by intercepting eavesdropping, spoofing, and malicious signal injection. These assaults are adversely affecting security such as authenticity, reliability, and privacy-related features. Thus, it is mandatory on the part of the network operator to redress these issues to safeguard IoT products and services.

In case of any hacking attacks, the user data are accessed and exploited for malicious intentions, and IoT services are severely interrupted and, thus, shoulder the responsibility of the service provider to secure the network against any cyber-attacks [7]. Because the number of connected IoT devices are exceeding 50 billion with users of wide and diverse backgrounds, naturally, the security of these gadgets and data has attained paramount importance and has become a hot topic in the industrial sector [8]. Due to the increase in heterogeneity of IoT networks, the security complexities also enhance in intricacy as well. Moreover, access control is posing a big threat to data from different sources; hence, it is mandatory to provide legal access to the user for authenticity, confidentiality, and integrity.

This research article is intended to analyze and review the privacy and security issues related to the IoT. The paper is organized as follows: Section 2 comprises the basic architecture of the IoT and its layers. In Section 3 of the article, smart applications, for instance, home, agriculture, transportation, and healthcare of the IoT, and the corresponding security issues, are identified and examined. In Section 4, security threats and vulnerabilities are introduced and confronted with each layer of the IoT. In Section 5, the security challenges are classified into seven different classes to elaborate on the threats of the IoT with the help of different models. Finally, in Section 6, the concluding remarks are added.

2. Internet of Things (IoT) Architecture

The internet of things is broadly categorized into three layers based on architecture. Each layer performs its predefined functionalities without overlapping the task of one another. Each layer of the IoT is meticulously designed to tackle the crucial phenomena of privacy and security. Addressing security issues in each layer will protect the entire IoT system against any malicious attacks, as depicted in Figure 2.

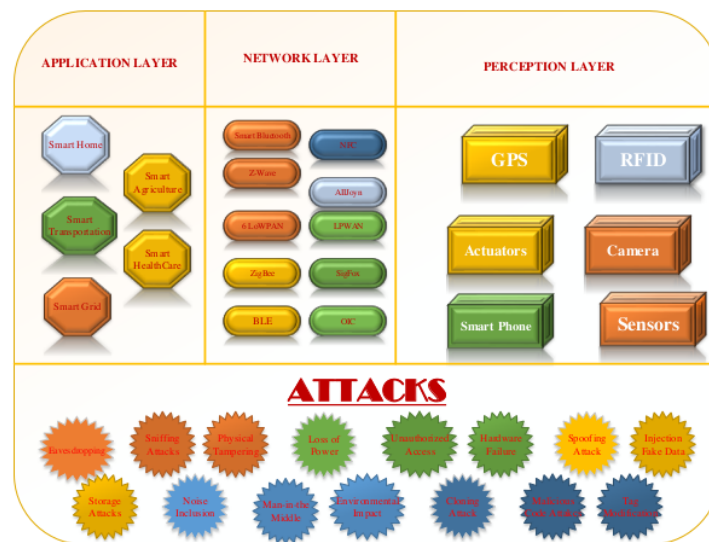


Figure 2. IoT Layered Architecture and Attacks.

2.1. Sensing Layer

This layer is alternatively called the Recognition Layer, Perception Layer, Sensory Layer, and Device Layer. This layer is responsible for sensing the environment-related data and the further submission to the communication layer for onward transmission to data warehouses or the cloud. The number of sensing devices in this layer are varied according to the practical requirement of the internet of things application, and data are collected in a plug-and-play mechanism [9]. The purpose of the layer is to collect the

data from the real world and store the information for further processing in the controller. Various physical parameters such as light, humidity, and location are sensed from the surroundings and are designed to perform the function of identification on the basis of distinct features. The smart gadgets in the sensing layer can also be programmed to execute the mechanical function as per sensing and processing information. Moreover, to minimize human interaction, devices in the layer can work in collaboration among heterogeneous devices. To enhance the scalability, devices in the layer can be configured into the mesh, ad-hoc, and multi-hop environment. The common devices used are Radio-Frequency Identification (RFID) readers, the Global Positioning System (GPS), Quick-Response (QR) code readers, Bluetooth devices, and numerous types of sensors [10].

2.2. Communication Layer

This layer normally known as the Network Layer or Transport Layer provides integration of a variety of protocols, technologies, and heterogeneous networks. To decide on behalf of the IoT system, the data perceived by the Perception Layer are transmitted for processing (Data Mining, Aggregation, and Encoding) through this layer. The Core Network in this layer acts as the backbone for the transmission of information. The internet has a significant role in internetworking, communicating physical items, and observing and controlling the actuators remotely [11]. The scope of geographically distributed networked devices is broadened through Wide Area Networks (WANs).

2.3. Application Layer

It consists of applications that are purposed to control and manage functionalities of the network globally. At the service layer, the decision is made based on processed data collected from the perception layer. Several intelligent processing and computational actions are conducted on the score of the enterprise services platform. Other activities such as data filtration, recognition, and categorization into spam, valid, and non-valid are also carried out at this layer of the IoT. Furthermore, the quality of service and directory service is ensured through service-oriented architecture. In addition, middleware functionalities such as intelligent computations, cloud computing, and the machine-to-machine application models service support platform is performed by the service layer [12]. Examples of consumer-oriented applications at this layer of the IoT are smart healthcare, smart homes, logistics and retail, intelligent transportation, safety and surveillance, resource and energy management, and smart cities. The application of the internet of things is made more accessible and user-friendly through numerous hand-held smart gadgets, for instance, laptops, mobile, and personal digital assistants.

3. Applications of the Internet of Things

The internet of things has numerous applications in a variety of real-life fields.

3.1. Smart Home

The term is frequently used for the application of innovative technologies such as artificial intelligence and the internet of things to create more ease and facilities in the home. Other related attributes are the capability to obtain information from surrounding areas and to receive responses accordingly [13]. The overall aims of introducing smart technologies are to upgrade the well-being of humans, and it has emerged as a strong pillar of innovative technologies [14]. The paradigm shifts of turning routine products and services into smart ones have revolutionized the technologies and have assisted to create the awareness of interoperability among heterogeneous devices [15]. The immense advantages of implanting small gadgets in the home to achieve significant objects have captured the attention of not only academicians but also the service providers in the IoT [16]. The functionalities of a smart home are drawn in Table 1 in the form of the type of IoT devices intended to realize the smart home and the purpose of the devices. Lifestyle and health-related

monitoring, automation for kitchenware, remote control, entertainment, and provisioning smart environments are key attributes of a smart home.

Table 1. Home Functionalities.

IoT Devices Installed at Smart Home	Purpose
Blood Pressure machine Temperature sensor Glucose level machine Physiological signs monitor Heart rate EGG for an epileptic, sleep disorder, Seizure Infrared Sensors Wearable Accelerometer Wearable Sensors Tele-healthcare	Upgradation of Lifestyle and Health
Kitchenware Washing	Automation
House Gates Windows Garden Wardrobe	Remotely controlled
TV Internet Laptop	Smart Entertainment
Heating and Ventilation Electricity Gas	Comfortable environment

3.2. Smart Agriculture

With the innovations of the latest sensor technologies in the IoT, the traditional way of farming has been fundamentally modified. Numerous farming issues have been redressed by the effective integration of wireless sensors that were previously impossible, for instance, pest control, yield optimization, drought response, and suitability of land. IoT sensors have a crucial role to acquire field information and conditions in the implementation of smart agriculture, as illustrated in Table 2. These smart objects are abundantly implanted in advanced agriculture machinery and tools as per the requirement.

Table 2. IoT involvement in Smart Agriculture.

Smart Agriculture Sensors	Function	Application
Acoustic Sensor	Work on the changes in noise level	Pest identification and detection [17], seed classification [18]
Optoelectronic Sensor	Differentiation of plant type	Detect herbicides, weeds, and unwanted plants [19], differentiation of soil and vegetation based on reflection spectra [20]
Airflow Sensor	Measure the moisture contents and air permeability	Determine different soil characteristics, e.g., structure, moisture, and compaction [21]
SWLB (Soft-Water-Level-Based) Sensor	Determine hydrological behaviors	Measure the stream and water flow, rainfalls [22]
Electromagnetic Sensors	Record the electromagnetic response and electrical conductivity	Various chemicals such as organic matter and nitrates [23]
Mechanical Sensors	Soil mechanical resistance based on pressure	Different levels of compaction [24]
Eddy Covariance-Based Sensor	Determine continuous flux on a large part of land [25]	Gases exchange quantification, that is, carbon dioxide, methane, and water vapor [26]
Optical Sensor	Soil's capability to the reflection of light [27]	Soil moisture, organic substance, and clay contents and minerals [28]
Ultrasonic Ranging Sensors	Work in association with the camera [29]	Uniform spray coverage, and tank and crop canopy monitoring [30]
Telematics Sensors	Collection of data from non-accessible points to avoid visits [31]	Reduce environmental effects through data management [32]

Table 2. Cont.

Smart Agriculture Sensors	Function	Application
Remote Sensing	Management and manipulation of geographical data [33]	Identification of pests and plants, degradation mapping, land cover, and yield dates forecasting and modeling [34]
FPGA (Field-Programmable Gate Array based) Sensor	Real-time monitoring due to reconfiguration flexibility but high cost [35]	Transpiration, humidity, and irrigation [36]
Electrochemical Sensor	Chemical analysis of soil [37]	Soil characteristics are pH, salinity, and soil macro- and micronutrients [38]
LIDAR (Light Detection & Ranging)	Estimation of dynamic measurement of agriculture data [39]	Monitoring erosion, 3-D modeling, and land mapping and segmentation [40]
Mass Flow Sensors	Measure the quantity of grain flow [41]	Grain moisture contents [42]

3.3. Smart Transportation

The Intelligent Transportation System (ITS) has created numerous opportunities in terms of navigation, route optimization, reduction in energy consumption and car emissions, and detection of traffic conditions based on streetlights and smart parking systems [43]. Smart parking reservation systems with the aid of visual devices, infrared sensors, and magnetic fields allow the reduction in searching time and availability of space at parking lots [44]. Information regarding road surfacing provided by implanted sensors is communicated to the application of handheld devices for taking timely action to avoid any accidents, as demonstrated in Table 3. Furthermore, an organized accident prevention system is also developed by using IoT smart gadgets. Moreover, vehicles are managed to exchange information not only with other vehicles but also with a social network in a machine-to-machine IoT system that has opened the floodgates of new avenues and possibilities [45]. The security issues related to connected and autonomous vehicles (CAVs) have been thoroughly reviewed to apply safe and reliable practices in intra- and inter-vehicle systems. The self-driving vehicle could be protected against cyberattacks by the application of AI practices [46].

Table 3. Key Features of Intelligent Transport System.

Intelligent Transport	Features
Accident Prevention	<ul style="list-style-type: none"> • Real-time monitoring of vehicles [47] • Vehicle-to-vehicle communication • Vehicle-to-social-network communication • Detection of blind spots by smart vehicles [48] • Traffic congestion detection [49] • The consciousness of drivers is continuously monitored [50] • Identification of accident-prone areas [51] • Detection of any obstacles or elements in the street [52]
Parking System	<ul style="list-style-type: none"> • Identification of free parking lots and creation of image [53] • Creation of parking lot databases [54] • Installation of smart signboards [55] • Availability inside the park is ensured through ultrasonic sensors [56] • Payment for the parking is made through the Android app • Furthermore, parking preferences are made by ASPIRE [57] • Communication to the local cloud is carried out with a private cloud server [58]
Road Condition	<ul style="list-style-type: none"> • Detection of potholes and bumps is processed with FF-NN [59] • Difficulties regarding the detection of distress are conducted [60]
Smart Street Light	<ul style="list-style-type: none"> • Lower the energy consumption and provide dynamic operation • The intensity of lights is adjusted according to the crowd in areas • The location of SSL is updated by GPS • ON/OFF of SSL are triggered by light sensors to save energy [61] • Wi-Fi hotspot transmits the information to the central server [62]

Table 3. Cont.

Intelligent Transport	Features
Transport Infrastructure	<ul style="list-style-type: none"> • M2M communication provides V2V (vehicle-to-vehicle) framework [63] • Near cars, location, and speed and movement data are fed to cars locally • User experience is promoted through the bus fleet monitoring system • IoT is combined with social network principles into the Social Internet of Vehicles • Congestion in communication is decreased by protocol (VSNP) [64]
Optimization of Route	<ul style="list-style-type: none"> • The opted best route for a specific location reduces congestion • Fuel consumption and time to travel are decreased • SERSU approach along with weather condition, pollution sensors, and camera optimize the route • Shortest time and path estimation is performed by crowdsourcing route planning [65]

3.4. Smart Healthcare

Comprehensive and intelligent health systems are used to coordinate the people from the different relevant departments that respond actively to the medical ecosystem with the assistance of the IoT, wearable devices, and mobile applications along with features, as shown in Table 4. The allocation of required resources and informed decisions is accordingly made. In other words, the information and communication system become part of the healthcare system [66].

Table 4. Key Features of Intelligent Healthcare System.

Intelligent Health Care	Features
Health Management	<ul style="list-style-type: none"> • Chronic diseases are confronting new challenges in terms of cost and treatment [67] • Traditional health model is not adequately capable to deal with disease [68] • Feedback of health data, self-management, and intervention doctors are possible with the application of IoT • Physiological indicators are received and monitored by implantable devices • Prognosis of abnormalities, if appropriately monitored, will lower risk [69] • Smartphone integrated with biosensors monitors the body and environment [70] • A healthy lifestyle is also associated with the implementation of smart home [71] • Integrated management strengthens medical decisions, resource utilization, and cost [72] • Numerous online facilities such as doctor–patient interactions, online appointments, and examinations [73]
Diagnosis and Treatment	<ul style="list-style-type: none"> • It happens more precise and accurately with the emergence of IoT, AI, and robots • AI diagnosis accuracy has surpassed human decisions [74] • IBM Watson is simply exemplary in clinical decision support systems [75] • In the treatment of tumors, the process can be dynamically observed through radionics [76] • Fast recovery and better results can be achieved by the involvement of robots in surgery even remotely [77] • Subversive changes are brought about due to clinical treatment and medical education [78]
Drug Research	<ul style="list-style-type: none"> • It comprises discovery of drugs, target screening, and clinical trials • Traditionally overlooked and slow target screening is significantly fast, e.g., genomic study [79] • The discovery efficiency of compounds for a drug can be improved [80]

Table 4. Cont.

Intelligent Health Care	Features
Smart Hospital	<ul style="list-style-type: none"> • ICT infrastructure in hospitals is automated and optimized by IoT [81] • Services for medical, patient, and administrators are the main components of smart hospitals • IoT helps to identify instruments, biological specimens, and staff management • It also has a critical role in inventory management, circulation, drug production, and anti-counterfeiting [82] • Decision-making on the part of performance and quality analysis lowers the cost and increases the utilization of resources • Overall benefits include shorter waiting time, concise treatment process, online appointments, and increased doctor–patient interaction
Virtual Assistance	<ul style="list-style-type: none"> • Algorithm virtual assistance helps in language understanding and session experience [83] • VA actively responds to parties, saving both material resources and manpower [84] • VA plays a responsible role to treat mentally ill patients and bring spiritual health to the patient [85]
Disease prevention and Risk Monitoring	<ul style="list-style-type: none"> • Results on data from wearable devices are analyzed and uploaded to the cloud in real-time [86] • Human lifestyle and behavior are adjusted by integrated and connected systems [87]

4. Security Threats and Vulnerabilities in IoT

In “*Authorized Access*”, the devices are physically protected to deny any access. The majority of IoT devices are vulnerable to intruding into devices without obtaining any permission from an authorized service provider, as detailed in Figure 3. In the internet of health things, sensitive wearable gadgets to monitor human health are accessed and authenticated by the hospital authority. Meanwhile, in “*Sniffing-Attacks*”, malicious sensors or authorized gadgets are placed on IoT devices to establish a link to working devices. During communication, spy devices capture data and further exploit them for malicious intentions. “*Physical Tampering*” normally occurs in an unattended environment and IoT elements are mainly susceptible to physical harm through the change in hardware. In another scenario of “*Loss of Power*”, the energy of IoT devices is accessibly consumed, turning objects off undesirably. To counter the attack, the power-saving strategy of the sleep mode is introduced by manufacturers. The IoT devices are adversely affected by “*Environmental-Attacks*” by applying extreme heat, cold, wind, snow, or rain. Hence, the operation of sensing objects is made unstable and unreliable in such a harsh environmental situation. Sometimes, attackers use “*Hardware Failure*” to attack internet of things devices, resulting in the wrong or incomplete information badly damaging the data stream. Thus, the wrong decision is taken based on misinformation, and RFID systems do not support any encryption scheme, because of memory limitation, so intruders’ endeavor to implant their transmitter to misguide or hack the entire system, normally termed “*Eavesdropping*”. The big data acquired from IoT devices is uploaded to fog or cloud computers and is arranged to store over each other. IoT devices perform their function as per the installed memory. However, in the case of compromise such as “*Storage Attacks*”, the linked internet of things items is adversely affected; hence, the protection of this storage is pivotal to smooth the operation of the system. In the internet of things, the exchange of information takes place through wireless communication. High-frequency impulses or undesirable “*noise*” can seriously interrupt and cause packet loss at the receiving end.

The communication path in the “*Man-in-the-Middle Attack*” is hacked by intruders and manipulated data are provided to the intended devices. The receiving devices remain unaware of misinformation; however, in the case of invalid data entry, the compromised network considers this error in the network [88]. Protection at the perception layer has become possible due to low-price sensory gadgets. Normally, “*Spoofing*” is the phenomenon of copying the Tag information and forwarding it to an RFID reader; however, attackers arrange to place data on the fake tag to obtain an illegitimate advantage [89]. Similarly, whenever a clone Tag is used to download network data from the transmitter and copy

it for malicious intention, it is called a “Cloning Attack”. Both spoofing and cloning are generally categorized as the same menace. Spoofing is a process of transferring the data on new data, while, in later cases, captured data are corrupted and the sender is misguided. Through “Malicious Code Attacks”, malware is introduced on the internet to attack a specific operating system. In this scenario, the connected devices operate abnormally, which become disastrous in sensitive applications such as a self-driving car. The attackers in “Tag Modification” exploit the modifiable tag to fulfill their malicious intention. In the majority of the cases, RFID tags are widespread and read-only but intruders search for the vulnerable tag and delete/modify the valuable information. To counter the assault, a read and write protection policy must strictly be implemented to avoid any damage and sensitive information. The inappropriate reaction observed in the system, whenever fed with the wrong information, is termed as an “Injecting Fake Data Attack”. Numerous “Wi-Fi-based attacks” are experienced in IoT-based network infrastructure where ciphering of the stream is compromised to recover the encryption key to determine the initialization vectors.

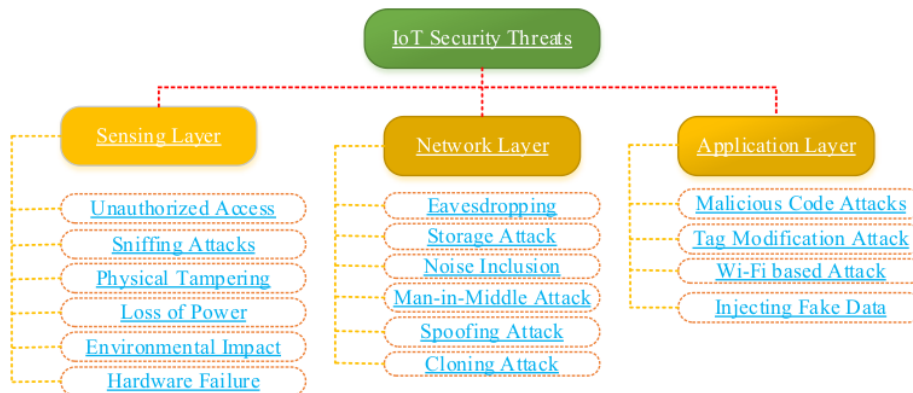


Figure 3. IoT Security Threats.

5. Classification of Security Challenges of the Internet of Things

Major security challenges confronted with IoT technologies are confidentiality, integrity, privacy, availability, authenticity, non-repudiation, and key management, as provided in Figure 4.

A significant amount of data is generated by internet of things items that require collection, processing, and onward submission for storage. The data comprised personal, commercial, and business confidentialities that must be protected against any possible attacks.

- I. In the context of business scenarios, data are a valuable asset to remain competitive in the market. The traditional treatment through “confidentiality” algorithms is not adequate to handle resource scarcity, heterogeneity, and scalability of data. To ensure the confidentiality of the IoT system, access control, authentication, and supervision of the network need strict compliance. Confidentiality of the data is compulsory to predict and estimate real-world problems. An IoT-based earlier warning system for tsunamis or earthquakes has a significant role in the evacuation of the population at risk to safeguard human life. The data obtained from the system must be accessible only to the pertinent body and disaster management department that issues necessary guidelines from time to time. The indiscriminate spread of such sensitive information may cause panic, unrest, hazards, public disorder, and law and order situations among a large group of people that may become out of control in some cases. Likewise, food company data of biosensors on bacterial composition must safely be stored and remain confidential. The leakage of the data may severely damage a firm’s reputation

and competitive advantage over competitors. The confidentiality of IoT data cannot directly be dealt with by customer solutions, due to scalability and changing access rights. To manage knowledge systems, trust-based techniques remain effective to handle the sheer amount of IoT data, out of which Role-Based-Access-Control is standard and has emerged as successful as compared to traditional access control, as illustrated in Figure 5. Each departmental user has different roles and permissions; however, access rights can be altered by dynamically modifying role assignments. In the context of the IoT as compared to a static database, the entire stream in real-time can be accessed through RBAC, termed a data stream management system [90].



Figure 4. Security Challenges of IoT.

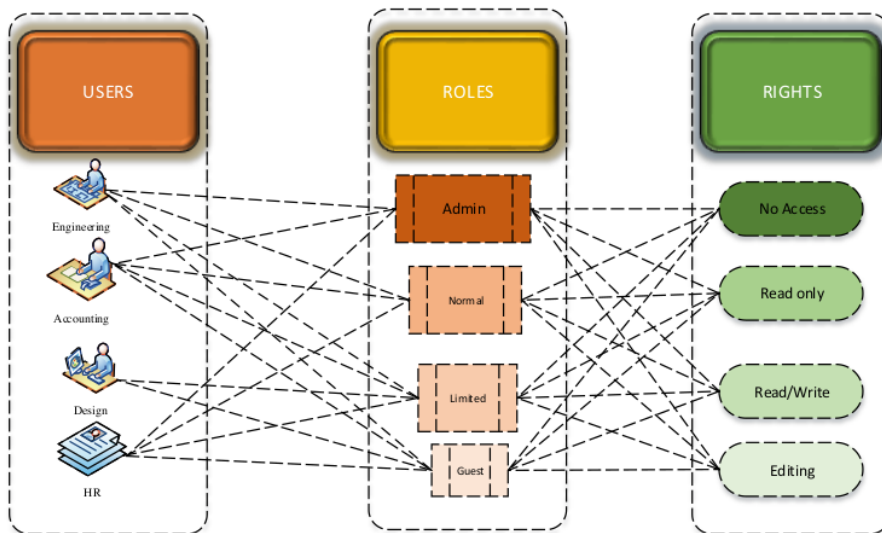


Figure 5. Role-based Access Control.

Furthermore, RBAC is protected against any unauthorized access by applying an operator at the stream level to sort out output tuples to maintain access control. In the case of the IoT, this approach has weaknesses to define certain control policies for the data from different sources [91]. The layer-wise security challenges confronted by the internet of things (IoT) are illustrated in Table 5.

Table 5. Layer-wise security challenges.

IoT Layers	Security Challenges
Application Layer	<ul style="list-style-type: none"> • Establishment of privacy protection • Authentication among different devices • Flexibility in terms of framework authorization • Key management
Communication	<ul style="list-style-type: none"> • Denial-of-service attack • Encryption of data • Man-in-the-middle attack • Authentication and data access • Creation of communication Session • Availability • Non-repudiation
Sensing Layer	<ul style="list-style-type: none"> • Authentication of the wireless sensory network (WSN) • Confidentiality of network • Integrity • Radio-frequency security issues • Node security and related threats • Creation of fake node • Node authentication

- II. The second challenge associated with the security of the IoT is “*Integrity*”, which means ensuring the data received to/from the perception layer are actual and pure from any kind of alteration. Further processing of manipulated data from sensors will give out erroneous results and, therefore, must not be trusted. The integrity is to be ensured for the internet of things system in general and data in particular [92]. The characteristics of integrity are extremely difficult phenomena to determine that data are received from the first and actual device. Moreover, the protection of information is not possible with the implementation of a password policy. This requires a sophisticated algorithm to establish integrity among devices and their data. In addition, advanced operating systems and configuration patterns support the algorithm. To fully implement integrity, an IoT system has three different states of information to consider that is either in motion, at rest, or in the processing stage. While traveling from the perception layer to communication channels to cloud computers for storage, the information must be protected against any modification in it. In the second stage of integrity, i.e., at the resting stage, the verification of information is carried out during the booting process. During the process in the third stage of integrity, periodic checks are conducted at operations at start-up and end. The sole purpose of a checksum of data during integrity is to make sure neither outer physical interference nor any cybercrime is committed [93]. In this connection, the uniqueness of contents and removal of errors from the data are ensured through CRC (Cyclic Redundancy Check) or Checksum techniques in comparison to traditional approaches of mathematical techniques such as SHA (Secure Hash Algorithm). Previously, the SHA technique was frequently applied; however, abusers arrange to modify the data, and the hash is recalculated; therefore, it becomes ineffective and obsolete [94]. In this connection, the internet of things system is shielded from Man-in-Middle assaults after ensuring that data are unaltered and safely received. The framework in this context is also determined in research endeavors conducted in [95].
- III The third security challenge is “*Privacy*” in which data intended for a specific user can only be accessed. Privacy can be preserved in the internet of health things by exchanging sensitive information between patients and systems. Most of the exchange of data of IoT systems is performed through wireless communication technologies that are always vulnerable to threats and present numerous issues of privacy violations. Some common attacks in this respect are masking and eavesdropping attacks. Hence,

the adoption of the IoT is strong for the resolution of privacy-related matters. Multiple models have been proposed to curtail the privacy problems of the IoT, for instance, Kaos, Tropos, NFR, GPRAM, and PRIS [96].

Out of this, a later model has demonstrated the actual definition of preserving the privacy of the IoT. The prominent feature in the model is the inclusion of comprehensive requirements even in the design phase of the IoT, as depicted in Figure 6 for transformation into rules and further implementation into techniques. The construction of a privacy-preserving mechanism is confronting a score of challenges. However, practical work will be developed from the general privacy model processing all fundamental parts and their intra-model relationship.

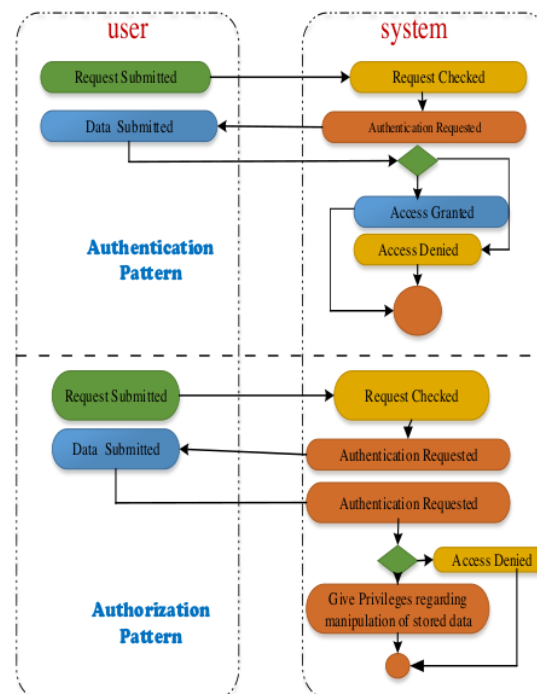


Figure 6. Privacy Requirement of PriS Methods.

- IV. The fourth security challenge is “Availability”, which is alternatively used for reliability and defined as the probability of performance of an element of the network system to give the desired output at a specific time under specific environmental conditions. Availability is particularly used to calculate the performance of any component of a system that becomes operational after recovering from a faulty status. It is worth mentioning that failure in the large-scale internet of things can be disastrous to operations when encountering an emergency in public facilities. It is pivotal to ensure resilience, reliability, and availability in large IoT public network deployment, and this must be included in future research directions [97]. To make reliable internet of things systems, significant numbers of IoT elements are required to be connected to design a large complex network. In addition, the objects should be mobile, and the dynamics and configuration are subject to change as per the network requirements. As the mentioned network is constituted of smart but heterogeneous objects, the interoperability and coordination among them, the environment, the platforms, and the supporting software are to be taken into special consideration. Specific hardware standards have been developed to ensure the reliability of the network of the IoT; the

first attempt in this regard was conducted in the military manual and termed MIL-HDBK-217, adopted by the majority of the engineering fraternity for the calculation of commercial and industrial reliability standards [98]. In contrast, software reliability is performed with numerous models that are not all acceptable, due to the non-specification of requirements, especially in the IoT. Safety and reliability are used in combination for the realization of the mutual goal defined for the software. Another terminology considered with availability is maintainability to obtain the optimal cost of the IoT life-cycle that should be taken into account even in the design phase. In the case of failure, and maintainability of the internet of things, the problematic components should easily be replaced without interruption of service and provide seamless connectivity. A highly maintainable system must produce effective, efficient, and satisfactory output [99].

The availability of IoT systems is described by the given equation:

$$Availability = \frac{Mean\ Time\ to\ failure}{Mean\ Time\ to\ failure + Mean\ Time\ to\ Repair}$$

Other factors such as protocols, security, energy efficiencies, and standardizations influence the phenomena of availability. Out of these parameters, energy efficiency has turned out to be a pressing issue in the domain of sensors. Various low consumptions of energy measures have been proposed in [100]. Keeping in view the failure of smart gadgets, new vulnerabilities in security arise. For example, hacking of self-driving cars and infusion pumps presents a threat and can cost human lives [101].

- V. The fifth security challenge is that “Authentication” is solely required in the internet of things to prevent intrusion into the system and the theft of private information. Normally, the heterogeneous devices connected to the network communicate with the local gateway for the outward provisioning of information. The local gateway obtains necessary permission from the cloud computing system to send the required information to the outside world. To filter out unauthorized persons, application request information must first authenticate to gain access into the network. The phenomenon of approving any smart object or user to grant permission for the collection of network information or data is called authorization, illustrated in detail in Figure 7. It comprises identification, putting requests by the user to the gateway or cloud platform, followed by authorization and authentication. Without following the requisite process, access will not be granted and authentication will fail.

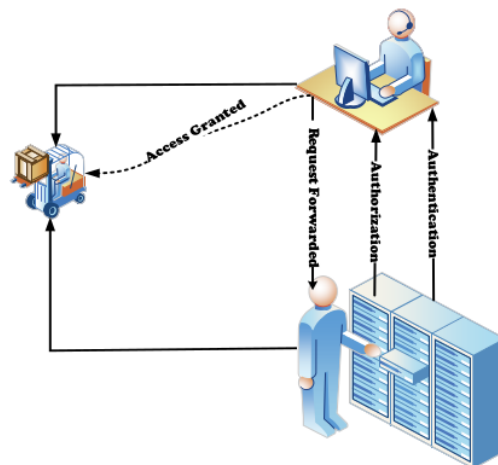


Figure 7. Authentication Process.

Traditionally, the SSL (Secure Socket Layer) has been prevalent by securing secret keys and web platforms on the internet. However, with the emergence of new techniques, passwords are applied less for large-scale internet applications. A similar situation is the case of the IoT to preserve the network from access by an unauthorized user. The IoT consists of a spectrum of large-scale domains such as wearables, smart homes, smart cities, and smart industrial applications. Therefore, it has become impossible to manually collect, analyze, and make the decision without a computer application. By considering the security of the system as the supreme requirement and preventing any damage caused by malicious gadgets, several protocols in this regard are proposed in [102], keeping in view multi-criteria classification. The authentication of the IoT can be classified on the bases of token-based, architecture, procedure, HW-based, IoT layers, and authentication factors [103,104], as depicted in Figure 8.



Figure 8. IoT Authentication.

In token-based authentication [105], an identity token or piece of data is generated by the server. The procedure for authentication involves one, two, or three-way authentication, and out of two parties, only one party, both parties, and a third-party act as a central party, and two interested parties will be authenticated for three types. Based on architecture, the authentication may be distributed or centralized among parties' members. Similarly, it is also divided based on application, network, or perception layers. While defining based on hardware-based (HW-based), it may be implicit or explicit. Authentication factors are the identity (use hash, symmetric, or asymmetric cryptographic algorithms) or context (physical or behavioral).

- VI. The sixth security challenge is "*non-Repudiation*", which is the computational settling of the dispute between the sender and receiver in a case when the sender refuses to send the message and the receiver declines to receive the message. Numerous protocols have been designed to minimize the denying phenomena [106]. In this situation, the distrusted parties may overall create an ineffective way of communication and a lack of promising service provision that unnecessarily causes concerns and anxiety among prime stakeholders. Some traditional non-repudiation mechanisms have been developed and divided into TTP (trusted party)-based approaches and non-TTP-based schemes to determine another way to control impediments to acceptance and development. In the former scenario, TTP plays the role of middleman between the client and service provider and helps to facilitate the exchange of information and acknowledgment of receiving the message [107]. Another method of activation of an off-line TTP service is where the sender provides encrypted data with a TTP key so that the receiver acquires the decrypted service only after obtaining acknowledgment [108]. These phenomena experience performance bottlenecks and single-point failure in distributed IoT systems because of the unavailability of third parties. It is dominated by a non-TTP-based approach in which the service provider manages to forward the message in encrypted form and then provide the true and

fake password for attempting multiple iterations. If the response is not received from the client side, the service provider terminates the process. One of the drawbacks of this scheme is that clients can cheat based on a true password [109]. The process has been further refined by proposing a protocol where the server furnishes part of the decryption key to run a series of iterations. Some disadvantages on the part of non-TTP-based schemes are lacking fairness, the high cost, and the performance issues to iterate for confirmations, which is certainly not possible for the internet of things technology. Currently, reliability and trustworthiness have been enhanced in terms of the security of industrial and transportation IoT by applying a non-repudiation mechanism in electronic events [110]. Furthermore, the non-repudiation mechanisms are digital signature (service provider sends private key and receiver verifies its authenticity), digital watermarking [111] (embedded with unique code for distribution to claim the ownership), sign-encryption [112] (signed by the originator and then encrypted), public key cryptography [113] (integrity and authentication), and certificate cryptography [114] (custody of user's secret key).

- VII. The seventh security challenge is "*Key Management*", which is an integral part of security infrastructure that is responsible for the management of numerous tasks of IoT systems. The key management may be asymmetric, as shown in Figure 9, or symmetric. In this connection, a symmetric-shared key [115] ensures safe and secure communication in resource-constrained IoT devices. The keys generated for the security of the entire system are generated and stored; however, the real issue confronted in the mobile system is their distribution [116]. Various standards and protocols are developed for IoT applications to redress security threats. Although MQTT (message queuing telemetry transport) and CoAPs (constrained application protocols) are frequently used by an IoT that lacks security mechanisms, the security services of SSL (Secure Socket Shell) are utilized [117].

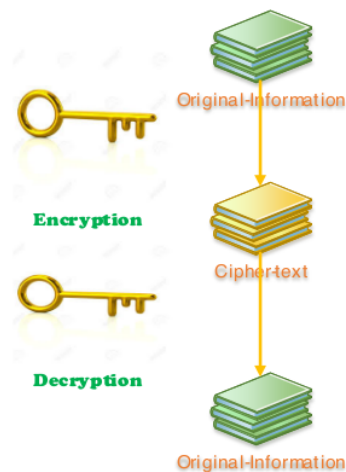


Figure 9. Asymmetric Key Management.

To enhance the security of IoT devices and two-factor authentication, the improved version of single-factor authentication termed KMS is introduced to minimize the associated risk with IoT objects.

6. Conclusions

The internet of things is presently providing an immense number of applications with a significant range of conveniences such as ease of use, efficiency, and cost-effectiveness to end users. The positive trend has been witnessed by market players to invest significantly

due to the sensing and communication potential capabilities of smart objects. This emerging technology has enabled connectivity and interconnection between anything and everything. Fully connected smart gadgets, sensors, and actuators are producing and dispatching significant quantities of data from expanded networks of ubiquitous IoT platforms. However, the dissemination of data on the protected medium is pivotal to safeguarding the interests of end users and service providers.

This article provides an overview of the internet of things (IoT) and its network, which is comprised of a three-layer architecture of the IoT. Various applications of the internet of things with special emphasis on smart agriculture, smart health systems, smart homes, and intelligent transport systems are judiciously discussed to highlight the significant features of the entire arena. We have reserved adequate space to understand and discuss the possible attacks that may adversely affect the data and infrastructure at various layers of the IoT. This indicates that the security and privacy of data are critical areas of data dissemination. The classification of security challenges is the last but not least part of data transportation and storage that is considered future research directions in the area of the internet of things. Furthermore, protocols applicable to security issues of IoT infrastructure and data are greatly proposed.

Author Contributions: The original draft of this endeavor of research was designed and prepared by Y.K. Moreover, M.B.M.S. and M.M.A. have supervised and assisted in determining the methodology of the paper. S.F.A. helped in data curation and formal analysis. N.A.S. and N.K. contributed in visualization, investigation and writing—review and editing. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Acknowledgments: We acknowledge Multimedia University, Malaysia for providing the funding for this research. We also appreciate the role of Iqra National University, Riphah International University, Institute of Business Management, Universitas Widya Gama Mahakam Samarinda and University of Chakwal for providing an opportunity to develop the research paper.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Pourghebleh, B.; Wakil, K.; Navimipour, N.J. A comprehensive study on the trust management techniques in the Internet of Things. *IEEE Internet Things J.* **2019**, *6*, 9326–9337. [CrossRef]
2. Young, S.-J.; Chiou, C.-L. Synthesis and optoelectronic properties of Ga-doped ZnO nanorods by hydrothermal method. *Microsyst. Technol.* **2018**, *24*, 103–107. [CrossRef]
3. Wei, L.; Wu, J.; Long, C. Blockchain-enabled trust management in service-oriented internet of things: Opportunities and challenges. In *Proceedings of the 2021 The 3rd International Conference on Blockchain Technology*, Shanghai, China, 26–28 March 2021; pp. 90–95.
4. Das, R.; Prasad, A. Survey of Blockchain Techniques for IoT Device Security. In *Blockchain Technology*; CRC Press: Boca Raton, FL, USA, 2022; pp. 57–72.
5. Li, S.; Tryfonas, T.; Li, H. The Internet of Things: A security point of view. *Internet Res.* **2016**, *26*, 337–359. [CrossRef]
6. Choo, K.R.; Dehghantanha, A.; Parizi, R.M. *Blockchain Cybersecurity, Trust and Privacy*; Advances in Information Security; Springer: Berlin/Heidelberg, Germany, 2020; Volume 79, pp. 28–29.
7. Sour, A.; Hussien, A.; Hoseyninezhad, M.; Norouzi, M. A systematic review of IoT communication strategies for an efficient smart environment. *Trans. Emerg. Telecommun. Technol.* **2022**, *33*, 3736. [CrossRef]
8. Gajewski, M.; Batalla, J.M.; Mastorakis, G.; Mavromoustakis, C.X. Anomaly traffic detection and correlation in smart home automation IoT systems. *Trans. Emerg. Telecommun. Technol.* **2020**, *33*, e4053. [CrossRef]
9. Perera, C.; Zaslavsky, A.; Christen, P.; Georgakopoulos, D. Context-aware computing for the internet of things: A survey. *IEEE Commun. Surv. Tutor.* **2013**, *16*, 414–454. [CrossRef]
10. Tamrakar, A.; Shukla, A.; Kaliyfullah, A.; Reegu, F.; Shukla, K. extended review on internet of things (IoT) and its characterization. *Int. J. Health Sci.* **2022**, *10*, 234.

11. Raza, U.; Kulkarni, P.; Sooriyabandara, M. Low power wide area networks: An overview. *IEEE Commun. Surv. Tutor.* **2017**, *19*, 855–873. [\[CrossRef\]](#)
12. Ngu, A.H.; Gutierrez, M.; Metsis, V.; Nepal, S.; Sheng, Q.Z. IoT middleware: A survey on issues and enabling technologies. *IEEE Internet Things J.* **2016**, *4*, 1–20. [\[CrossRef\]](#)
13. Kim, H.; Choi, H.; Kang, H.; An, J.; Yeom, S.; Hong, T. A systematic review of the smart energy conservation system: From smart homes to sustainable smart cities. *Renew. Sustain. Energy Rev.* **2021**, *140*, 110755. [\[CrossRef\]](#)
14. Bakhshi, K.K.; Rahmani, A.M.; Sabbagh Molahosseini, A. A fault-tolerant architecture for internet-of-things based on software-defined networks. *Telecommun. Syst.* **2021**, *77*, 155–169. [\[CrossRef\]](#)
15. Hong, J.; Shin, J.; Lee, D. Strategic management of next-generation connected life: Focusing on smart key and car-home connectivity. *Technol. Forecast. Soc. Chang.* **2016**, *103*, 11–20. [\[CrossRef\]](#)
16. Khedekar, D.C.; Truco, A.C.; Oteyza, D.A.; Huertas, G.F. Home automation—A fast-expanding market. *Thunderbird Int. Bus. Rev.* **2017**, *59*, 79–91. [\[CrossRef\]](#)
17. Coughlan, T.; Mackley, K.L.; Brown, M.; Martindale, S.; Schlögl, S.; Mallaband, B.; Arnott, J.; Hoonhout, J.; Szostak, D.; Brewer, R.; et al. Current issues and future directions in methods for studying technology in the home. *Psychology J.* **2013**, *11*, 159–184.
18. Bhugubanda, M.; Rao, S.L.A.; Shanmukhi, M.; Rao, A. Sustainable And Intelligent IoT Based Precision Agriculture—Smart Farming. *Solid State Technol.* **2020**, *63*, 17824–17833.
19. Mankin, R.; Hagstrum, D.; Guo, M.; Eliopoulos, P.; Njoroge, A. Automated applications of acoustics for stored product insect detection, monitoring, and management. *Insects* **2021**, *12*, 259. [\[CrossRef\]](#)
20. Joshi, V.; Adhikari, M.S. IoT-Based Technology for Smart Farming. In *Electronic Devices and Circuit Design*; Apple Academic Press: Palm Bay, FL, USA, 2022; pp. 223–242.
21. Pisman, T.I.; Erunova, M.G.; Botvich, I.Y.; Emelyanov, D.V.; Kononova, N.A.; Bobrovsky, A.V.; Kryuchkov, A.A.; Shpedt, A.A.; Shevyrnogov, A.P. Information Content of Spectral Vegetation Indices for Assessing the Weed Infestation of Crops Using Ground-Based and Satellite Data. *Izv. Atmos. Ocean. Phys.* **2021**, *57*, 1188–1197. [\[CrossRef\]](#)
22. Islam, N.; Rashid, M.M.; Pasandideh, F.; Ray, B.; Moore, S.; Kadel, R. A review of applications and communication technologies for internet of things (IoT) and unmanned aerial vehicle (UAV) based sustainable smart farming. *Sustainability* **2021**, *13*, 1821. [\[CrossRef\]](#)
23. Mukhopadhyay, S.C.; Nag, A.; Gooneratne, C. Printed and flexible sensors: A review of products and techniques. In *Printed and Flexible Sensor Technology*; IOPscience: Bristol, UK, 2021; p. 11.
24. Garcia, A.P.; Umez, C.K.; Polania, E.C.M.; Neto, A.F.D.; Rossetto, R.; Albiero, D. Sensor-Based Technologies in Sugarcane Agriculture. *Sugar Tech.* **2022**, *24*, 679–698. [\[CrossRef\]](#)
25. Brown, S.; Wagner-Riddle, C.; Debruyn, Z.; Jordan, S.; Berg, A.; Ambadan, J.T.; Congreves, K.A.; Machado, P.V.F. Assessing variability of soil water balance components measured at a new lysimetric facility dedicated to the study of soil ecosystem services. *J. Hydrol.* **2021**, *603*, 127037. [\[CrossRef\]](#)
26. Kumar, A.; Bhatia, A.; Fagodiya, R.K.; Malyan, S.K.; Meena, B.L. A Promising Technique for Greenhouse Gases Measurement Eddy Covariance Flux Tower. *Adv. Plants Agric. Res.* **2017**, *7*, 337–340.
27. Murray, S.C. Optical sensors advancing precision in agricultural production. *Photon. Spectra* **2018**, *51*, 48.
28. Povh, F.P.; Anjos, W.d.G.d.; Yasin, M.; Harun, S.W.; Arof, H. Optical sensors applied in agricultural crops. In *Optical Sensors-New Developments and Practical Applications*; IntechOpen: London, UK, 2014; pp. 141–163.
29. Upendar, K.; Agrawal, K.N.; Vinod, K.S. The Role of Sensing Techniques in Precision Agriculture. In *Machine Vision for Industry 4.0*; CRC Press: Boca Raton, FL, USA, 2022; pp. 63–78.
30. Gómez Álvarez-Arenas, T.; Gil-Pelegrin, E.; Cuello, J.E.; Fariñas, M.D.; Sancho-Knapik, D.; Burbano, D.A.C.; Peguero-Pina, J.J. Ultrasonic sensing of plant water needs for agriculture. *Sensors* **2016**, *16*, 1089. [\[CrossRef\]](#)
31. Sharma, V.; Tripathi, A.K.; Mittal, H. Technological revolutions in smart farming: Current trends, challenges & future directions. *Comput. Electron. Agric.* **2022**, *13*, 107217.
32. Savickas, D.; Steponavičius, D.; Domeika, R. Analysis of Telematics Data of Combine Harvesters and Evaluation of Potential to Reduce Environmental Pollution. *Atmosphere* **2021**, *12*, 674. [\[CrossRef\]](#)
33. Jaafar, H.H.; Woertz, E. Agriculture as a funding source of ISIS: A GIS and remote sensing analysis. *Food Policy* **2016**, *64*, 14–25. [\[CrossRef\]](#)
34. Yalwe, S.G.; van Griensven, A.; Mul, M.L.; van der Zaag, P. Land suitability analysis for agriculture in the Abbay basin using remote sensing, GIS and AHP techniques. *Model. Earth Syst. Environ.* **2016**, *2*, 101. [\[CrossRef\]](#)
35. Ramu, P.; Santosh, B.S.; Chalapathi, K. Crop-land suitability analysis using geographic information system and remote sensing. *Prog. Agric. Eng. Sci.* **2022**, *36*, 77–94. [\[CrossRef\]](#)
36. Leelavathi, G.; Shaila, K.; Venugopal, K.R. Hardware performance analysis of RSA cryptosystems on FPGA for wireless sensor nodes. *Int. J. Intell. Netw.* **2021**, *2*, 184–194. [\[CrossRef\]](#)
37. Chugh, B.; Thakur, S.; Singh, A.K.; Joany, R.M.; Rajendran, S.; Nguyen, T.A. Electrochemical sensors for agricultural application. *Nanosensors for Smart Agriculture*; Elsevier: Amsterdam, The Netherlands, 2022; pp. 147–164.
38. Qureshi, T.; Saeed, M.; Ahsan, K.; Malik, A.A.; Muhammad, E.S.; Touheed, N. Smart Agriculture for Sustainable Food Security Using Internet of Things (IoT). *Wirel. Commun. Mob. Comput.* **2022**, *2022*, 9608394. [\[CrossRef\]](#)

39. del-Moral-Martínez, I.; Rosell-Polo, J.R.; Company, J.; Sanz, R.; Escolà, A.; Masip, J.; Martínez-Casasnovas, J.A.; Arnó, J. Mapping vineyard leaf area using mobile terrestrial laser scanners: Should rows be scanned on-the-go or discontinuously sampled? *Sensors* **2016**, *16*, 119. [CrossRef]
40. Basri, M.A.M.; Adnan, M.A. Autonomous Agriculture Robot for Monitoring Plant using Internet of Things. *ELEKTRIKA-J. Electr. Eng.* **2022**, *21*, 14–19. [CrossRef]
41. Khan, N.; Ray, R.L.; Sargani, G.R.; Ihtisham, M.; Khayyam, M.; Ismail, S. Current progress and future prospects of agriculture technology: Gateway to sustainable agriculture. *Sustainability* **2021**, *13*, 4883. [CrossRef]
42. Javaid, M.; Haleem, A.; Singh, R.P.; Suman, R. Enhancing smart farming through the applications of Agriculture 4.0 technologies. *Int. J. Intell. Netw.* **2022**, *3*, 150–164. [CrossRef]
43. Al-Dweik, A.; Muresan, R.; Mayhew, M.; Lieberman, M. IoT-based multifunctional scalable real-time enhanced roadside unit for intelligent transportation systems. In *Proceedings of the 2017 IEEE 30th Canadian Conference on Electrical and Computer Engineering (CCECE)*, Windsor, ON, Canada, 30 April–3 May 2017; pp. 1–6.
44. Messaoud, S.; Ahmed, O.B.; Bradai, A.; Atri, M. Machine learning modeling-powered IoT systems for smart applications. In *IoT-Based Intelligent Modelling for Environmental and Ecological Engineering*; Springer: Berlin/Heidelberg, Germany, 2021; pp. 185–212.
45. Jain, B.; Brar, G.; Malhotra, J.; Rani, S.; Ahmed, S.H. A cross-layer protocol for traffic management in Social Internet of Vehicles. *Future Gener. Comput. Syst.* **2018**, *82*, 707–714. [CrossRef]
46. Wang, Z.; Wei, H.; Wang, J.; Zeng, X.; Chang, Y. Security Issues and Solutions for Connected and Autonomous Vehicles in a Sustainable City: A Survey. *Sustainability* **2022**, *14*, 12409. [CrossRef]
47. Ozbayoglu, M.; Kucukayan, G.; Dogdu, E. A real-time autonomous highway accident detection model based on big data processing and computational intelligence. In *Proceedings of the 2016 IEEE International Conference on Big Data (Big Data)*, Washington, DC, USA, 5–8 December 2016; pp. 1807–1813.
48. Kwon, D.; Park, S.; Baek, S.; Malaiyappan, R.K.; Yoon, G.; Ryu, J.-T. A study on the development of the blind spot detection system for the IoT-based smart connected car. In *Proceedings of the 2018 IEEE International Conference on Consumer Electronics (ICCE)*, Las Vegas, NV, USA, 12–14 January 2018; pp. 1–4.
49. Devi, S.; Neetha, T. Machine Learning based traffic congestion prediction in an IoT based Smart City. *Int. Res. J. Eng. Technol.* **2017**, *4*, 3442–3445.
50. Ghosh, A.; Chatterjee, T.; Samanta, S.; Aich, J.; Roy, S. Distracted driving: A novel approach towards accident prevention. *Adv. Comput. Sci. Technol.* **2017**, *10*, 2693–2705.
51. Ryder, B.; Wortmann, F. Autonomously detecting and classifying traffic accident hotspots. In *Proceedings of the 2017 ACM International Joint Conference on Pervasive and Ubiquitous Computing and Proceedings of the 2017 ACM International Symposium on Wearable Computers*, Maui, HI, USA, 11–15 September 2017; pp. 365–370.
52. Munoz-Organero, M.; Ruiz-Blaquez, R.; Sánchez-Fernández, L. Automatic detection of traffic lights, street crossings and urban roundabouts combining outlier detection and deep learning classification techniques based on GPS traces while driving. *Comput. Environ. Urban Syst.* **2018**, *68*, 1–8. [CrossRef]
53. Amato, G.; Carrara, F.; Falchi, F.; Gennaro, C.; Meghini, C.; Vairo, C. Deep learning for decentralized parking lot occupancy detection. *Expert Syst. Appl.* **2017**, *72*, 327–334. [CrossRef]
54. You, Z.; Yang, K.; Luo, W.; Lu, X.; Cui, L.; Le, X. Iterative Correlation-based Feature Refinement for Few-shot Counting. *arXiv* **2022**, arXiv:2201.08959.
55. Zantalis, F.; Koulouras, G.; Karabetsos, S.; Kandris, D. A review of machine learning and IoT in smart transportation. *Future Internet* **2019**, *11*, 94. [CrossRef]
56. Gupta, A.; Kulkarni, S.; Jathar, V.; Sharma, V.; Jain, N. Smart car parking management system using IoT. *Am. J. Sci. Eng. Technol.* **2017**, *2*, 112–119.
57. Rizvi, S.R.; Zehra, S.; Olariu, S. Aspire An agent-oriented smart parking recommendation system for smart cities. *IEEE Intell. Transp. Syst. Mag.* **2018**, *11*, 48–61. [CrossRef]
58. Araújo, A.; Kalebe, R.; Giraõ, G.; Gonçalves, K.; Neto, B. Reliability analysis of an IoT-based smart parking application for smart cities. In *Proceedings of the 2017 IEEE International Conference on Big Data (Big Data)*, Boston, MA, USA, 11–14 December 2017; pp. 4086–4091.
59. Egaji, O.A.; Evans, G.; Griffiths, M.G.; Islas, G. Real-time machine learning-based approach for pothole detection. *Expert Syst. Appl.* **2021**, *184*, 115. [CrossRef]
60. Gopalakrishnan, K. Deep learning in data-driven pavement image analysis and automated distress detection: A review. *Data* **2018**, *3*, 28. [CrossRef]
61. Kokilavani, M.; Malathi, A. Smart street lighting system using IoT. *Int. J. Adv. Res. Appl. Sci. Technol.* **2017**, *3*, 8–11.
62. Tripathy, A.K.; Mishra, A.K.; Das, T.K. Smart lighting: Intelligent and weather adaptive lighting in street lights using IoT. In *Proceedings of the 2017 International Conference on Intelligent Computing, Instrumentation and Control Technologies (ICICT)*, Kerala, India, 6–7 July 2017; pp. 1236–1239.
63. Chowdhury, D.N.; Agarwal, N.; Laha, A.B.; Mukherjee, A. A vehicle-to-vehicle communication system using IoT approach. In *Proceedings of the 2018 Second International Conference on Electronics, Communication and Aerospace Technology (ICECA)*, Coimbatore, India, 29–31 March 2018; pp. 915–919.

64. Naveed, Q.N.; Alqahtani, H.; Khan, R.U.; Almakdi, S.; Alshehri, M.; Abdul Rasheed, M.A.; Jain, B.; Brar, G. An intelligent traffic surveillance system using integrated wireless sensor network and improved phase timing optimization. *Sensors* **2022**, *22*, 3333. [[CrossRef](#)]
65. Fan, X.; Liu, J.; Wang, Z.; Jiang, Y.; Liu, X. Crowdsourced road navigation: Concept, design, and implementation. *IEEE Commun. Mag.* **2017**, *55*, 126–128. [[CrossRef](#)]
66. Zhang, X.; Wang, Y. Research on intelligent medical big data system based on Hadoop and blockchain. *EURASIP J. Wirel. Commun. Netw.* **2021**, *2021*, 7. [[CrossRef](#)]
67. Merck, S.F. Chronic disease and mobile technology: An innovative tool for clinicians. *Nurs. Forum* **2017**, *52*, 298–305. [[CrossRef](#)] [[PubMed](#)]
68. Sharp, L.K.; Biggers, A.; Perez, R.; Henkinsi, J.; Tilton, J.; Gerber, B.S. A Pharmacist and Health Coach–Delivered Mobile Health Intervention for Type 2 Diabetes: Protocol for a Randomized Controlled Crossover Study. *JMIR Res. Protoc.* **2021**, *10*, 171. [[CrossRef](#)] [[PubMed](#)]
69. Vijayalakshmi, A.; Jose, D.V.; Unnisa, S. Wearable Sensors for Pervasive and Personalized Health Care. In *IoT in Healthcare and Ambient Assisted Living*; Springer: Berlin/Heidelberg, Germany, 2021; pp. 123–143.
70. Zhang, D.; Liu, Q. Biosensors and bioelectronics on smartphone for portable biochemical detection. *Biosens. Bioelectron.* **2016**, *75*, 273–284. [[CrossRef](#)] [[PubMed](#)]
71. Akmandor, A.O.; Jha, N.K. Keep the stress away with SoDA: Stress detection and alleviation system. *IEEE Trans. Multi-Scale Comput. Syst.* **2017**, *3*, 269–282. [[CrossRef](#)]
72. Haque, N.; Rahman, M.A.; Shahriar, M.H.; Khalil, A.A.; Uluagac, S. A novel framework for threat analysis of machine learning-based smart healthcare systems. *arXiv* **2021**, arXiv:2103.03472.
73. Esteva, A.; Kuprel, B.; Novoa, R.A.; Ko, J.; Swetter, S.M.; Blau, H.M.; Thrun, S. Dermatologist-level classification of skin cancer with deep neural networks. *Nature* **2017**, *542*, 115–118. [[CrossRef](#)]
74. Kumar, S.; Lim, W.M.; Sivarajah, U.; Kaur, J. Artificial intelligence and blockchain integration in business: Trends from a bibliometric-content analysis. *Inf. Syst. Front.* **2022**, 1–26. [[CrossRef](#)]
75. Yamin, M.M.; Ullah, M.; Ullah, H.; Katt, B. Weaponized AI for cyber attacks. *J. Inf. Secur. Appl.* **2021**, *57*, 102722. [[CrossRef](#)]
76. Peters, B.S.; Armijo, P.R.; Krause, C.; Choudhury, S.A.; Oleynikov, D. Review of emerging surgical robotic technology. *Surg. Endosc.* **2018**, *32*, 1636–1655. [[CrossRef](#)]
77. Sood, S.K.; Rawat, K.S.; Kumar, D. A visual review of artificial intelligence and Industry 4.0 in healthcare. *Comput. Electr. Eng.* **2022**, *101*, 107948. [[CrossRef](#)]
78. Winkler, E.C.; Wiemann, S. Findings made in gene panel to whole genome sequencing: Data, knowledge, ethics—and consequences? *Expert Rev. Mol. Diagn.* **2016**, *16*, 1259–1270. [[CrossRef](#)] [[PubMed](#)]
79. Wang, X.; Liu, Z.; Fan, F.; Hou, Y.; Yang, H.; Meng, X.; Zhang, Y.; Ren, F. Microfluidic chip and its application in autophagy detection. *TrAC Trends Anal. Chem.* **2019**, *117*, 300–315. [[CrossRef](#)]
80. Zhang, J.Z.; Li, Y.K.; Cao, L.Y.; Zhang, Y. Research on the construction of smart hospitals at 424 homes and abroad. *Chin. Hos. Manag.* **2018**, *38*, 64–66.
81. Wang, K.; Zhao, Y.; Gangadhari, R.K.; Li, Z. Analyzing the adoption challenges of the Internet of things (IoT) and artificial intelligence (AI) for smart cities in China. *Sustainability* **2021**, *13*, 10983. [[CrossRef](#)]
82. White, R.W. Skill discovery in virtual assistants. *Commun. ACM* **2018**, *61*, 106–113. [[CrossRef](#)]
83. Ortiz, C.L. Holistic conversational assistants. *AI Mag.* **2018**, *39*, 88–90. [[CrossRef](#)]
84. Raghuvanshi, A.; Singh, U.K.; Joshi, C. A review of various security and privacy innovations for IoT applications in healthcare. In *Advanced Healthcare Systems: Empowering Physicians with IoT-Enabled Technologies*; Wiley: Hoboken, NJ, USA, 2022; pp. 43–58.
85. Redfern, J. Smart health and innovation: Facilitating health-related behavior change. *Proc. Nutr. Soc.* **2017**, *76*, 328–332. [[CrossRef](#)]
86. Zeevi, D.; Korem, T.; Zmora, N.; Israeli, D.; Rothschild, D.; Weinberger, A.; Ben-Yacov, O.; Lador, D.; Avnit-Sagi, T.; Lotan-Pompan, M.; et al. Personalized nutrition by prediction of glycemic responses. *Cell* **2015**, *163*, 1079–1094. [[CrossRef](#)]
87. Kumar, A.; Jain, A.K. RFID Security issues, defenses, and security schemes. In *Handbook of Research on Machine Learning Techniques for Pattern Recognition and Information Security*; IGI Global: Hershey, PA, USA, 2021; pp. 293–310.
88. Tu, Y.-J.; Kapoor, G.; Piramuthu, S. On Group Ownership Delegate Protocol for RFID Systems. *Inf. Syst. Front.* **2021**, 1–8. [[CrossRef](#)]
89. Parkinson, S.; Khan, S. A Survey on Empirical Security Analysis of Access Control Systems: A Real-World Perspective. *ACM Comput. Surv. (CSUR)* **2022**, *98*, 109–111. [[CrossRef](#)]
90. Misra, S.; Roy, C.; Mukherjee, A. *Introduction to Industrial Internet of Things and Industry 4.0*; CRC Press: Boca Raton, FL, USA, 2021; pp. 86–89.
91. Thilakarathne, N.N.; Kagita, M.K.; Priyashan, W.D. Green internet of things: The next generation energy efficient internet of things. In *Applied Information Processing Systems*; Springer: Berlin/Heidelberg, Germany, 2022; pp. 391–402.
92. Bhattacharjee, S.; Salimitari, M.; Chatterjee, M.; Kwiat, K.; Kamhoua, C. Preserving data integrity in IoT networks under opportunistic data manipulation. In Proceedings of the 2017 IEEE 15th Intl Conf on Dependable, Autonomous and Secure Computing, 15th Intl Conf on Pervasive Intelligence and Computing, 3rd Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress (DASC/PiCom/DataCom/CyberSciTech), Orlando, FL, USA, 6–10 November 2017; pp. 446–453.

93. Zhang, G.; Kou, L.; Zhang, L.; Liu, C.; Da, Q.; Sun, J. A new digital watermarking method for data integrity protection in the perception layer of IoT. *Secur. Commun. Netw.* **2017**, *2017*, 3126010. [[CrossRef](#)]
94. Meng, Y.; Li, J. Data sharing mechanism of sensors and actuators of industrial IoT based on blockchain-assisted identity-based cryptography. *Sensors* **2021**, *21*, 6084. [[CrossRef](#)] [[PubMed](#)]
95. Bender, T.; Huesmann, R.; Heinemann, A. Software Development Processes for ADs, SMCs and OSCs supporting Usability, Security, and Privacy Goals—an Overview. In *Proceedings of the 16th International Conference on Availability, Reliability and Security*, Vienna, Austria, 17–20 August 2021; pp. 1–6.
96. Zhu, Q.; Uddin, M.Y.S.; Venkatasubramanian, N.; Hsu, C.; Hong, H. Enhancing reliability of community internet-of-things deployments with mobility. In *Proceedings of the IEEE INFOCOM 2018-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, Honolulu, HI, USA, 15–19 April 2018; pp. 1–2.
97. Pokorni, S. Reliability prediction of electronic equipment: Problems and experience. In *Proceedings of the 7th International Scientific Conference on Defensive Technologies OTEH*, Belgrade, Serbia, 6–7 October 2016; pp. 695–700.
98. Thomas, M.O.; Rad, B.B. Reliability evaluation metrics for internet of things, car tracking system: A review. *Int. J. Inf. Technol. Comput. Sci. (IJITCS)* **2017**, *9*, 1–10. [[CrossRef](#)]
99. Al-Fuqaha, A.; Guizani, M.; Mohammadi, M.; Aledhari, M.; Ayyash, M. Internet of things: A survey on enabling technologies, protocols, and applications. *IEEE Commun. Surv. Tutor.* **2015**, *17*, 2347–2376. [[CrossRef](#)]
100. Lu, Y.; Xu, L.D. Internet of Things (IoT) cybersecurity research: A review of current research topics. *IEEE Internet Things J.* **2018**, *6*, 2103–2115. [[CrossRef](#)]
101. El-Hajj, M.; Fadlallah, A.; Chamoun, M.; Serhrouchni, A. A survey of internet of things (IoT) authentication schemes. *Sensors* **2019**, *19*, 1141. [[CrossRef](#)]
102. Deep, S.; Zheng, X.; Jolfaei, A.; Yu, D.; Ostovari, P.; Bashir, A.K. A survey of security and privacy issues in the Internet of Things from the layered context. *Trans. Emerg. Telecommun. Technol.* **2022**, *33*, 3935. [[CrossRef](#)]
103. 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, 10–20 October 2017; pp. 1–3.
104. Chae, C.-J.; Choi, K.; Choi, K.; Yae, Y.; 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**, *1*, 21–28. [[CrossRef](#)]
105. Xu, Y.; Ren, J.; Wang, G.; Zhang, C.; Yang, J.; Zhang, Y. A blockchain-based nonrepudiation network computing service scheme for industrial IoT. *IEEE Trans. Ind. Inform.* **2019**, *6*, 3632–3641. [[CrossRef](#)]
106. Adil, M.; Khan, M.K. Emerging IoT applications in sustainable smart cities for covid-19: Network security and data preservation challenges with future directions. *Sustain. Cities Soc.* **2021**, *75*, 103311. [[CrossRef](#)]
107. Asokan, N.; Schunter, M.; Waidner, M. Optimistic protocols for fair exchange. In *Proceedings of the 4th ACM Conference on Computer and Communications Security*, Zurich, Switzerland, 1–4 April 1997; pp. 7–17.
108. Markowitch, O.; Roggeman, Y. Probabilistic non-repudiation without trusted third party. In *Proceedings of the Second Conference on Security in Communication Networks*, Sydney, Australia, 9–11 November 1999; Volume 99, pp. 25–36.
109. Chen, C.-L.; Deng, Y.; Weng, W.; Zhou, M.; Sun, H. A blockchain-based intelligent anti-switch package in tracing logistics system. *J. Supercomput.* **2021**, *77*, 7791–7832. [[CrossRef](#)]
110. Singh, A.; Anand, A. Data leakage detection using cloud computing. *Int. J. Eng. Comput. Sci.* **2017**, *6*, 234. [[CrossRef](#)]
111. Liu, J.; Ren, A.; Zhang, L.; Sun, R.; Du, X.; Guizani, M. A novel secure authentication scheme for heterogeneous internet of things. In *Proceedings of the ICC 2019–2019 IEEE International Conference on Communications (ICC)*, Shanghai, China, 20–24 May 2019; pp. 1–6.
112. Salman, A.; Diehl, W.; Kap, J. A lightweight hardware/software co-design for pairing-based cryptography with low power and energy consumption. In *Proceedings of the 2017 International Conference on Field Programmable Technology (ICFPT)*, Melbourne, Australia, 11–13 December 2017; pp. 235–238.
113. Karati, A.; Fan, C.; Zhuang, E. Reliable data sharing by certificates encryption supporting keyword search against vulnerable KGC in the industrial internet of things. *IEEE Trans. Ind. Inform.* **2021**, *17*, 3661–3669. [[CrossRef](#)]
114. Chakrabarty, S.; Engels, D.W. A secure IoT architecture for smart cities. In *Proceedings of the 2016 13th IEEE Annual Consumer Communications & Networking Conference (CCNC)*, Las Vegas, NV, USA, 9–12 January 2016; pp. 812–813.
115. Shivraj, V.L.; Rajan, M.A.; Singh, M.; Balamuralidhar, P. One-time password authentication scheme based on elliptic curves for Internet of Things (IoT). In *Proceedings of the 2015 5th National Symposium on Information Technology: Towards New Smart World (NSITNSW)*, Riyadh, Saudi Arabia, 17–19 February 2015; pp. 1–6.
116. Nguyen, D.C.; Ding, M.; Pathirana, P.N.; Seneviratne, A.; Li, J.; Niyato, D.; Dobre, O.; Poor, H.V. 6G Internet of Things: A comprehensive survey. *IEEE Internet Things J.* **2021**, *1*, 234. [[CrossRef](#)]
117. Choi, W.; Kim, J.; Lee, S.; Park, E. Smart home and internet of things: A bibliometric study. *J. Clean. Prod.* **2021**, *301*, 126908. [[CrossRef](#)]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.

Architectural Threats to Security and Privacy: A Challenge for Internet of Things (IoT) Applications

ORIGINALITY REPORT

3%

SIMILARITY INDEX

3%

INTERNET SOURCES

0%

PUBLICATIONS

0%

STUDENT PAPERS

MATCH ALL SOURCES (ONLY SELECTED SOURCE PRINTED)

3%

★ pseccommunity.org

Internet Source

Exclude quotes Off

Exclude bibliography Off

Exclude matches < 3%