The Seybold Report

ISSN 1533-9211

DOI 10.17605/OSF.IO/YSZDC

AN IoT-BASED RECENT SURVEY ON CYBER SECURITY

R. KARTHIGAICHELVI

Research Scholar, Centre for Information Technology & Engineering, Manonmaniam Sundaranar University, Abishekapatti, Tirunelveli, Tamilnadu, India. Assistant Professor, Hajee Karutha Rowther Howdia College Uthamapalayam. Email: karthigaichelviramar2014@gmail.com

Dr. B. BALAKUMAR

Assistant Professor, Centre for Information Technology & Engineering, Manonmaniam Sundaranar University, Abishekapatti, Tirunelveli, Tamilnadu, India.

Abstract

The global network made up of people, intelligent things, smart gadgets, and information and data have been completely transformed by the Internet of Things (IoT), a young technology. There are still numerous challenges that need to be resolved while IoT development is still in its early stages. Everything is to be embedded as part of the Internet of Things. Accessibility, integrity, availability, scalability, confidentiality, and interoperability are all areas where the Internet of Things has a big possibility to improve the world. The challenge is figuring out how to defend IoT. The development of IoT is built on system security. An in-depth analysis of IoT cyber security is presented in this article. The integration of diverse smart devices and Information Communication Technologies (ICT), as well as their protection, make up the paradigm's core components. We cover topics relevant to those who are interested in IoT cyber security, such as current research in the field, IoT cyber security architecture and taxonomy, important enabling countermeasures and strategies, major applications in sectors, research trends and problems, and more.

Keywords: Wireless Sensor Networks (WSNs), IoT, Cyber security, Business Systems, Informatics in Industry, Ingenious Device, RFIDs

1. INTRODUCTION

The Internet of Things (IoT) has significantly altered end users' daily lives as an emergent technology—indeed, as a revolution. Individuals use surroundings with intelligence (home and city), Systems for transportation and eHealth to benefit from their living, learning, and working activities within the IoT network. Innovations for organisations or institutions, such as improved industrial and automation manufacturing, Management of data and information interchange, and intelligent and self-altering processes and systems, are gaining popularity [1]. IoT may work in any way, at any time, and everywhere with things, networks, RFID, and WSNs attributable to telecommunications systems' rapid expansion. The unavoidable problem with IoT development is cyber security, which must be addressed. If the problem is not properly handled, hackers will take advantage of the flaws and vulnerabilities in devices and objects, alter data, or interfere with systems through the global IoT network. Attacks and IoT failures can outweigh any advantages. Additionally, due to scalability, integrity, and interoperability of contemporary devices are at unsatisfactory levels, the use of conventional security mechanisms and techniques is inappropriate. Therefore, to meet the IoT's requirements for dependability, security, and privacy, new strategies and technologies must be developed. [2]–[6]. Particularly diverse devices are just one aspect of the Internet of Things. IoT had 4.9 billion linked items

The Seybold Report
ISSN 1533-9211
DOI 10.17605/OSF.IO/YSZDC

by 2015 and by 2020; there will be 25 billion connected things [1]. Despite the great flexibility and scalability of IoT, the likelihood of a security catastrophe is increased by this massive quantity. The risk to an individual, the network, and the cyber security of the global infrastructure increases when a person connects more devices. In 2003, there were just 0.08 or less devices per person. The number went up to 1.84 in 2010. There will be 6.58 devices per person by the year 2020 [1]. The worldwide Internet of Things is experiencing rapid and widespread device development; however these devices are also regarded to be weak points in the IoT network since they are susceptible to attack. As a result, IoT cyber security architecture makes sure that users may use devices responsibly and those they are maintained in a secure environment. The IoT smart devices have many different parts, including a CPU, mobile phone, communication interfaces, OS, weightless services, and preloaded programmes, to name just a few. Intelligent devices that are outfitted with RFID sensors or actuators are capable of acting appropriately, making decisions on their own, and safely distributing information to users [7, 8]. IoT cyber security has become more prevalent as a result of the development of smart devices, wireless communication, IP protocol, sensor network technologies, and internet and wireless communication. These cutting-edge technologies are also having a significant impact on Industry 4.0 and new ICT [7]. Cyber security applies to the IoT network, a global infrastructure of diverse intelligent devices that combines technology for sensing, communicating, networking, and processing information [1]. In addition, a wide range of other IoT technologies and gadgets, including barcodes, smartphones, social networks, and cloud computing, have a slight impact on cyber security. Countries and institutions frequently point to the cyber security of IoT when implementing standards and rules to reach a high level of cyber security. The US, China, and the UK are the three nations most vulnerable to cyber security vulnerabilities associated with the Internet of Things, primarily from attacks on smart homes [9]. To control and improve the cyber security of intelligent devices as well as the infrastructure as a whole, the US has implemented the Cyber security for the IoT project. [10]. China's Cyber security Law (CSL) becomes effective on June 1st, 2017. The Cyberspace Administration of China is the main government agency in charge of overseeing and implementing the CSL (CAC). The CSL handles monitoring, early warning, and emergency response operations on Chinese soil and manages many aspects of cyber security, such as network operation security and network information security [11]. Europe has advanced in a number of fields, including energy, transportation, and domestic cyber security [12].

2. SYSTEM FOR MANAGING CYBER SECURITY BASED ON IoT

IoT combines diverse smart gadgets into a secure network. IoT cyber security is a method for strategically enhancing IoT and includes all of the adjustments made to this technology to guarantee the security of the overall environment.

2.1 IoT Architecture Focused on Cyber security

The most common IoT cyber security architectures are listed in Table I from various angles. The table makes it abundantly evident that there are three main categories into which experts divide IoT cyber security frameworks: the fundamental three-layer architecture, the deduced

The Seybold Report
ISSN 1533-9211
DOI 10.17605/OSF.IO/YSZDC

complex five-layer structure, and a four-layer structure. The layers are the interface layer, the application (service) layer, the middleware layer, the network layer, and the accessing layer. The layer at the top is the perception (sensing) layer.

Table 1: A recap of various IoT architectures

Quantity of Layers	Important Technologies
3	Application, Network, Sensing [2]
	Application, Perception, Network [14]
	Transportation, Application, Perception [15]
	Network, Application, Perception [16]
	Service, Network, Perception [17]
	Application, Perception, Network [18] [23]
4	Interface, Service, Networking, Sensing [1]
	Application, Support, Network, Perception [7]
5	Application, Middleware, Internet, Access Gateway, Field Data Acquisition [3]
	Business, Application, Network, Middleware, Perception [19]

According to [2], the three fundamental levels of an IoT architecture are the application layer, the network layer, and the sensor layer. The framework is separated into four layers: the network layer, the sensing layer, the interface layer, and the service layer when taking into account services, according to [1] a division based on the SOA (Service-Oriented Architecture). Also included is a description of using IoT architecture various studies. As an illustration, most studies [14] have the same findings three-layered building as Atzori. Throughout the four-layered structure, as opposed architecture of Xu, the support layer, which is specifically for cloud computing, is built into the third tier [7]. Based on Atzori's architecture, [15] developed the middleware and business layers for the five-layered architecture. [3] Presented a generic, a five-layered Internet of Things architecture accommodates different industries. The Internet layer provides the top two levels of communication media (the application layer and the middleware layer) are in charge of data usage, and data gathering is processed by the access gateway and field data collecting layers, which are the two lowest layers. the principles and functionalities of heterogeneous and ubiquitous devices, wireless networking, and communication, authentic, weightless technologies, etc. are all aspects of the architectural design of IoT-based cyber security. In terms of technology, the architecture's design demands interoperability across diverse smart devices, accessibility, integrity, availability, scalability, and confidentiality [16]. Memory, tamper-proof packaging, embedded software, processing and energy, embedded architecture design, and dynamic architecture design should all be used together patching in light of the hardware/software limits. To support IoT devices that dynamically interact with other things, an adaptable architecture is required because cyber security may change or may require real-time intervention within the relevant ecosystem. IoT networks and services are susceptible to malicious assaults at every layer, which can impair or completely wipe them out. In our study, a four-layered IoT architecture is built from the standpoint of cyber security (Table II).

The Seybold Report
ISSN 1533-9211
DOI 10.17605/OSF.IO/YSZDC

Table 2: An IoT-oriented, four-layer cyber security-oriented architecture

Layers	Description	Attack Methods
Sensing Layer	Object and data sensing. Attack target: discretion.	Attacks using replays, timing, node capture, malicious data, and side channel attacks.
Network Layer	Transfer of data and networking. Attack focusing on compatibility, secrecy, and privacy.	Route information that has been tampered with, changed, or replayed Sybil, Wormholes.
Middleware Layer	Transfer of data. Attacking with a focus on truthfulness, loyalty, and discretion.	he underlying infrastructure, third-party connections, malicious insider, threat from virtualization
Application Layer	Provided the requested service. Attacks with a focus on identity verification and data privacy.	Malicious Scripts, Trojan Horse and Spyware, Worms, Viruses, and Unauthorized Access.

2.2 Cyber security and the Four Layers

The Internet of Things (IoT) is a global network that enables the connection and control of physical items using smart devices like Radio-Frequency Identification (RFID) tags and readers [17], sensors, actuators, smartphones, and other gadgets. IoT-related objects are vulnerable to DoS attacks at every layer because of their constrained storage, power, and computing capabilities. An attempt to prevent end users from using IoT resources (such as a machine or network resources) is known as a denial of service (DoS) attack. Potential channels for DoS attacks include expired configuration information, interference channels, memory, disc space, bandwidth, and other resources [4], [18]. There are two different forms of DoS attacks: Distributed Denial of Service (DDoS) and Standard DoS [19].

1) The Sensing Layer

Data sensors and networks make up the sensing layer, which is capable of detecting, gathering, processing, and transmitting access to the entire network, information, or data [1]. At this tier, there are three significant difficulties with cyber security: Wireless signal strength, sensor node exposure in IoT devices, dynamic IoT design, and communication, computation, storage, and memory restrictions are just a few of the elements that need to be considered [20]. To secure the Internet of Things network, this layer uses three well-liked security techniques: node authentication, access control, and lightweight encryption. The secrecy of the perception layer is the target of numerous attacks and crimes in reality, including attacks such as replay, timing, node capture, malicious data, and others. Replaying, spoofing, or modifying the IoT network's smart device identifiers constitutes a replay attack. An adversary who uses a time attack steals the encryption key linked to time and other important details [21]. An assault known as a node capture occurs when control of nodes steals valuable data and information. Additionally, by introducing a new node to the network, the attacker can send a layer harmful data. [20]. An attempt to compromise the encryption device's side channel information through device operation (such as time, power, electromagnetic radiation, etc.) is referred to as a Side Channel Attack (SCA) [14]. Hanney, for instance, needs Jerry to verify her identification before she can use a web account. Hanney gives Jerry her password when he asks for identification. Jack is

The Seybold Report
ISSN 1533-9211
DOI 10.17605/OSF.IO/YSZDC

listening in on the chat at the same time and records the password. Later, as evidence of access to Hanney's online profile, Jack presents Jerry with the password.

2) The Network Layer

Data routing and transmission to different IoT hubs and devices are handled by the network layer across both mobile networks and the Internet [2]. During this layer, devices such as WiFi, to run cloud computing platforms, switching, and routing hardware, LTE, Bluetooth, 3G/4G, Zigbee, and Internet gateways are used. Network gateways serve as a connection point between multiple IoT nodes by collecting, filtering, and transmitting data to and from various sensors. The primary cyber security concerns at this layer are compatibility, confidentiality, and privacy. The interactive function in the IoT global network could be machine-to-machine, human-to-human, human-to-machine, or machine-to-machine. Wired or wireless procedures are used to manage connections among various smart devices. Since everything is connected to the IoT network, attackers have a good probability of finding illicit activities. Specifically, the network layer can be seriously endangered by a type of attack known as a Man-in-the-Middle attack. Modern protocols, software, and hardware can detect anomalous behavior or conditions to make IoT secure [21], [22].

The mutual direct assaults of spoofing, modification, and replay aim at data interchange, produce phony and incorrect messages, and produce routing loops between nodes. A single node that can be present simultaneously in various places and under multiple identities is a Sybil assault. Sybil attacks compromise the integrity and resource use of the Internet of Things by disseminating malware and stealing information. Sybil attacks can happen on social media sites like Facebook and Twitter [23].

An attacker, for instance, could spread malware throughout the network by disseminating bogus information on routes. Before permitting a person to access the phony Twitter log in page, a survey is requested on Twitter. The phony page can capture the consumer login information, show the log in issue, and send the user to a legitimate page on Facebook. Information about the client may be taken during this process.

3) The Middleware Layer

The foundation of Middleware is the layer that Service Oriented Architecture (SOA) concept [2]. Between network and application levels, it is a software layer. The operation and management of the authenticity, integrity, and secrecy of all transferred data are required at this level. Intelligent middleware can use the pervasiveness of sensor networks and other recognized things to create dynamic processes for the physical world in the digital/virtual world, high spatial-temporal resolution, and the Internet of Things architecture [26].

Internal attackers who purposefully alter and extract data or information from the network are said to be conducting a malicious inside attack [27]. PaaS-based (Platform as a Service) attacks are known as underlying attacks. IoT application securities as well as the lower tiers' levels of security are the developers' key concerns [28]. Mashups and other third-party components boost the safety of networks and data on PaaS by preventing third-party relationship attacks

ISSN 1533-9211

DOI 10.17605/OSF.IO/YSZDC

[24]. A virtual machine may be harmed during a virtualization attack, which could also impact other virtual machines. Attacks can take many different forms [25].

Assume, for instance, that an insider gains unauthorized access to a system or network and looks into its design to find weak spots. A workstation could then be run to lose or leak information or data.

4) The Application Layer

For the benefit of the users, the application layer researches all system capabilities by defined protocols and service technologies [1].

Unwanted data is transmitted and traded among application-layer smart devices. For both professionals and academics, the protection of data security and privacy as well as the identification of objects using non-standard authentication procedures provide significant issues [16]. Data access restrictions, identity verification, data protection and recovery, handling of large amounts of data, and software vulnerabilities are common security issues in this layer [14].

A phishing assault is carried out by an attacker who steals and authentication authorization, such as login credentials or credit card details, to get relevant information or data from the user [31]. The attacker utilizes worms, Trojan horses, malware, and other malicious software to introduce malware into the system to prevent service, modify data, and/or access confidential data [32]. The system shuts down whenever a user watches the entryway and executes the script for Active-X. Access can be restricted, and data can be taken [26]. In an unapproved access attack, an assailant might simply harm the system by preventing users from using relevant IoT services or by erasing data that has already been stored.

2.3 Taxonomy of Attacks

The attacks seem malicious because of the diversity of intelligent devices, communication standards, software, and services. We divide various attacks into eight categories [13]. Figure 1 provides information.

ISSN 1533-9211

DOI 10.17605/OSF.IO/YSZDC

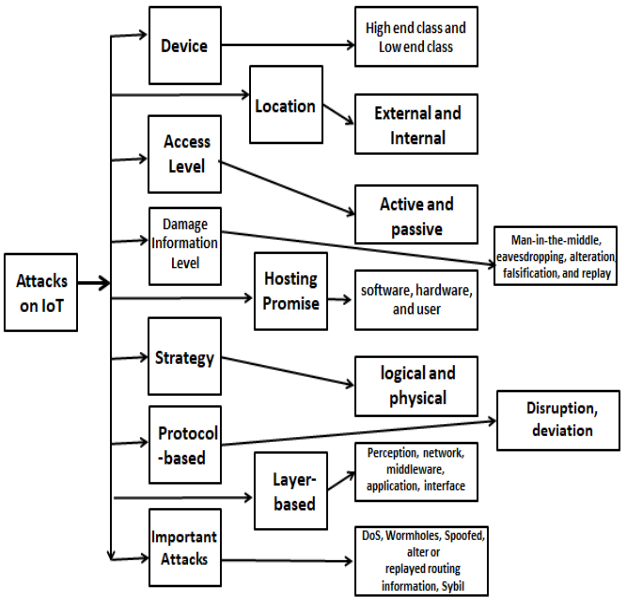

Figure 1: Cyber security classification IoT-related attack

Low-cost and high-end technology assaults fall under device-based attacks. There are attacks from both inside and outside that are due to location. Attacks, both direct and indirect, based on access level are also possible [27–29]. Interruption, eavesdropping, alteration, fabrication, replay, and man-in-the-middle attacks are examples of assaults based on information damage. Users, hardware, and software attacks are all types of host-based attacks. Physical and intellectual attacks are both types of attacks based on strategy. Disruption attacks based on the protocol are deviation attacks. Layer-based attacks include those that target perception, networks, middleware, and applications.

Low-power devices are used in low-end device assaults to conduct assaults on the IoT framework, whereas high-power/full-featured devices are used in high-end device assaults. [30]. External threats ("Outsider") and internal threats ("Insider") originate within the IoT network, whereas external threats ("Outsider") originate within the IoT network [31]. An insider attack entails the attacker attempting to use IoT network smart devices to run his malicious code. Internal attacks can be classified into four categories: emotionally motivated attackers, inadvertent attackers, affected roles, and technological expertise roles. An aggressor tries to remotely outside access to IoT smart gadgets of the network at random and with the user's ignorance.

Passive attacks entail monitoring and listening to recover information in the IoT network without interfering with data and communication [26], [32]. Attacks that are active rather than passive have a direct the IoT's effect network mechanism for communication. Active attacks can disable smart devices, corrupt data, and destroy information [39], [40].

The goal of the Interrupt Attack is to prevent the system from being available. Resources would run out and smart gadgets would shut down as a result [7], [33]. The receiver device is unable

The Seybold Report
ISSN 1533-9211
DOI 10.17605/OSF.IO/YSZDC

to choose which packets to deliver if someone is listening in on the communication channel. RFID technology is susceptible to eavesdropping attempts [34]. Attackers may change or change data or information clever IoT devices to deceive the protocol for communication. The integrity of the IoT network security requirements is threatened by this assault [35]. To harm the IoT information system and jeopardize IoT authentication, an attacker must enter false data into the IoT architecture. This is known as a fabrication attack [34].

It is possible to misuse and exploit data or information about credentials (such as passwords or keys) connected to actual clients [36]. Attackers target software due to resource buffer overflow or IoT device fatigue vulnerabilities. An attacker can launch a hardware attack by connecting to a device, injecting malicious code, or stealing the device's driver.

Physical attacks are likely to interfere with hardware because most smart gadgets are used outdoors. Hardware attacks resemble physical assaults. Without endangering physical objects, logical attacks cause communication systems via the IoT network to malfunction.

Attackers may unusually target IoT. On the IoT network, external attackers who pose as insiders may run malicious malware. As a result, attackers can target protocols like protocols for key management and data aggregation, synchronization protocol, etc. by interfering with networks either internal or external. The two major types of protocols are application and network target protocols attacks of deviance [39].

3. MEASUREMENTS KEY TO ENABLEMENT

The Internet of Things is vulnerable to several security assaults from hackers or other types of criminals. Numerous researchers have investigated layer-level perspectives on IoT security countermeasures. The relevant attacks and defenses are outlined for each tier. But there are a lot of things, threats, and defenses dispersed throughout the flexible network. For example, DoS attacks manifest the maximum IoT network layers via malicious attacker perspectives, and various countermeasures are used by RFID devices to deal with attacks across the IoT. As a result, we briefly discuss some typical countermeasures in this part that apply to all network layers as well as smart devices, intelligent objects, and diverse layer combinations.

The two core technologies for the construction and growth of IoT are WSNs (Wireless Sensor Networks) and RFID (Radio Frequency Identification). Furthermore, elaborate illustrations of security plans and actions including technology devices are provided.

3.1 Authentication techniques based on RFID

Using wireless communication, the author can With RFID technology; you can obtain personal information from the microchip. It is possible to identify any item that has an RFID tag or label attached, followed and observed by people and things utilizing RFID apparatus. RFID has been heavily utilized in transportation systems, medical records, and supply chain management [37]. However, RFID and similar technologies and tools make the IoT more risky and practical, in particular when one takes into account possible identification applications in the IoT global network, Technology relating to RFID and tools being the foundation using IoT.

The Seybold Report
ISSN 1533-9211
DOI 10.17605/OSF.IO/YSZDC

To enable identifying procedures within an IoT network, each item with an RFID tag or label. To stop data breaches and authentication are two crucial and practical connections between two items. Controlling access, encrypting data, using IPSEC-based security channels, using cryptography technology, and using physical security, cybersecurity all schemes are types of RFID, cyber security methods.

Access management, such as antenna energy analysis, chip protection, and label failure, is a method to stop assailants from obtaining using incorrect information or data from RFID devices. RFID signals are encrypted using an algorithm by data encryption technology, which forbids data privacy. Additionally, this approach shields data during transmission against eavesdropping and modification by intruders. IPSec protocols and security procedures are integrated into the IPSec-based secure channel to carry out authentication and encryption across the IoT network. Cryptographic technology solutions, which are based on secure communication protocols, the confidentiality, validity, and integrity of RFID systems, as well as the protection of user privacy. The two types of physical security measures are hiding and masking. The covering strategies the encryption devices' intermediate values should be randomly generated, and the covert tactics remove data on energy dependence usage [14].

3.2 Measures based on WSNs

Interconnected smart devices are used in Wireless Sensor Network (WSN) technology for detecting and observing. Applications for it comprise tracking traffic, monitoring businesses, monitoring businesses of the environment, etc.

Through WSN, data and information are gathered and communicated, and attackers actively and aggressively target data or objects with a WSN connection. As a result, it is advised that numerous proper protective measures be implemented to counteract various threats.

Key Management, first. The right algorithm could be created with WSN and security keys shall be generated and updated.

Privacy extensions, forwarding, and backward are common behaviors done to discover authentication and stop collusion attacks. Simple key distribution protocols, Hierarchical key management, dynamic key management, and key pre-distribution procedures protocols are the four used protocols. 2) Confidential Crucial Algorithms. Asymmetric and symmetric important algorithms include both types of key algorithms. Strictly speaking, symmetric key approaches use Skipjack and RC5. Rivest-Shamir-Adleman (RSA) and Elliptic Curves Cryptography (ECC) are two unsymmetrical key methods [38], [39]. Security Routing Protocol is #3. The following techniques are frequently employed by secure routing procedure algorithms: clustering mechanisms, fusion mechanisms for data, numerous hops routing techniques, and vital mechanisms. The Secure Network Encryption Protocol (SNEP) and the Micro Timed Efficient Streaming Loss-tolerant Authentication Protocol (TESLA) are two protocols that are a part of the widely used safe routing technology SPINS security framework protocol. (4) Access Control and Authentication. Lightweight public key authentication, PSK (Pre-Shared Key), random key pre-distribution authentication, auxiliary information authentication, and one-way hash function authentication are examples of authentication technologies. Access

ISSN 1533-9211

DOI 10.17605/OSF.IO/YSZDC

control uses systems for symmetric and asymmetric cryptography. Designing for physical protection. The two elements are node design and antenna design. Node layout entails selecting a security chip, affixing the chip, creating an RF circuit, and creating a data collection device. The antenna's construction must be appropriate over a prolonged period of transmission distances, high adaptability, stability, and other factors.

3.3 Security plans

We briefly list the three types of IoT security systems in this section: those based on the Host Identity Protocol (HIP), Datagram Transport Layer Security (DTLS), and Capability-based Access Control (CapBAC). The benefits and drawbacks of the particular plans are also covered and analysed. In Figure 2, an evaluation chart is shown.

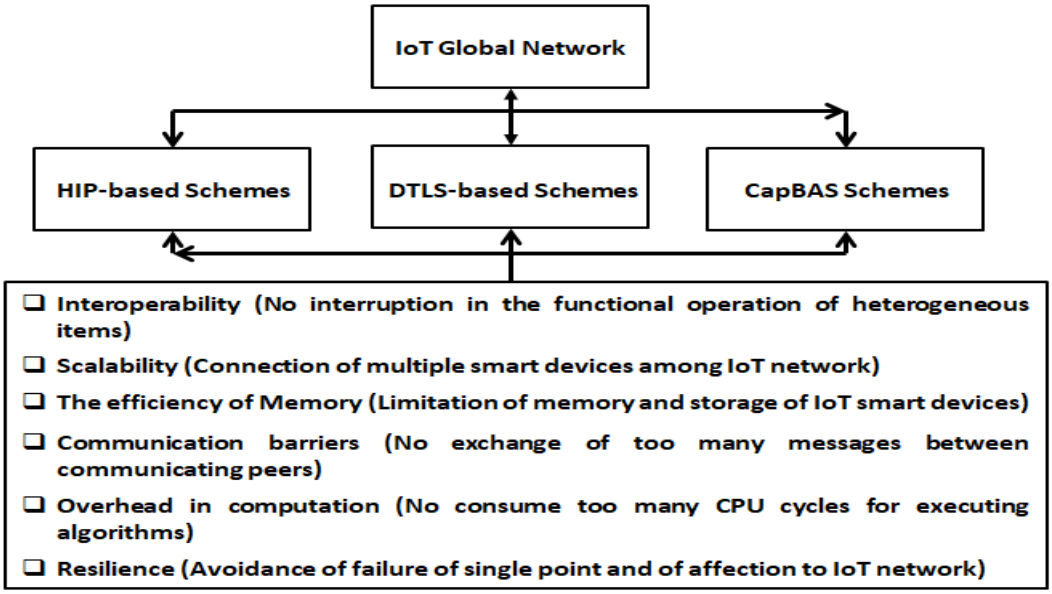

Figure 2: An IoT Security Schemes Evaluation Chart

1) Host Identity Protocol-based systems

These techniques, such as interoperability, and the authentication of IoT devices takes into account scalability, memory efficiency, connection, and computation overhead, and resilience based on device mobility security features [40].

While HIP-TEX [41] uses cryptographic computations for the key exchange in a collaborative setting, HIP-DEX and Slimfit use ECDH (Elliptic Curve Diffie- Hellman) to exchange keys in non-collaborative settings. Because it will drive more IoT traffic, HIP-TEX lacks communication efficiency but is rather efficient in terms of computing and memory. Although Slimfit lacks scalability and interoperability, it offers the benefits of resilience, memory, and communication skills, making it potentially appropriate for IoT. Due to its complicated computation and capacity to attain high degrees that of interoperability, robustness, memory, communication complexity, and scalability, HIP-DEX might ideally be ideal for IoT.

The Seybold Report
ISSN 1533-9211
DOI 10.17605/OSF.IO/YSZDC

2) Methods based on Datagram Transport Layer Security (DTLS)

DTLS-based (Datagram Transport Layer Security) techniques were suggested to protect the IoT network and are based on a new Internet of Things standard. Systems based on DTLS must meet the requirements of interoperability, resilience, communication, memory, computation, and scalability, just like HIP-based schemes.

Smart devices can be mutually authenticated in the Internet of Things, a DTLS based on the X.509 certificates technique was developed [43] without processing a chain of certificates or checking a list of revocations. A trustworthy entity Delegation Server (DS) was used by the delegation-based DTLS methods to manage home network certificate validation. While facilitating interoperability, resilience, and scalability, certificate-based DTLS methods fall short in terms of computing, communication, and memory. In contrast, the benefits of memory, processing, and communication are present based on delegation DTLS methods. Delegation-based systems, however, are susceptible to DoS attacks and single points of failure.

3) Schemes for capability-based access control

Capability-based Access Control (CapBAC) is the method used in the Internet of Things to limit access to authorized users [66]. CapBAC protects access privileges and rights via a cryptographic token. The CapBAC schemes are divided into two categories: distributed and centralized. Distributed CapBAC studies the integration of logic for access control IoT intelligent devices. The distributed schemes include Proxy Assisted schemes, Embedded PDP, etc., whereas the centralized schemes include XACML, SAML-based methods, RADIUS-based schemes, OAuth-based schemes, Kerberos-based schemes, and context-aware systems.

The demands of interoperability, computing complexity, and memory effectiveness are met by a centralized approach. However, there must be a heavy demand for the connection between mobile devices and a third party. A distributed strategy, on the other hand, is good at scaling but falls short concerning interoperability and memory efficiency [39].

4. IMPORTANT INDUSTRIAL APPLICATIONS

To be able to offer safe services for customers, the IoT fully utilizes things, such as devices with intelligence and data from the real world, in a worldwide network. The IoT cyber security system will benefit people from all walks of life in real ways. The level of standard procedures and services, the amount of managing a life-cycle, and the level of corporate cooperation all increase with increased interactions and interoperability. Data networks, sensor technology, and control systems are crucial to the industry. The drawbacks of this trend have increased both the quantity and variety of cyber security threats. Healthcare, smart cities, interior design, transportation and parking management, and other industries have all witnessed an increase in cyber-attacks against systems and infrastructure.

4.1 Industry of Healthcare Services

IoT's fundamental traits include thorough information recognition, dependable information delivery, and intelligent information processing. The Internet of Things (IoT) revolution has

The Seybold Report
ISSN 1533-9211
DOI 10.17605/OSF.IO/YSZDC

accelerated the medical system's informationization process. The integration and cooperation in healthcare use of the conventional information technology sector will be improved by the deployment of IoT technology [1], [2].

Information on medicine, identity, urgent medical situations, remote supervision, home health, the manufacture of drugs oversight, tracking of healthcare waste and equipment, management of blood, preventing infection, and numerous other aspects of the healthcare sector are all connected to IoT cyber security. To create networks, information, and personal functions, for instance, medical information has typically required manual entry. Information is asymmetrical, and each department and participant is comparatively independent. IoT technology entirely overcomes these restrictions thanks to its accessibility and terminal scalability. It helps healthcare systems to cooperate on a range of service tasks and increase overall information levels more successfully.
Wireless wearables are instruments that can be used in the healthcare sector to enhance fundamental operations and become more cost-effective. Cyber security assaults, such as denial-of-service attacks (DoS), remote brute force attacks, man-in-the-middle attacks, password sniffing, Trojan horses, and data manipulation, directly endanger the integrity, accessibility, and confidentiality of healthcare systems. The Security and confidentiality issues that Smart devices and wireless technologies for the healthcare industry face are addressed in.

Because IoT technology is widely employed in the healthcare sector, there are now more security and privacy concerns. It permits object tracking and unlawful item identification in addition to data privacy, dependability, and integrity. For instance, a hacker may use an RFID tag fake to send the reader a warning message or utilize an overlapping signal to block an endless a reader and an RFID tag are connected via a communication connection in the Internet of Things. This will drastically jeopardize patient safety and confuse the medical information system. Health care will advance IoT and related technologies have evolved into intelligence, e-information, AI, personalization, and mobility [19].

4.2 Smart sites

IoT has linked individuals to various objects, including social networks, Smart meters, smart meters in cities, smart meters in households, and smart devices. Unprecedented gains in quality of life will result from IoT. The creation of intelligent surroundings and self-aware/autonomous devices, such as smart homes, smart cities, smart transportation, smart health, and smart living, is one of the objectives of the Internet of Things.

Attacks and unauthorized access to information are included in cyber security, which causes service availability to be disrupted. Technical problems in intelligent environments are brought on by data privacy and emergency response. For cyber security, the IoT infrastructure must be private, self-reliant, and dependable to safeguard and advance the intelligent setting. Only authorized users, for instance, can view all IoT-related smart devices in a smart home. It's important to keep the password for IoT-related smart devices private. A family is shielded from prospective attackers by auto-immunity through an alert. A smart house is made up of various smart systems' parts. By combining the network layer, the application layer, and the awareness

The Seybold Report
ISSN 1533-9211
DOI 10.17605/OSF.IO/YSZDC

layer, a dynamic heterogeneous architecture is created. The universal IoT devices all operate under the same operating standard the IoT-based architecture for the smart house. Without directly gaining access to associated devices, the IoT device organization system establishes a connection with the access center. Access centers and IoT devices frequently communicate using wireless technologies. IoT device management and user interaction are possible through a variety of platforms. Take a personal computer, for instance. Directly communicating through the access with the device center and accessing the Internet center via a cloud service on the internet are two often utilized interaction techniques.

4.3 System for transportation and parking

In the framework of IoT development, the Transportation IoT was proposed. Concerning the use of IoT-related technologies. It can set up the entire method of vehicle monitoring, traffic efficiency and safety, smart traffic management in cities, and automatic vehicle acquisition comprehensive information about road conditions enable the automatic vehicle. Transport and logistics systems are undergoing a new revolution because of IoT technology. IoT traffic management and control will be effective thanks to the intelligent transportation system. To prevent electronic toll collection, mobile emergency command and dispatch, traffic enforcement, vehicle violation monitoring, environmental pollution reduction, and anti-theft systems, as well as to avoid traffic jams, traffic accidents, intelligent beacons, and reduce arrival delays, IoT-based infrastructure and systems can be used.

These IoT applications are still in their early stages and do not yet form a substantial network. Future intelligent transportation will be made possible by connecting vehicles to other vehicles, interacting between people and vehicles, and using a vast network of vehicle connections. It will be properly resolved to address transportation issues like congestion in the traffic, pollution in the environment, and safety incidents [1], [2].

5. ISSUES IN RESEARCH & PROJECTED TRENDS

There are numerous types of devices and applications in the global IoT network. Nevertheless, some products might not be created securely issues the first location in mind due to a variety of scenarios and requirements.

To improve IoT cyber security, several difficult problems still need to be solved, including data integrity, data confidentiality, authentication, access control, etc. To achieve the high IoT requirements of cyber security, several technologies, standardization initiatives, and other developing currently, research initiatives are underway. A network system called the IoT connects objects and makes information possible to share and exchange. The main objectives of IoT are simplicity, efficiency, and intelligence. Infrastructure and modern technology form the basis for the use of IoT technology.

5.1 Standardization

Norms and procedures must be changed and combined with diverse things due to the complicated structure of IoT objects. To accomplish shared objectives, a diverse array of

The Seybold Report
ISSN 1533-9211
DOI 10.17605/OSF.IO/YSZDC

people, objects, operating systems as well as languages can be supported by a standardized Internet of Things architecture made up of interfaces, protocols, and data models [16], [28].

The primary organizations that develop new communications and security protocols are the Institute of Electrical and Electronics Engineers (IEEE) and the Internet Engineering Task Force (IETF); they will be crucial to safeguarding the global IoT network. Standards and protocols are listed in full in Table III.

Table 3: Cyber security standards & protocols for IoT

Standards	Security Issue	Application
IEEE 802.15.4	Replay attack, Integrity, Confidentiality, and Authentication	Time-synchronized communications, an access control technique
6LowPAN	Integrity, authenticity, non-repudiation, and confidentiality	Transparent end-to-end security and 6LoWPAN device communications
RPL	Integrity, authenticity, and confidentiality Non-repudiation, replay attack management of the keys	protecting both routing control messages and actions from forged routing updates
CoAP	Integrity, Authentication, Non-repudiation, Replay Protection, and Confidentiality	CoAP application-layer message protection, transparent, granular end-to-end security.

The fundamental guidelines for lower-level communications are established by IEEE 802.15.4, which also serves as the basis to support more advanced IoT connection protocols. In addition to implementing techniques for packet fragmentation and reassembly, 6LoWPAN allows the transmission of IPv6 packets via IEEE 802.15.4. The IETF's Low-Power, Lossless Network Routing (ROLL) Working Group developed the Low-power and Lossy Networks (RPL) to build routing solutions for IoT applications. For particular kinds of applications, RPL offers a framework. Communications at the application layer are supported through the Constrained Application Protocol (CoAP), which is currently being developed by the IETF's Constrained RESTful Environments (CoRE) Working Group.

In actuality, we lack a standardized framework that can combine IoT protocols, applications, and services with data models, ontologies, and data formats. To ensure the compatibility and reliability of IoT systems, programs, and services, a more extensive and generic architecture must be established due to the existing disparate standards.

The Internet of Things (IoT) system is a huge platform made up of diverse hardware, software, and protocol. Standardization might be an Eden-like ecosystem for IoT systems, at least temporarily, are unable to accomplish. However, standardization may be the result that enhances and spurs the growth of IoT security. The companies or organizations that implement standardized concerns for both security and IoT.

5.2 Issues in Data

The enormous amount of data produced by the Internet of Things in several industries, including basic personal information about the user, account transaction information, records of their insurance coverage, and information about their employment. When these data are exposed, it will significantly affect people's lives and jobs. In the IoT network, malicious data must be processed. One of the promising cyber security issues in the various IoT cyber security

The Seybold Report
ISSN 1533-9211
DOI 10.17605/OSF.IO/YSZDC

infrastructure layers is data. Data integrity, confidentiality, and privacy are the main concerns. To safeguard data security and information within the IoT network, numerous strategies have been devised. One of the key data challenges in IoT cyber security is data confidentiality. A properly set scenario ensures that only authorised parties may access and use the data, while also preventing the intrusion of uninvited parties. Access control and the authentication process are two crucial cyber security technologies.

From earlier literature, a variety of access control methods have been suggested to protect IoT data confidentiality. Role-Based Access Control is one such strategy (RBAC). To guarantee data authenticity, confidentiality, and integrity during transmission, RBAC interfaces with real-time and dynamic data stream management systems in the Internet of Things. In wireless sensor networks like SEDAN and SAWAN, secure data aggregation using a key distribution method is the second mechanism. Additionally, strategies for anonymization based on data suppression, randomization, or cloaking have been suggested to prevent unwanted access.

The administration, exchange, and gathering of data privately raise new research questions in IoT. Using techniques and technologies connected to RFID is a useful strategy for data security. Multiple mechanisms, comprising Kaos, Tropos, NFR, GBRAM, and PRIS, have been put out to address the IoT's data privacy issues in cyber security. Additionally, security measures like biometric verification and data protection can stop unauthorized consumers' access to data. Data reliability is the maintenance of the data's validity, reliability, and unfalsifiability [2]. It also refers to the protection of information or data against attacks or outside effects when they are being sent and received. Version Control and Cyclic Redundancy Check (CRC) are security measures. Data accessibility guarantees that permitted users can take advantage of their information resources in both typical and unusual circumstances. One of the common threats that should be the focus of cyber security is the denial-of-service (DoS) attack. The majority of functional devices pose some sort of security risk. For instance, the camera, home alarms, and the car's central display system. IoT devices are constantly concerned about the capabilities of the enlarged device rather than strengthening the safety of informational data when it comes to access, transfer, and storage. The IoT-induced information revolution and new security concerns can't be accommodated by traditional security paradigms. The growth and use of IoT are directly impacted by security challenges. Security concerns do not prevent issues with data disposal and security [1].

People now have more convenience thanks to the quick development of big data and IoT, but there are also unprecedented hazards to our information security. American automakers started recalling more than a million Unconnected-equipped vehicles as early as July 2015. The in-vehicle technology has significant security flaws, which is why. These flaws allow hackers to turn off the engine, accelerate, and decelerate using a remote control for the onboard system of the car, and disable the brakes. IoT operates in a virtual environment, therefore gathering and processing data resources is essential to its operation. IoT and technology for large data currently combine numerous services. For instance, hardware, devices, and software for wireless communication (Bluetooth, WI-FI, ZigBee), as well as applications for mobile and cloud services. In terms of mobile, a mobile device (such as a phone) first downloads the mobile

The Seybold Report
ISSN 1533-9211
DOI 10.17605/OSF.IO/YSZDC

application, communicates through the cloud, or is transmitted straight to the terminal, and then sends the instructions for controlling the terminal device. In this manner, IoT intelligent devices can be managed in any circumstance that might through interfering with the internet, sophisticated data activities are made possible.

5.3 Trending in Research

A recent innovation the Internet of Things is changing society on all levels, affecting both individuals and businesses. Numerous cutting-edge technologies and methods are being introduced as a result of the development of the IoT.

1. Secure cloud services

Distributed computing, parallel computing, grid computing, and virtualization are the foundations of cloud computing. IoT may benefit from the vast data storage and analytics offered by cloud computing. How to evaluate and handle a lot of data and information is a serious issue with the development of IoT. Integrating cloud computing into an IoT system is one potential remedy. Costs can be decreased and effective calculation and storage can be achieved by making use of cloud computing develop a platform for IoT [40]. IoT can grow rapidly thanks to cloud computing, which offers a high-quality and dependable infrastructure for the technology. The system for cloud computing is a rather broad platform, though; therefore there are numerous security dangers in how it operates.

System and service IoT have the propensity to be dispersed and housed through cloud platforms so that hardware and software can be accessed whenever, whenever, and without limitations. Wireless Internet and Wi-Fi connectivity systems allow for the deployment of smart devices and their connection to cloud services. To store sensor data, the IoT uses cloud services like Storage-as-a-Service (SaaS) and Database-as-a-Service (DaaS) [41]. However, worries about cyber security have grown. More and more focus will be placed on how to better integrate and utilize the IoT systems and methods already in place to guard against attacks on cloud-based IoT services. The security of cloud databases and services, including software, platforms, and infrastructure as a service (SaaS), and infrastructure, is achieved via technologies, security controls, and tactics (IaaS).

IoT large data is kept on a server using cloud computing technology. Worldwide servers for cloud computing are dispersed. The user does not know where the data is stored because of the server's diversity and complexity, and there are security problems. Cloud computing generally uses virtual technology for data distribution, where numerous simulated machines share only one source. If one data point is not isolated or encrypted, the information gets exposed and is open to easy exploitation by unauthorized users. The complete security of user data is not a promise made by utilising the cloud computing platform. The system for cloud computing is handed over to the client. Platforms for cloud computing may access, analyze, and process data. This limits the end-ability of user's to fully control the data. Data can be easily leaked while being calculated and processed in the cloud. Data transmission and use in IoT devices both carry security issues [42].

The Seybold Report
ISSN 1533-9211
DOI 10.17605/OSF.IO/YSZDC

Creating a secure network setting. For data storage and online applications, a reliable cloud computing platform offers supercomputing capabilities. Its use of cloud computing security measures, like physical security, Security of systems, networks, databases, etc., guarantees the platform's fundamental ability to compute and safeguard end users' data privacy and security against unauthorized access and potential threats. Data protection is achieved via encryption technologies. To properly manage secret codes and locks, use encryption. Within the next several days, data security and systems for the Internet of Things (IoT) based on cloud computing, encryption, access control, and anonymous algorithms will all safeguard privacy.

2. 5G Networks

Wireless and network technologies are two of the foundational components of 5G. Multiple access, massive MIMO, ultra-high density network technologies, modulation coding technology, and multi-carrier technology are examples of wireless technologies. Network technologies include technology for separating the control and user planes and for reconstructing the network functions, mobile edge computing technology, and network slicing technology. 5G will improve the ubiquity, stability, scalability, and cost-effectiveness of seamless global IoT by advancing networking technologies and integrating with smart devices [43]. Since more bandwidth is required to address greater traffic problems and delays, in the IoT, IPv6 is replacing IPv4 implementation since there are more things with IP addresses. The result is, the five-generation (5G) wireless technology has been created and can offer speeds between 10-800Gbps, whereas the previous generation (4G) could only offer speeds between 2-1000 Mbps. Both IPv4 and IPv6 can be integrated by 5G technology. Massive MIMO, Multiple Radio Access, Software Defined Networks (SDNs), Heterogeneous Networks (HetNets), and other technologies will all benefit from the adoption of 5G. Users can now attain exponential growth of data due to the development of smartphones and mobile devices. Demonstrates how tiny cells, like femtocells, are used in an IoT setting. The femtocell will combine voice, video, and data for mobile users. Femtocell networks' efficiency in the Internet of Things will be enhanced by appropriate traffic modeling and deployment techniques. Also, embedded sensors are the main method for gathering and transferring data in the Industrial Internet of Things (IIoT), a fast-developing Internet network [24]. Healthcare systems and 5G technology can be combined. Using safe WMSN (wireless Medical Sensor Network), clients can communicate utilizing a variety of sensors.

Rich source data combines countless systems, but as a worldwide dynamic environment, Intruders possess a fantastic the chance to spot weak goals and conduct assaults within the IoT network. For 5G technology to be compatible with the IoT, cyber security problems such as information privacy, management of information transmission, security procedures, and processes they must all taken into account. Mobile communication networks must meet strict security standards. The high standard of security and confidentiality is made possible by industry security standards and QoS. Services connected to IoT will continue to be in demand. The central component of IoT support is a widespread connection between various objects that has a delay of around one millisecond. There are hard-to-remove bottlenecks in the current

The Seybold Report
ISSN 1533-9211
DOI 10.17605/OSF.IO/YSZDC

network. Because of 5G's low latency, extensive coverage, ultra dense networks, and massive connections, this gap may be filled by 5G networks.

3. Design based on QOS (Quality of Service)

Complex cyber security systems are needed by the pervasive IoT to complete a variety of tasks. The entire IoT network might benefit from and be protected by cyber security architecture built on a QoS-based (Quality of Service) foundation. To help the Internet of Things develop, QoS research is required. Systems for QoS management can raise the bar for RFID technology and cyber security infrastructure.

QoS for IoT cyber security remains an unknown research area, despite extensive research regarding IoT security challenges, applications, design of architecture and protocols, and countermeasures. Consider, for instance, (1) resource limitations connected to IoT.

To address the IoT's resource, bandwidth, memory, and other limits, QoS-based cyber security procedures should be made simpler. (2) Data security. Data privacy is a key concern for IoT security and should be taken into account by QoS-based cyber security methods. Scalability, third. Many sensor nodes and smart devices should be able to be added to a QoS-based network security mechanism.

6. CONCLUSION

Individuals, wireless communication, networking, objects, and technologies collaborate virtually entities to carry out joint goals in the IoT. The entire globe and our daily lives have been significantly changed by IoT. IoT will develop into a secure network for people, computers, devices, procedures, and objects thanks to cyber security. If so, more advanced security will be provided via IoT interoperability, accessibility, integrity, availability, Scalability, confidentiality, and global accessibility. In the coming years, one of the main IoT jobs will be addressing cyber security threats. We have thoroughly examined the crucial facets of IoT cyber security in this article, including the current state of affairs, the nature of the issue, and potential future directions, the most successful defenses from IoT risks, and the applications in various industries. In addition, we presented IoT taxonomy cyber security assaults and the possibility of a four-layered cyber security building block for IoT.

References

1. Salih, K.O.M.; Rashid, T.A.; Radovanovic, D.; Bacanin, N. A Comprehensive Survey on the Internet of Things with the Industrial Marketplace. Sensors 2022, 22, 730. https://doi.org/10.3390/s22030730.
2. Xu H, Yu W, Griffith D, Golmie N. A Survey on Industrial Internet of Things: A Cyber-Physical Systems Perspective. IEEE Access. 2018;6:10.1109/access.2018.2884906. doi: 10.1109/access.2018.2884906. PMID: 35531371; PMCID: PMC9074819.
3. Ghasempour, A. Internet of Things in Smart Grid: Architecture, Applications, Services, Key Technologies, and Challenges. Inventions 2019, 4, 22. https://doi.org/10.3390/inventions4010022.
4. Tawalbeh, L.; Muheidat, F.; Tawalbeh, M.; Quwaider, M. IoT Privacy and Security: Challenges and Solutions. Appl. Sci. 2020, 10, 4102. https://doi.org/10.3390/app10124102.

The Seybold Report
ISSN 1533-9211
DOI 10.17605/OSF.IO/YSZDC

5. K. Shaukat, T. M. Alam, I. A. Hameed, W. A. Khan, N. Abbas and S. Luo, "A Review on Security Challenges in Internet of Things (IoT)," 2021 26th International Conference on Automation and Computing (ICAC), Portsmouth, United Kingdom, 2021, pp. 1-6, doi: 10.23919/ICAC50006.2021.9594183.
6. Rahmani, A.M., Bayramov, S. & Kiani Kalejahi, B. Internet of Things Applications: Opportunities and Threats. Wireless Pers Commun 122, 451–476 (2022). https://doi.org/10.1007/s11277-021-08907-0.
7. Y. Lu, "Industry 4.0: a survey on technologies, applications and open research issues," J. of Ind. Inform. Integ., vol. 6, pp. 1-10, 2017.
8. R. H. Weber, "Internet of things-new security and privacy challenges, Comput. Law Security Rev., vol. 26, no. 1, pp. 23–30, 2010.
9. El-hajj, M.; Fadlallah, A.; Chamoun, M.; Serhrouchni, A. A Survey of Internet of Things (IoT) Authentication Schemes. Sensors 2019, 19, 1141. https://doi.org/10.3390/s19051141.
10. Q. Jing, A. V. Vasilakos, J. Wan, J. Lu, and D. Qiu, "Security of the internet of things: perspectives and challenges," Wireless Networks, vol. 20, pp. 2481–2501, 2014.
11. Kazi Masum Sadique, Rahim Rahmani, Paul Johannesson, Towards Security on Internet of Things: Applications and Challenges in Technology, Procedia Computer Science, Volume 141, 2018, Pages 199-206, ISSN 1877-0509, https://doi.org/10.1016/j.procs.2018.10.168.
12. Landaluce H, Arjona L, Perallos A, Falcone F, Angulo I, Muralter F. A Review of IoT Sensing Applications and Challenges Using RFID and Wireless Sensor Networks. Sensors (Basel). 2020 Apr 28;20(9):2495. doi: 10.3390/s20092495. PMID: 32354063; PMCID: PMC7249175.
13. F. Alsubaei, A. Abuhussein, and S. Shiva. "Security and Privacy in the Internet of Medical Things: Taxonomy and Risk Assessment," Local Computer Networks Workshops (LCN Workshops), 42nd Conference on. IEEE, 2017, pp. 112-120, doi: 10.1109/LCN.Workshops.2017.72.
14. S. A. Alabady, F. Al-Turjman, and S. Din, "A novel security model for cooperative virtual networks in the IoT era", Springer International Journal of Parallel Programming, 2018, doi: 10.1007/s10766-018-0580-z.
15. Krishna, R.R.; Priyadarshini, A.; Jha, A.V.; Appasani, B.; Srinivasulu, A.; Bizon, N. State-of-the-Art Review on IoT Threats and Attacks: Taxonomy, Challenges and Solutions. Sustainability 2021, 13, 9463. https://doi.org/10.3390/su13169463.
16. A. R. Sadeghi, C. Wachsmann, and M. Waidner. "Security and Privacy Challenges in Industrial Internet of Things," In Annual Design Automation Conference, ACM, 2015, pp. 54.
17. M. Farooq, M. Waseem, A. Khairi, and S. Mazhar, "A critical analysis on the security concerns of internet of things (IoT)," Perception, vol. 111, no. 7, pp. 1-6, 2015.
18. Panagiotis I. Radoglou Grammatikis, Panagiotis G. Sarigiannidis, Ioannis D. Moscholios, Securing the Internet of Things: Challenges, threats and solutions, Internet of Things, Volume 5, 2019, Pages 41-70, ISSN 2542-6605, https://doi.org/10.1016/j.iot.2018.11.003.
19. R. E. Crossler, F. Bélanger, and D. Ormond, "The quest for complete security: An empirical analysis of users' multi-layered protection from security threats," Information Systems Frontiers, pp. 1-15, 2017, Online published, doi:10.1007/s10796-017-9755-1.
20. S. Li and L. Xu, Securing the Internet of Things. Syngress Publishing, Cambridge, MA, 2017
21. A.Mukherjee, ''Physical-Layer Security in the Internet of Things: Sensing and Communication Confidentiality under Resource Constraints,'' In Proc. IEEE, vol. 103, no. 10, pp. 1747–1761, Oct. 2015.

The Seybold Report
ISSN 1533-9211
DOI 10.17605/OSF.IO/YSZDC

22. Mishra, S., Sharma, S.K. & Alowaidi, M.A. Retracted Article: Analysis of security issues of cloud-based web applications. J Ambient Intell Human Comput 12, 7051–7062 (2021). https://doi.org/10.1007/s12652-020-02370-8.
23. A. K. S. Sanger and R. Johari, "Survey of Security Issues in Cloud," 2022 International Mobile and Embedded Technology Conference (MECON), Noida, India, 2022, pp. 490-493, doi: 10.1109/MECON53876.2022.9751959.
24. M. Hossain, M. Fotouhi, and R. Hasan, "Towards an analysis of security issues, challenges, and open problems in the IoT," In Services (SERVICES), 2015 IEEE World Congress on IEEE, 2015, pp. 21-28.
25. A. Mayzaud, R. Badonnel, and I. Chrisment, "A taxonomy of attacks in rpl-based internet of things," International Journal of Network Security, vol. 18, no. 3, pp. 459–473, 2016.
26. S. Alam and D. De, "Analysis of security threats in wireless sensor network," International Journal of Wireless and Mobile Networks, vol. 6, no. 2, pp. 35–46, Apr. 2014.
27. T. Heer, O. Garcia-Morchon, R. Hummen, S. Loong Keoh, S. S. Kumar, and K.Wehrle, "Security challenges in the IP-based internet of things," Wireless Pers. Commun., vol. 61, pp. 527–542, 2011.
28. Yuchong Li, Qinghui Liu, A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments, Energy Reports, Volume 7, 2021, Pages 8176-8186, ISSN 2352-4847, https://doi.org/10.1016/j.egyr.2021.08.126.
29. M. Ali, S. U. Khan, and A. V. Vasilakos, "Security in cloud computing: opportunities and challenges," Inf. Sci., vol. 305, pp. 357– 383, 2015, doi:10.1016/j.ins.2015.01.025.
30. A. Johnson, J. Molloy, J. Yunes, J. Puthuparampil and A. Elleithy, "Security in Wireless Sensors Networks," 2019 IEEE Long Island Systems, Applications and Technology Conference (LISAT), Farmingdale, NY, USA, 2019, pp. 1-3, doi: 10.1109/LISAT.2019.8817338.
31. Miguel Calvo, Marta Beltrán, A Model For risk-Based adaptive security controls, Computers & Security, Volume 115, 2022, 102612, ISSN 0167-4048, https://doi.org/10.1016/j.cose.2022.102612.
32. A. Perrig et al., "SPINS: security protocols for sensor networks," Wireless Networks, vol. 8, pp. 521–34, 2000.
33. F. Al-Turjman and S. Alturjman, "Confidential Smart-Sensing Framework in the IoT Era", The Springer Journal of Supercomputing, 2018, doi: 10.1007/s11227-018-2524-1.
34. Y. B. Saied and A. Olivereau, "D-HIP: A distributed key exchange scheme for HIP-based Internet of Things," in WoWMoM, IEEE, 2012, Online published, doi: 10.1109/WoWMoM.2012.6263785.
35. R. Hummen, J. Ziegeldorf, H. Shafagh, S. Raza, and K. Wehrle, "Towards Viable Certificate-based Authentication for the Internet of Things," In Proc. 2nd ACM Workshop Hot Topics Wireless Netw. Security Privacy, 2013, pp. 37–42.
36. R. Hummen, J. Hiller, M. Henze, and K. Wehrle, "Slimfit—A HIP DEX Compression Layer for the IP-based Internet of Things," In Proc. IEEE 9th Int. Conf. WiMob, 2013, pp. 259–266.
37. Omoogun, Michelle, et al. "When eHealth Meets the Internet of Things: Pervasive Security and Privacy Challenges." In Cyber Security and Protection Of Digital Services (Cyber Security), 2017 International Conference on. pp. 1-7, IEEE.
38. A. S. Elmaghraby, M. M. Losavio, "Cyber security challenges in smart cities: safety, security and privacy," Journal of Advanced Research, Volume 5, No. 4, pp. 491-497, July 2014, doi: 10.1016/j.jare.2014.02.006.

The Seybold Report
ISSN 1533-9211
DOI 10.17605/OSF.IO/YSZDC

39. Z. K. Zhang, M. C. Y. Cho, C. W. Wang, C. W. Hsu, C. K. Chen, and S. Shieh, "IoT security: ongoing challenges and research opportunities." In Service-Oriented Computing and Applications (SOCA), 2014 IEEE 7th International Conference on, IEEE, 2014, pp. 230-234.
40. C. Bormann, A. Castellani, and Z. Shelby, "CoAP: An application protocol for billions of tiny internet nodes," IEEE Internet Comput., vol. 1, no. 2, pp. 62–67, Mar./Apr. 2012.
41. Y. Chen, H. Chen, A. Gorkhali, Y. Lu, Y. Ma, and L. Li, "Big data analytics and big data science: a survey," Journal of Management Analytics, vol.3, no.1, pp. 1-42, 2016.
42. A. T. Hashem, I. Yaqoob, N. B. Anuar, S. Mokhtar, A. Gani, and S. U. Khan, "The rise of "big data" on cloud computing: Review and open research issues," Information Systems, 47, pp. 98-115, 2015.
43. M. R. Palattella et al., "Internet of things in the 5G era: Enablers, architecture, and business models," IEEE J. Sel. Areas Commun., vol. 34, no. 3, pp. 510–527, Mar. 2016.