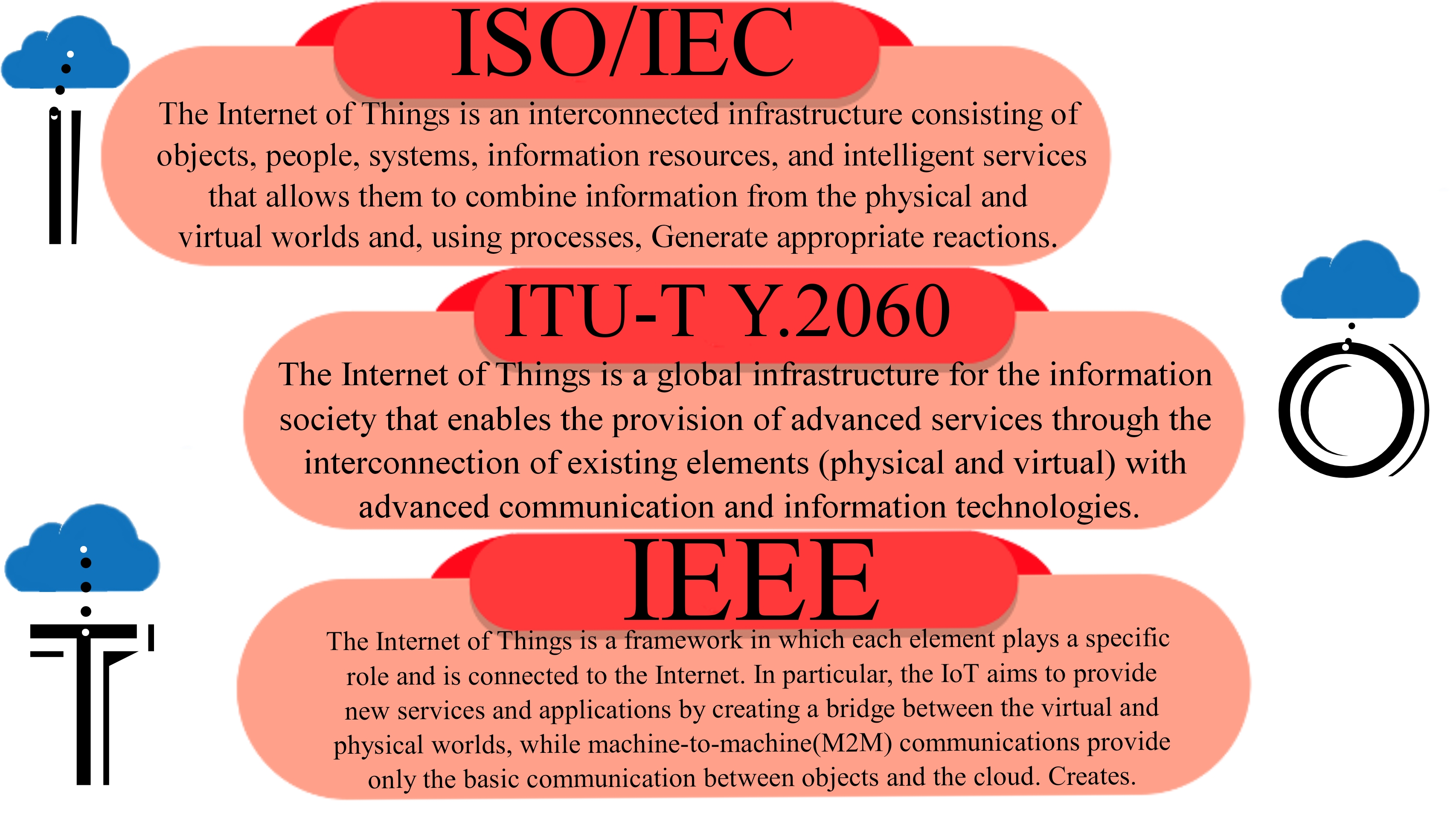
# **Abstract(آخرسر نوشته خواهد شد)**

# **Introduction**

The Internet of Things has evolved from the convergence of wireless technologies, micro electromechanical systems (MEMS), micro services, and the Internet. This convergence has helped to bridge the gap between operational technology (OT) and information technology (IT). and enable the analysis of unstructured data generated by the machine to achieve the desired insight to improve the status quo, Provided. With the advent of the Internet of Things, the two terms real-world and virtual-world seem to be losing their meaning. And the virtual and real worlds will be connected without the human interaction via the Internet. In the IOT, human beings, like other components (computer equipment, mechanical and digital machines, objects, animals) with unique identifiers (UIDs) are identified and have the ability to transmit data over the network. There is no difference between a human being and other components in a bold look. The Internet of Things was first introduced in 1999 by Kevin Ashton, who wanted to draw the attention of executives to a new and exciting technology called RFID. But the idea of ​​connected devices has been known since the 1970s as "embedded Internet" or embedded Internet, and pervasive computing exist. The first Internet object was a beverage machine at Carnegie Mellon University in the early 1980s. However, the concept of "IoT ecosystem" was not realized until mid-2010. Figure 1 shows the definition of the Internet of Things from the perspective of various authorities.



## Figure 1: the definition of the IOT

The scope of IoT applications is divided into consumer, commercial, industrial and infrastructure spaces. One of the main components of IoT devices is made for consumer use. This category includes smart cars, smart homes, wearable technologies, health tools, and remote monitoring programs. In the field of commercial applications, we can mention medicine and health, transportation, home and building automation. IoT in industry includes technology for obtaining and analyzing data from equipment connected to operational technology, situations and individuals in manufacturing and agriculture. In the field of infrastructure, it includes infrastructure management and energy management.

The IoT architecture is composed of several layers, layered architecture provides features that can meet the needs of different industries, companies, institutions, communities, governments. Three-layer architecture includes application, network, and perception layers. The five-layer architecture includes the business layer, the application layer, the middleware layer, the network layer, and the perception layer. The first layer is the layer of perception or objects, which represent the physical sensors of the Internet of Things and are responsible for collecting information (such as location, temperature, weight, motion, vibration, acceleration and humidity, etc.) and processing them. The job of the object abstraction layer is to transfer the data generated by the perception layer through a secure communication channel to the service management layer. The service management layer, or middleware based on name and address, associates the service with its requester. The application layer is responsible for providing the services requested by users and consumers. The business layer manages the overall operations and services of the IoT system. This layer is responsible for creating a graphical and flowchart model based on the data it receives from the application layer.

There are three different types of Internet connection objects:

Device to device (D2D): In this connection, the devices communicate with each other.

Device to server (D2S): In this connection, device data is collected and sent to the server.

Server to Server (S2S): In this connection, server data is shared among other servers for analysis and retransmission to the device.

Four protocols that connect to all different types of connections:

MQTT (Telematics Message Queuing) - This protocol is used to collect device data and transfer it to the server.

XMPP (Extendable Presence and Messaging Protocol) - This protocol is used to connect devices to people who are connected to servers.

DDS (Data Distribution Services) - This protocol is used for fast communication between smart devices.

AMQP (Advanced Message Alignment Protocol) - This protocol is used for effective communication between different servers.

Securing is perhaps the biggest challenge in the Internet of Things. Of course, Internet security is also a big challenge today, but in the Internet of Things, everything is getting bigger. The Internet of Things will create new challenges for IOT tools, their platforms, operating systems, communications, and even interconnected systems. We need advanced security technologies to protect IOT devices and platforms from data breaches, physical vandalism, communications encryption, and response to new challenges (such as copying and executing sleep deprivation attacks that destroy battery packs). IOT security will be complex for many reasons, such as simple existing processors and operating systems that cannot perform complex security measures. IOT experts are also scarce, and security solutions are currently incompatible, and multiple providers may be involved. New threats will emerge in the coming years as cybercriminals develop new attack methods for IOT protocols and devices. Durable objects may have software and hardware that will be updated throughout the life of the product. Further distribution of the network, resulting in more access points to the system as well as more wireless communications, simplifies the conversation and is now more encrypted on the Internet. Encryption is also seen as the key to ensuring information security in the Internet of Things. Finally, many IOT components are characterized by low power and computing power and therefore cannot support complex security support schemes. In particular, the main problems associated with authentication are related to data security and integrity. Authentication is difficult because it usually requires the right infrastructure and authentication servers to achieve the goal by exchanging the right messages between nodes. In the IOT, such methods are not possible because disabled RFID tags cannot exchange many messages with authentication servers. Also, many IOT devices are not currently strong enough to support strong encryption. To enable IOT encryption, algorithms must be more efficient and consume less energy, and effective key distribution programs are required. The same argument (equally limiting) applies to sensor nodes. The last reason is that the Internet of Things is much closer to real life than the current Internet. In fact, infiltrating such a network affects the daily lives of users.

Key management refers to the management of cryptographic keys in a cryptographic system. Managing these keys is a vital activity in an IOT security infrastructure that deals with generating, exchanging, storing, using, and replacing keys as needed at the user level. Key management is an important aspect of any encrypted communication that uses keys to provide information confidentiality and integrity. Key management and protocols used to set up, maintain and control secure relationships between systems are implemented.

**1.1 Contributions**

The initial research contributions of this paper are as follows.

1) Systematic review and classification of previous articles on key management in the Internet of Things. After reviewing the Internet of Things environment, we review its basic features, life cycle process, hierarchical architectures, and security. Then, by providing a precise definition of key management, we follow a structured approach to comprehensively reviewing all key management-related search efforts, including publications and patents.

2) Requirements and challenges we categorize security schemes of key management mechanisms based on IOT architecture layers. We also review and highlight key management schemes separately by creating a framework for analysis and evaluation.

3) Relevant proposed countermeasures with respect to IOT environment. This analysis emphasizes the importance Key management as an essential security requirement that must be applied to all layers of IOT architecture, and I mention the benefits of key management in data and object and communication security.

4) Identify challenges, open issues and future research opportunities to develop key management plans according to the strengths, weaknesses and limitations of key management plans and at the sametime provide guidelines and recommendations with detailed discussions.

Organization

The structure of this survey is as follows: Section 2 introduces the IOT environment definition and IOT key management. Considering the implementation of key management and subsequent comprehensive analysis of key management solutions IOT security requirements And the challenges of identifying IOT security attacks, followed by a discussion of countermeasures, benefits, and key management challenges in the IOT are discussed in Section 3. Then, Section 4 provides a comprehensive analysis and comparison of existing research, as well as existing surveys related to challenges and open issues in Section 5.(این قسمت حتما بعدا تغییراتی خواهد داشت.)

# **Background**

## Internet of Things

Internet of Things is a relatively new concept in the world of information and communication technology and in short it is a modern technology in which for any creature (human, animal or objects) the ability to send and receive data through communication networks, whether Internet or intranet, will be provided. Due to the process of mobile mobilization and people being connected to networks, the implementation of this technology in various fields can make organizations more easily adapted to global and technological changes in the long run, as well as transform their efficiency and profitability. The concept of the Internet of Things is defined as a network of sensors and sensors that collect data from a variety of sources, including clocks, autonomous cars, and thermostats and manufacturing facilities, and ultimately process it at the edge or in the cloud to meet the user's needs. (Whether company or consumer) Extensive use of connected sensors creates a digital world. Data obtained from automated and interconnected physical devices enable the process of transforming the physical world into a digital world.

Three-layer, four-layer and five-layer architectures have been introduced in various articles for the Internet of Things. In this article, five-layer architecture is examined.

The first layer digitizes the perceived data layer and transmits it to the next layer through a secure communication channel. It is in this layer that bulky data is generated.

In the object abstraction layer, data can be transmitted through various technologies such as RFID, 3G, GSM, UMTS, wifi, Bluetooth, Low energy, ZigBee and infrared and non-infrared. In addition, other tasks such as cloud computing and data management can be performed at this layer.

The service management layer allows programmers to work with heterogeneous objects without regard to a specific hardware platform. It is also capable of processing incoming data, making decisions, and providing the required services through network protocols.

The application layer can provide the size of the temperature and the amount of humidity according to the type of user request. The importance of this layer for the IoT is that this layer can provide high quality intelligent services to consumers to meet their needs.

The business layer designs, analyzes, implements, evaluates, and monitors IoT-related elements. This layer enables the support of decision-making process based on the analysis of large data, in addition to the task of monitoring and managing the four lower layers. This layer also compares the output of each layer with the output of the ideal state to improve the quality of services and protect the privacy of individuals.

* 1. Security in the Internet of Things

With the expansion of communication networks and devices connected to this network and the formation of what it calls the Internet of Things, the need for a completely new approach to network security and protection (Protect) of the core services of this network Cyberattack attacks are increasingly.In fact, by attaching a piece/device to a network, cyber attackers are likely to attack. If the security of designing these embedded devices- is devices that have a system that is designed for a specific purpose with limited processing capabilities, which is sometimes referred to as embedded systems- The critical infrastructure of this network is in danger. In other words, the vital infrastructure of each network also requires the real-time monitoring of physical devices. Because these embedded devices are highly specialized and often require specific programming and hardware skills, protecting these devices is a challenge. If the system consists of several pieces and the device is not well protected, each of its components can be a route to attack. While computers and old networks have a wide range of security solutions that can be selected, there is no such thing in the Internet space of objects. Here, the use of traditional antivirus programs on these low power devices alone does not work, or it can reduce the face of the device and do not deserve it. In fact, many of these devices are designed to reduce the processing cycle and memory consumption, which the use of viruses hurts. Trying to overcome the security challenge is not an easy task for developers working on the Internet space objects. Recent efforts have been made to establish security standards for the Internet of Things by major security professionals such as Symantec and AMR. But the fact is that given the large number of devices connected to networks at the moment, these activities can be considered late. Extensive security approaches exist to protect the network as a whole, if the components of the network, such as embedded devices, cannot protect themselves. Data-centric methods, such as Machine Learning, can bridge traditional security solutions, Internet of Things, cloud computing and network technologies. Embedded devices are usually not able to store large volumes of data and processing, and generally the problem is not to be aware of a device from its surroundings, but also the problem and opportunity for developers to use machine learning algorithms in order to The rapid processing of input data from millions of devices is uncertain to identify the optimal algorithms between them.

# **3. Goals and Research Questions**

Examining multiple reasons for compromising information on the Internet: objects, types of physical layer attacks; type of attack on wireless information. Considering major threats to technologies such as wireless sensor networks, IPv6, and 6LOWPAN, which are the foundations for the Internet of things, we will discuss security measures. In common with the Internet architecture of objects and above all, the security measures, system encryption will be considered. Checking the security issues in four key layers of the Internet of Things.

Checking how to provide security in terms of the inherent complexity and volume of data and the multiplicity of devices and objects connected to provide appropriate support. Ultimately, it is expected that exactly the needs and standards of security on the Internet can be identified.

And to answer the following questions:

1. Are examining techniques to deal with distributed denial-of-service attacks and ensure that information is recovered after the attack?

2. Are there any measures to protect points of the creation and transmission of information centers, command points, and network entries?

3. The importance of providing security to address the information and communication gap that has emerged and the trust of users?

4. Discover ways to reduce gaps and build confidence?

5. The biggest IPsec issue and the transmission layer approach are their interconnection nodes in order to provide full end-to-end security. Can intermediate nodes be removed and end to end security?

6. Are there solutions to ensure the mobility of connected nodes?

7. Security on which layer of the Internet is the objects more important than the rest of the layers?

# **4. Methods for Reviewing and Extracting Information**

The purpose of this article is to carefully examine the concept of the Internet of Things, to express its fundamental challenges and to provide security solutions on the Internet of Things, as well as to provide a comprehensive classification for existing solutions. In order to achieve this purpose, the Internet-forming layers of objects and components of each identification layer Became.

In order to collect the contents of this research, first, the keywords of the Internet of Things, big data, IOT, WSN, Machine to machine, RFID, networking, dynamic network were searched from different databases to determine the initial sections of the article. Then, to write other sections and zoom on the subject of security on the Internet, the objects were words: Security, Privacy, Trust, Identification, Access Control, Security challenges, Security of IOT, IOT platform, End-To-End Security, COAP, attacks, IOT architecture, searched.

Eventually, 132 articles published in prestigious Elsevier magazines, Springer and IEEE Xplore, as well as articles from some valid conferences, were collected from the databases IEEE Xplore, Science Direct, Google Scholar, Cisco, elsevier.com, Springer.com and analyzed precisely. In addition, the reviewed articles are mostly from 2010 to 2017. The results obtained for viewing are shown in Figures 2 and 3.

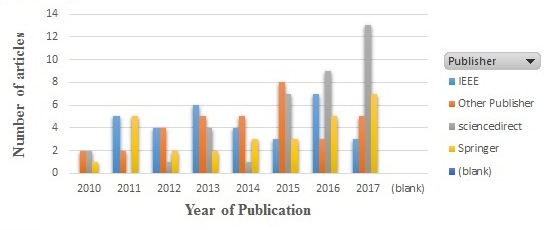


Figure 8: Articles used by year, publications and type

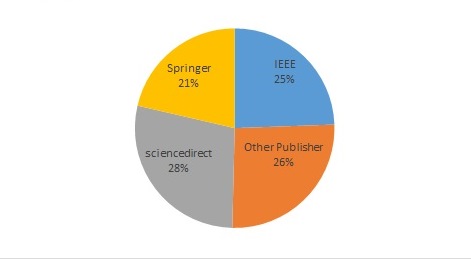


Figure 9: Publications used articles

# **4.** **Related works**

In [25], the classification of communication technologies between two devices or systems for the exchange of automated data of wireless sensor networks, including independent nodes for communication with frequency and bandwidth is limited.

In [52] Examine existing protocols and mechanisms to secure communications in the IoT, as well as issues related to open investigations.

Article [53] The threats in the IOT systems are categorized into four categories: Perceived layer threats, including fake messages, blocker signals, spy or nodes, a DOS based attack, nodes, and eavesdropping of network layer threats. Sybil attack, Python attack, Wormhole, Hail silas, Flood verification. Backup threats such as data abuse, denial of service, unauthorized access The threat target layer is mainly data storage technology. Application layer threats including Sniffer / Loggers, infusion, snap sessions, distributed denial-of-service attacks, and social engineering. Security requirements for Internet objects of the objects: integrity, authorization, confidentiality, integrity, availability and continuity.

In the survey [54] IOT focused on security architecture and security issues and divided the IOT into three layers: the perception layer, the layer of transport, and the layer and application layer. Analyze the security features and security issues of each layer and provide different solutions for these issues.

The [55] Providing security and privacy issues in applications and IOT systems, providing IOT battery limitations and resource calculations, possible solutions for expanding battery life and light weight calculations, as well as the available classification methods for attacks.

In [56] It is anticipated that integrated computing will be integrated with the Internet of Things (IOT) to provide computing devices deployed on the edge of the network in order to improve the user experience and flexibility in the event of a failure. By using distributed architecture and close to end users, fog calculations can provide faster responses and better service quality for IOT applications.

Survey [57] reviews existing protocols and mechanisms to secure communications in the IoT, as well as issues related to open investigations. Also analyzes how existing procedures provide basic security needs and protect communications in the IoT. Along with open challenges and future research strategies in the region. Summarizes the main characteristics of the mechanisms and suggestions analyzed during the review, along with its operational layer, and the security features and supported features.

In [58], the history, background, IoT statistics and security-based Io architectural analysis are discussed. The risks associated with important IoT-related technologies and IoT architecture security have been discussed. In addition, the classification of security challenges in the IoT environment and the classification of various defense mechanisms are presented. There are also various research challenges that still exist in the literature that better understand the problem, provide the current solution space, and future guidelines to defend the IoT against various attacks.

The actual expansion of the IoT service requires the assurance of personal security and security. The extensive review that has been conducted with the [60] review, an overview of security requirements and privacy in a heterogeneous environment, including different technologies and communication standards, is still missing. Appropriate solutions should be designed and implemented that are platform-independent and capable of ensuring: confidentiality, access control and privacy for users and things, assurance among devices and users, compliance with security policies and policies.

Table 3: Comparison of reviews

|  |  |  |  |
| --- | --- | --- | --- |
| Survey | Year | IOT vision | Security issues |
| A Roadmap for Security Challenges in Internet of Things | 2017 |  |  |
| A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications | 2017 | Fog/edge computing | Privacy, Trust, Availability, Integrity, Confidentiality, Identification and Authentication |
| A Survey on Security and Privacy Issues in Internet-of-Things | 2016 | IOT 4-Layer Security | DEVICE LIMITATIONS: battery  capacity and computing power |
| Advanced lightweight encryption algorithms for IOT devices: survey, challenges and solutions | 2017 | encryption algorithms | Security, privacy, trust |
| Determining the Internet of Things (IOT) Challenges on Smart Cities: A Systematic Literature Review | 2016 | smart cities | Concentration of population, scarcity of resources, environmental concerns |
| The Internet of Things: A  survey | 2010 | Things-oriented,  Internet-oriented and Semantic-oriented | Identification,  authentication, integrity,  privacy, trust |
| Internet of things: Vision,  applications and research  challenges | 2012 | anything communicates,  anything is identified, and  anything interacts | Data confidentiality,  privacy, trust |
| Context Aware Computing for The Internet of Things: A Survey | 2013 | Things to be connected  Anytime, Anyplace, with  Anything and Anyone,  using Any path, network  And Any service. | Identification, privacy,  trust |
| Internet of Things (IOT):  A Vision, Architectural  Elements, and Future  Directions | 2012 | up centric vision | Identification,  authentication, integrity,  privacy |
| Security for the Internet  of Things: A Survey of  Existing Protocols and  Open Research issues | 2015 | 5-Layer architecture | Authentication, integrity,  confidentiality, trust,  access control |
| Security, privacy and  trust in Internet of  Things: The road ahead | 2015 | A collection of smart  devices that interact on a  collaborative basis to  fulfill a common goal | Privacy, trust, integrity,  confidentiality,  identification,  authentication |
| Internet of Things: A  Review of Surveys Based  on Context Aware  Intelligent Services | 2016 | Different perspectives:  services, connectivity,  communication and  Networking viewpoints. | Privacy, integrity, access  control, trust,  Identification. |
| The Internet of Things: A  Survey from the  Data-Centric Perspective | 2013 | Things-oriented,  Internet-oriented and  Semantic-oriented | Identification, integrity,  Privacy |
| Internet of Things: A  Review of Surveys Based  on Context Aware  Intelligent Services | 2016 | Different perspectives:  services, connectivity,  communication and  Networking viewpoints. | Privacy, integrity, access  control, trust,  Identification. |
| Towards Internet of  Things: Survey and  Future Vision | 2013 | 3-Layer architecture,  5-Layer architecture | Physical security, privacy |
| Security, privacy and trust in Internet of Things: The road ahead | 2015 | Secure middleware’s, FTBAC framework | Trust‌, Privacy, Enforcement |
| Survey of Security and Privacy Issues of Internet of Things |  | information exchange technologies‌, surveyed all the security flaws  existing in the Internet of Things | On the secrecy and authentication  Silent attacks on service integrity  Attacks on network availability |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

### **IKEv2/IPsec-based solutions**

IKE is an IPsec component used to perform cross-authentication and to create and maintain security associations (SAs). Based on the Oakley and ISAKMP protocols, IKE uses the X.509 certification to authenticate - or before it is shared. Distributed or distributed using DNS (preferably with DNSSEC) and a Diffie-Hellman key exchange - to create a shared shared repository from which the encryption key is obtained. Additionally, a security policy for each partner who establishes the connection must be kept manually. IKE will usually listen to and send to the UDP port 500, although IKE messages can also be received on a slightly different UDP port 4500 port. Since the UDP protocol is a datagram protocol (unreliable), the IKE uses its definition of transmission errors, including packet loss, packet playback and packet forging. IKE is designed to be designed for as long as at least one of the packages sent before its destination reaches its destination, and the channel of unpacked and unpacked packets does not spread to the capacity of the network or CPU of each end point. Destroy Even in the absence of the minimum functional requirements, IKE is designed to run on a regular basis (as the network is broken). Although IKEv2 messages are intended, they are short, but they include structures that have no limitations (in particular X.509), and IKEv2 does not have a place to segment large messages. IP defines a mechanism for splitting large UDP messages, but implementations are supported at the maximum message size. In addition, using IP fragmentation opens up implementation for denial of service. Finally, some NAT and / or firewall implementations may block IPs [90].

The IKEv2 exchange is variable. At best, it can exchange as few as four packets. At worst, this can increase to as many as 30 packets (if not more), depending on the complexity of authentication, the number of Extensible Authentication Protocol (EAP) attributes used, as well as the number of SAs formed. IKEv2 combines the Phase 2 information in IKEv1 into the IKE\_AUTH exchange, and it ensures that after the IKE\_AUTH exchange is complete, both peers already have one SA built and ready to encrypt traffic. This SA is only built for the proxy identities that match the trigger packet. Any subsequent traffic that matches other proxy identities then triggers the CREATE\_CHILD\_SA exchange, which is the equivalent of the Phase 2 exchange in IKEv1. There is no Aggressive Mode or Main Mode.

In effect, IKEv2 has only two initial phases of negotiation:

IKE\_SA\_INIT Exchange: IKE\_SA\_INIT is the initial exchange in which the peers establish a secure channel. After it completes the initial exchange, all further exchanges are encrypted. The exchanges contain only two packets because it combines all the information usually exchanged in MM1-4 in IKEv1. As a result, the responder is computationally expensive to process the IKE\_SA\_INIT packet and can leave to process the first packet; it leaves the protocol open to a DOS attack from spoofed addresses. In order to protect from this kind of attack, IKEv2 has an optional exchange within IKE\_SA\_INIT to prevent against spoofing attacks. If a certain threshold of incomplete sessions is reached, the responder does not process the packet further but instead sends a response to the Initiator with a cookie. For the session to continue, the Initiator must resend the IKE\_SA\_INIT packet and include the cookie it received. The Initiator resends the initial packet along with the Notify payload from the responder that proves the original exchange was not spoofed.

IKE\_AUTH Exchange: After the IKE\_SA\_INIT exchange is complete, the IKEv2 SA is encrypted; however, the remote peer has not been authenticated. The IKE\_AUTH exchange is used to authenticate the remote peer and create the first IPsec SA. The exchange contains the Internet Security Association and Key Management Protocol (ISAKMP) ID along with an authentication payload. The contents of the authentication payload is dependent on the method of authentication, which can be Pre-Shared Key (PSK), RSA certificates (RSA-SIG), Elliptic Curve Digital Signature Algorithm certificates (ECDSA-SIG), or EAP. In addition to the authentication payloads, the exchange includes the SA and Traffic Selector payloads that describe the IPsec SA to be created [91] [92] [93].

## **Encryption Security**

In the traditional network layer, we use the step-by-step encryption method, in this way, the information is encrypted during the sending process, but it is necessary that the main message is maintained at each node through encryption and encryption operations. Meanwhile, in the traditional applications layer, the encryption mechanism is end-to-end encryption, so that the information is explicit for senders and recipients, and encryption is always done in the forwarding and forwarding nodes. In the IOT, the network layer and the application layer are closely interconnected so that end-to-end and close-up approaches should be used, we can only protect the links that need to be protected because, in the network layer, we can apply it to all businesses, which will create a secure implementation of various applications. In this way, the security mechanism in the business applications is clear, which makes it easy for the end user. In this way, this mode creates features in a by-hop mode such as low latency, high efficiency, low cost, and so on. However, due to the decoding operation in the sending node, the use of the by-hop method in each node can lead to the main message of the code, which results in high credibility in the nodes being sent.

Using end-to-end encryption, we can choose different security rules based on the type of business, thus, it can create a high level of security protection in the business security requirements. However, end-to-end encryption cannot encrypt the destination address, since each node determines how to send a message based on the address so that the results cannot be hidden from the source and destination in the message sent, and the unwanted attacks create.

The encryption algorithm is used and their goals are Advanced Encryption Standard

For reliability, Rivest Shamir Adelman, or elliptic curve encryption for digital signature transfer, Diffie-hellman (DH) for the purpose of basic matching and the SHA-1 / SHA-256 algorithm. With the goal of integrity. Generally, the symmetric encryption algorithm is used to encrypt data for reliability such as the Advanced Encryption Standard (AES); the non-symmetric algorithm is also used for use in digital signature applications and important transitions. ECC alignment has also dropped and may be welcomed in recent applications. In order to use these cryptographic algorithms, available resources such as processor speed and memory are required. As a result, how to apply these encryption methods to the IOT is not clear [62].

## **Key management in IOT**

Key management is the mainstay of the security mechanism, and it's a hard side to cryptographic security. Lightweight or high-performance encryption algorithms for sensor nodes are not currently functional, so the sensor network is rarely used on a large scale, on the one hand, an efficient key management protocol that provides complete security for IoT devices are enabled. Optimal storage protocol for devices and sensors is required due to limited resources (save and compute) [96]. Key end-to-end lightweight key management protocols include the initial exchange phase, secure communications between two parties proving representatives of third parties from constration nodes to remote server secret generation and delivery termination phase [97].

Public Key Infrastructure (PKI) is the basis for Internet security (IoT). PKI is one of the mainstays of confidentiality of information, information integrity, authentication, and data access as an accepted and reliable standard. The PKI is the basis for communicating between IoT devices and operating systems. The protection of the IoT requires the assurance of proper security and deployment that includes three key elements of trust: the basic security of the device, data and privacy, and compliance with standards and critical maintenance. The PKI is unique to providing the essential and essential IoT security needs. The PKI provides the necessary authentication and encryption components for IoT for data security, and this is a proven solution and market platform ready for today's IoT security. PKI is a robust technology solution for authenticating and encrypting device communications [98]. Security in both networks and the link layer requires two key management protocols. IKE is a heavyweight protocol, and IKE is not perfect for restricted UI resources on the Internet (IoT). But the IKEv2 compressed 6LoWPAN style, which can be pre-run and evaluated with the 6LoWPAN compressed IPsec, and also the use of IKEv2 for key management for IEEE 802.15.4, is also suitable for link layer security [99].

# **10. Conclusion**

|  |  |
| --- | --- |
| Abbreviation | Definition |
| AAA  AMQP  API  AES  4G | Authentication, Authorization and Accounting  Advanced Message Queuing Protocol  Application programming interfaces  Advanced Encryption Standard  The fourth generation of broadband cellular network technology |
| 6LoWPAN | is an acronym of IPv6 over Low-Power Wireless Personal Area Networks |
| CoAP  CoRE  CPS  DDS | The Constrained Application Protocol  Constrained Restful Environments  Cyber-Physical systems  Data Distribution Service |
| DoS  DSCPs  EMPP | Denial of Service  Distributed stream computing platforms  Extensible Messaging and Presence Protocol |
| HVAC | Heating Ventilation and Air Conditioning |
| ICT  IDS  IETF | Information and Communication Technology  Intrusion Detection System  Internet Engineering Task Force |
| IOT | Internet of Tings |
| IPv6  LLLNs  LPWAN  MQTT  NB-IoT | Internet Protocol version 6  Low-power and Lossy Networks  low-power network  Message Queue Telemetry Transport  Narrowband IoT |
| NFC  OAuth | Near-field communication  Open Authorization |
| OSI | Open Systems Interconnection |
| QR code | Quick Response Code |
| RFID  RSA | Radio-frequency identification  Rivest Shamir Adelman |
| SIoT | Social IoT |
| SLR | Systematic Literature Reviews |
| TCP | Transmission Control Protocol |
| TEE | Trusted Execution Environment |
| UDP | User Datagram Protocol |
| UMTS | Universal Mobile Telecommunications Service |
| Wi-Fi | Wireless Internet |
| WiMAX | Worldwide Interoperability for Microwave Access |
| WSN | wireless sensor network |
|  |  |
|  |  |

**Abbreviation table**

# **References**

[1] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, “Internet of Things (IoT): A vision, architectural elements, and future directions,” *Futur. Gener. Comput. Syst.*, vol. 29, no. 7, pp. 1645–1660, 2013.

[2] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, “Security, privacy and trust in Internet of Things: The road ahead,” *Comput. Networks*, vol. 76, pp. 146–164, 2015.

[3] S. Singh, P. Kumar, S. Seo, Y. Moon, and J. Hyuk, “Advanced lightweight encryption algorithms for IoT devices : survey, challenges and solutions,” *J. Ambient Intell. Humaniz. Comput.*, vol. 0, no. 0, p. 0, 2017.

[4] A. Riahi Sfar, E. Natalizio, Y. Challal, and Z. Chtourou, “A Roadmap for Security Challenges in Internet of Things,” *Digit. Commun. Networks*, 2017.

[5] S. Li, L. Da Xu, and S. Zhao, “The internet of things: a survey,” *Inf. Syst. Front.*, vol. 17, no. 2, pp. 243–259, 2015.

[6] M. Weiser, “The Computer for the 21st Century.”

[7] A. Whitmore, A. Agarwal, and L. Da Xu, “The Internet of Things???A survey of topics and trends,” *Inf. Syst. Front.*, vol. 17, no. 2, pp. 261–274, 2015.

[8] L. Atzori, A. Iera, and G. Morabito, “The internet of things: A survey,” *Comput. networks*, vol. 54, no. 15, pp. 2787–2805, 2010.

[9] D. Miorandi, S. Sicari, F. De Pellegrini, and I. Chlamtac, “Internet of things: Vision, applications and research challenges,” *Ad Hoc Networks*, vol. 10, no. 7, pp. 1497–1516, 2012.

[10] L. A. Grieco, M. Ben Alaya, T. Monteil, K. Drira, and P. Bari, “Architecting Information Centric ETSI-M2M systems,” pp. 211–214, 2014.

[11] N. Aleisa and K. Renaud, “Privacy of the internet of things: a systematic literature review (extended discussion),” pp. 1–10, 2016.

[12] J. Zhou, Z. Cao, X. Dong, and A. V Vasilakos, “Security and privacy for cloud-based IoT: challenges,” *IEEE Commun. Mag.*, vol. 55, no. 1, pp. 26–33, 2017.

[13] L. Lann, “Open Archive Toulouse Archive Ouverte ( OATAO ),” vol. 7, pp. 61–78, 2013.

[14] E. I. Systems, “A conceptual framework and classification of capability areas for business process maturity,” no. May, 2012.

[15] S. Li, L. Da Xu, and S. Zhao, “The internet of things: a survey,” *Inf. Syst. Front.*, vol. 17, no. 2, pp. 243–259, 2015.

[16] L. Atzori, A. Iera, G. Morabito, and M. Nitti, “The Social Internet of Things ( SIoT ) – When Social Networks meet the Internet of Things : Concept, Architecture and Network Characterization $,” vol. 56, no. 16, pp. 3594–3608, 2012.

[17] T. Yousuf, R. Mahmoud, F. Aloul, and I. Zualkernan, “Internet of Things ( IoT ) Security : Current Status, Challenges and Countermeasures,” vol. 5, no. 4, pp. 608–616, 2015.

[18] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, “A survey on internet of things: architecture, enabling technologies, security and privacy, and applications,” *IEEE Internet Things J.*, 2017.

[19] H. Cai *et al.*, “IoT-Based Con fi gurable Information Service Platform for Product Lifecycle Management,” vol. 10, no. 2, pp. 1558–1567, 2014.

[20] S. Fang *et al.*, “An Integrated System for Regional Environmental Monitoring and Management Based on Internet of Things,” vol. 10, no. 2, pp. 1596–1605, 2014.

[21] S. Ri *et al.*, “Applications of Internet of Things on smart grid in China,” pp. 13–17, 2011.

[22] H. Hsu, C. Lee, J. C. Hung, and T. K. Shih, “Smart object reminders with RFID and mobile technologies,” vol. 7, pp. 317–327, 2011.

[23] H. Schaffers, N. Komninos, M. Pallot, and B. Trousse, “Smart Cities and the Future Internet : Towards Cooperation Frameworks for Open Innovation,” pp. 431–446.

[24] L. Atzori, S. Member, A. Iera, S. Member, and G. Morabito, “SIoT : Giving a Social Structure to the Internet of Things,” vol. 15, no. 11, pp. 1193–1195, 2011.

[25] Y. E. Gelogo, H. J. Hwang, and H. Kim, “Internet of Things ( IoT ) Framework for u-healthcare System,” vol. 9, no. 11, pp. 323–330, 2015.

[26] W. S. Network, “Internet of Things : Survey of the Security Challenges and Countermeasures,” no. January 2016, 2017.

[27] F. A. Alaba, M. Othman, A. T. Hashem, and F. Alotaibi, “Author ’ s Accepted Manuscript Internet of things Security : A Survey Reference :,” 2017.

[28] A. Aktas, K. Erhan, S. Ozdemir, and E. Ozdemir, “Experimental investigation of a new smart energy management algorithm for a hybrid energy storage system in smart grid applications,” *Electr. Power Syst. Res.*, vol. 144, pp. 185–196, 2017.

[29] M. R. Elhebeary, M. A. A. Ibrahim, M. M. Aboudina, and A. N. Mohieldin, “Dual-Source Self-Start High-Efficiency Microscale Smart Energy Harvesting System for IoT,” *IEEE Trans. Ind. Electron.*, vol. 65, no. 1, pp. 342–351, 2018.

[30] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, “Security, privacy and trust in Internet of Things: The road ahead,” *Comput. Networks*, vol. 76, pp. 146–164, 2015.

[31] M. A. Razzaque, M. Milojevic-jevric, A. Palade, and S. Clarke, “Middleware for Internet of Things : a Survey Middleware for Internet of Things : A Survey,” no. January, 2015.

[32] S. Bandyopadhyay, M. Sengupta, S. Maiti, and S. Dutta, “R OLE OF M IDDLEWARE FOR I NTERNET OF T HINGS : A S TUDY,” vol. 2, no. 3, pp. 94–105, 2011.

[33] J. F. Ensworth, S. Member, M. S. Reynolds, and S. Member, “BLE-Backscatter : Ultralow-Power IoT Nodes Energy ( BLE ) Smartphones and Tablets,” pp. 1–9, 2017.

[34] A. F. H. Iii, V. Khanna, G. Tuncay, R. Want, and R. Kravets, “Bluetooth Low Energy in Dense IoT Environments,” no. December, pp. 30–36, 2016.

[35] S. R. Hussain, S. Mehnaz, and S. Nirjon, “Secure Seamless Bluetooth Low Energy Connection Migration for Unmodified IoT Devices,” vol. 1233, no. c, pp. 1–17, 2017.

[36] H. Chang, “A connectivity-increasing mechanism of ZigBee-based IoT devices for wireless multimedia sensor networks,” no. 580, 2017.

[37] A. H. Joyce and M. Saravanan, “Design of Digital ZigBee Transmitter for IoT Application,” vol. 1, no. 3, pp. 153–156, 2017.

[38] I. Vaccari, E. Cambiaso, and M. Aiello, “Remotely Exploiting AT Command Attacks on ZigBee Networks,” pp. 1–14, 2017.

[39] C. W. Badenhop, B. W. Ramsey, B. E. Mullins, and L. O. Mailloux, “Extraction and analysis of non-volatile memory of the ZW0301 module , a Z-Wave transceiver,” *Digit. Investig.*, vol. 17, pp. 14–27, 2016.

[40] C. W. Badenhop, S. R. Graham, B. W. Ramsey, B. E. Mullins, and L. O. Mailloux, “The Z-Wave routing protocol and its security implications,” *Comput. Secur.*, vol. 68, pp. 112–129, 2017.

[41] S. Raza, T. Voigt, and U. Roedig, “6LoWPAN Extension for IPsec 6LoWPAN Extension for IPsec,” no. January 2011, 2014.

[42] H. A. A. Al-kashoash, S. Member, M. Hafeez, A. H. Kemp, and S. Member, “Congestion Control for 6LoWPAN Networks :,” vol. 4662, no. c, pp. 1–11, 2017.

[43] R. Muhendra, A. Rinaldi, and M. Budiman, “Development of WiFi Mesh Infrastructure for Internet of Things applications,” *Procedia Eng.*, vol. 170, pp. 332–337, 2017.

[44] S. Member, M. O, O. Ali, and I. F. Akyildiz, “RF Energy Harvesting and Transfer for Spectrum Sharing Cellular IoT Communications in 5G Systems,” vol. XX, no. 114, 2017.

[45] M. Sain, Y. J. Kang, and H. J. Lee, “Survey on Security in Internet of things : state of the art and challenges,” pp. 699–704, 2017.

[46] T. Borgohain, U. Kumar, and S. Sanyal, “Survey of security and privacy issues of Internet of Things,” *arXiv Prepr. arXiv1501.02211*, pp. 1–7, 2015.

[47] A. Whitmore, A. Agarwal, and L. Da Xu, “The Internet of Things—A survey of topics and trends,” *Inf. Syst. Front.*, vol. 17, no. 2, pp. 261–274, 2015.

[48] R. H. Weber, “Internet of Things–New security and privacy challenges,” *Comput. law Secur. Rev.*, vol. 26, no. 1, pp. 23–30, 2010.

[49] R. Roman, J. Zhou, and J. Lopez, “On the features and challenges of security and privacy in distributed internet of things,” *Comput. Networks*, vol. 57, no. 10, pp. 2266–2279, 2013.

[50] C. World, “THE INTERNET OF THINGS :,” no. October, 2015.

[51] N. Lavinia, “Security in the Internet of Things : A Survey on Application Layer Protocols,” 2017.

[52] J. Granjal, J. S. Silva, E. Monteiro, and J. S. Silva, “Security for the internet of things: a survey of existing protocols and open research issues,” *IEEE Commun. Surv. Tutorials*, vol. 17, no. 3, pp. 1294–1312, 2015.

[53] E. Leloglu, “A Review of Security Concerns in Internet of Things,” *J. Comput. Commun.*, vol. 5, no. 1, pp. 121–136, 2017.

[54] Q. Jing, A. V Vasilakos, J. Wan, J. Lu, and D. Qiu, “Security of the internet of things: Perspectives and challenges,” *Wirel. Networks*, vol. 20, no. 8, pp. 2481–2501, 2014.

[55] Y. Yang, L. Wu, G. Yin, L. Li, and H. Zhao, “A Survey on Security and Privacy Issues in Internet-of-Things,” *IEEE Internet Things J.*, pp. 1–10, 2017.

[56] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, “A survey on internet of things: architecture, enabling technologies, security and privacy, and applications,” *IEEE Internet Things J.*, vol. 4662, no. c, pp. 1–1, 2017.

[57] J. Granjal and J. S. Silva, “Security for the Internet of Things : A Survey of Existing Protocols and Open Research issues,” no. c, 2015.

[58] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, “Internet of Things (IoT): A vision, architectural elements, and future directions,” *Futur. Gener. Comput. Syst.*, vol. 29, no. 7, pp. 1645–1660, 2013.

[59] Q. Jing, A. V Vasilakos, J. Wan, J. Lu, and D. Qiu, “Security of the internet of things: Perspectives and challenges,” *Wirel. Networks*, vol. 20, no. 8, pp. 2481–2501, 2014.

[60] S. Sicari, A. Rizzardi, and L. A. Grieco, “Security , Privacy & Trust in Internet of Things : the road ahead,” *Comput. NETWORKS*, no. November, 2014.

[61] Z. Yan, P. Zhang, and A. V Vasilakos, “Journal of Network and Computer Applications A survey on trust management for Internet of Things,” *J. Netw. Comput. Appl.*, vol. 42, pp. 120–134, 2014.

[62] H. Suo, J. Wan, C. Zou, and J. Liu, “Security in the internet of things: A review,” *Proc. - 2012 Int. Conf. Comput. Sci. Electron. Eng. ICCSEE 2012*, vol. 3, no. March, pp. 648–651, 2012.

[63] P. P. Ray, M. Mukherjee, and L. Shu, “Internet of Things for Disaster Management: State-of-the-Art and Prospects,” *IEEE Access*, vol. 5, no. i, pp. 18818–18835, 2017.

[64] T. Zink and M. Waldvogel, “X. 509 User Certificate-based Two-Factor Authentication for Web Applications,” *10. DFN-Forum Kommun.*, pp. 51–61, 2017.

[65] T. Kothmayr, C. Schmitt, W. Hu, M. Br, and G. Carle, “DTLS based Security and Two-Way Authentication for the Internet of Things $,” no. May, 2013.

[66] A. Nayeem, F. Shafiq, M. Aftab, R. S. Pirzada, and S. Ghazala, “Comparison of Security Challenges and Issues of Mobile Computing and Internet of Things,” *World Acad. Sci. Eng. Technol. Int. J. Comput. Inf. Eng.*, vol. 5, no. 6, 2018.

[67] K. Naito, “A Survey on the Internet-of-Things: Standards, Challenges and Future Prospects,” *J. Inf. Process.*, vol. 25, no. 0, pp. 23–31, 2017.

[68] K. Kuladinithi, O. Bergmann, Thomas Pötsch, M. Becker, and C. Görg, “Implementation of coap and its application in transport logistics,” *Proc. Extending Internet to Low Power Lossy Networks*, pp. 1–7, 2011.

[69] A. Bashir and A. H. Mir, “Internet of Things Security Issues, Threats, Attacks and Counter Measures,” in *International Journal of Computing and Digital Systems*, 2018, vol. 7, no. 2.

[70] C. D. Tuen, “Security in Internet of Things,” vol. 9, no. June, p. 100, 2015.

[71] K. Zhao and L. Ge, “A survey on the internet of things security,” *Proc. - 9th Int. Conf. Comput. Intell. Secur. CIS 2013*, pp. 663–667, 2013.

[72] P. Cheng, L. Shi, and B. Sinopoli, “Guest Editorial Special Issue on Secure Control of Cyber-Physical Systems,” *IEEE Trans. Control Netw. Syst.*, vol. 4, no. 1, pp. 1–3, 2017.

[73] D. Barrera, I. Molloy, and H. Huang, “IDIoT: Securing the Internet of Things like it’s 1994,” 2017.

[74] J. A. Jerkins, “Motivating a market or regulatory solution to IoT insecurity with the Mirai botnet code,” *2017 IEEE 7th Annu. Comput. Commun. Work. Conf. CCWC 2017*, 2017.

[75] C. Cao, L. Guan, P. Liu, N. Gao, J. Lin, and J. Xiang, “Hey, you, keep away from my device: remotely implanting a virus expeller to defeat Mirai on IoT devices,” pp. 1–15, 2017.

[76] M. De Donno, N. Dragoni, A. Giaretta, and M. Mazzara, “AntibIoTic: Protecting IoT Devices Against DDoS Attacks,” 2017.

[77] A. Laszka, S. Farhang, and J. Grossklags, “On the Economics of Ransomware,” *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 10575 LNCS, pp. 397–417, 2017.

[78] H. Xu, D. Sgandurra, K. Mayes, and P. Li, “Analysing the Resilience of the Internet of Things against Physical and Proximity Attacks,” vol. 3.

[79] Y. Yang, L. Wu, G. Yin, L. Li, and H. Zhao, “A Survey on Security and Privacy Issues in Internet-of-Things,” pp. 1–10.

[80] G. C. Hadjichristofi, “Internet of Things : Security vulnerabilities and challenges Internet of Things : Security Vulnerabilities and Challenges,” no. July, 2015.

[81] L. Li and I. Engineering, “Study on Security Architecture in the Internet of Things,” no. Mic, pp. 374–377, 2012.

[82] A. Mpitziopoulos, D. Gavalas, C. Konstantopoulos, and G. Pantziou, “A Survey on Jamming Attacks and Countermeasures in WSNs,” vol. 11, no. 4, pp. 42–56, 2009.

[83] L. Yang, C. Ding, M. Wu, and K. Wang, “PT US CR,” *Comput. Networks*, 2017.

[84] S. Tweneboah-koduah, K. E. Skouby, and R. Tadayoni, “Cyber Security Threats to IoT Applications and Service Domains,” *Wirel. Pers. Commun.*, 2017.

[85] P. Moreno-sanchez *et al.*, “Securing the IP-based internet of things with HIP and DTLS Securing the IP-based Internet of Things with HIP and DTLS,” no. April, 2013.

[86] T. Heer, O. G. René, S. Loong, K. Sandeep, and S. K. Klaus, “Security Challenges in the IP-based Internet of Things,” pp. 527–542, 2011.

[87] A. A. Chavan and M. K. Nighot, “Secure and Cost-effective Application Layer Protocol with Authentication Interoperability for IOT,” *Procedia - Procedia Comput. Sci.*, vol. 78, no. December 2015, pp. 646–651, 2016.

[88] S. Sahraoui and A. Bilami, “Efficient HIP-based approach to ensure lightweight end-to-end security in the internet of things,” *Comput. Networks*, vol. 91, pp. 26–45, 2015.

[89] T. Kothmayr, C. Schmitt, W. Hu, M. Brünig, and G. Carle, “Ad Hoc Networks DTLS based security and two-way authentication for the Internet of Things q,” *Ad Hoc Networks*, vol. 11, no. 8, pp. 2710–2723, 2013.

[90] C. Cremers, “Key Exchange in IPsec revisited : Formal Analysis of IKEv1 and IKEv2.”

[91] J. Liu, Q. Li, R. Yan, and R. Sun, “Efficient authenticated key exchange protocols for wireless body area networks,” 2015.

[92] R. A. G. P. Biswas, “Cryptanalysis and Design of a Three-Party Authenticated Key Exchange Protocol Using Smart Card,” 2015.

[93] R. Bonetto, N. Bui, V. Lakkundi, A. Olivereau, A. Serbanati, and M. Rossi, “Secure Communication for Smart IoT Objects : Protocol Stacks , Use Cases and Practical Examples,” 2012.

[94] F. V. Meca, J. H. Ziegeldorf, P. M. Sanchez, and O. G. Morchon, “HIP security architecture for the IP-based Internet of Things,” 2013.

[95] S. Raza, *Lightweight Security Solutions for The Internet of Things*, vol. 2013, no. 139. 2013.

[96] S. Saurabh, A. R. Pais, and S. Chatterjee, “Efficient Key Management in IoT Using Mobile Aggregator BT - Security in Computing and Communications: 4th International Symposium, SSCC 2016, Jaipur, India, September 21-24, 2016, Proceedings,” P. Mueller, S. M. Thampi, M. Z. Alam Bhuiyan, R. Ko, R. Doss, and J. M. Alcaraz Calero, Eds. Singapore: Springer Singapore, 2016, pp. 161–172.

[97] “An overview on security featu.”

[98] A. Kukec, S. Groš, and V. Glavini, “Implementation of certificate based authentication in IKEv2 protocol.”

[99] S. Raza, T. Voigt, and V. Jutvik, “Lightweight IKEv2 : A Key Management Solution for both the Compressed IPsec and the IEEE 802 . 15 . 4 Security,” 2012.