A Survey on Privacy and Security of Internet of Things

Mark Mbock Ogonji[a], George Okeyo[b], Joseph Muliaro Wafula[c]

[a]School of Computing and Information Technology, Jomo Kenyatta University of Agriculture & Technology, P. O. Box 62000-00200 Nairobi, Kenya
Email: mmogonji@yahoo.com

[b]School of Computer Science and Informatics, De Montfort University, The Gateway, LE1 9BH, Leicester, United Kingdom
Email: george.okeyo@dmu.ac.uk

[c]School of Computing and Information Technology, Jomo Kenyatta University of Agriculture & Technology, P. O. Box 62000-00200 Nairobi, Kenya
Email: muliaro@icsit.jkuat.ac.ke

Abstract: Internet of Things (IoT) has fundamentally changed the way information technology and communication environments work, with significant advantages derived from wireless sensors and nanotechnology, among others. While IoT is still a growing and expanding platform, the current research in privacy and security shows there is little integration and unification of security and privacy that may affect user adoption of the technology because of fear of personal data exposure. The surveys conducted so far focus on vulnerabilities based on information exchange technologies applicable to the Internet. None of the surveys has brought out the integrated privacy and security perspective centered on the user. The aim of this paper is to provide the reader with a comprehensive discussion on the current state of the art of IoT, with particular focus on what have been done in the areas of privacy and security threats, attack surface, vulnerabilities and countermeasures and to propose a threat taxonomy. IoT user requirements and challenges were identified and discussed to highlight the baseline security and privacy needs and concerns of the user. The paper also proposed threat taxonomy to address the security requirements in broader perspective. This survey of IoT Privacy and Security has been undertaken through a systematic literature review using online databases and other resources to search for all articles that meet certain criteria, entering information about each study into a personal database, and then drawing up tables summarizing the current state of literature. As a result, the paper distills the latest developments in IoT privacy and security, highlights the open issues and identifies areas for further research.

Keywords – Internet of Things; Security; Privacy; Wireless Sensors; Nanotechnology

1. Introduction

The term “Internet of Things (IoT)” was first used in 1999 by Kevin Ashton, a British technology pioneer [1]–[6]. According to Kevin Ashton, Internet of Things defines the system of physical objects in the world that connect to the internet via a sensor. Internet of Things (IoT) comprises intelligent machines that interact with other machines, objects, environments, and infrastructures. This new technology has had tremendous impact on people’s lives as it helps people to live and work smarter, as well as gain complete control over their lives. In addition to offering smart devices to automate homes, IoT is essential to business. IoT provides businesses with a real-time look into how their systems really work, delivering insights into everything from the performance of machines to supply chain and logistics operations.

Consequently, this new technological reality involves collection and management of vast volumes of data from a rapidly growing network of devices and sensors, processing them and then sharing them with other related things. These new interactions create tremendous opportunities for new services. IoT enables companies to automate processes and reduce labor costs. It also cuts down on waste and improves service delivery, making it less expensive to manufacture and deliver goods, as well as offering transparency into customer transactions. As such, IoT is one of the most important technologies of everyday life, and it will continue to pick up steam as more businesses realize the potential of connected devices to keep them competitive.

The IoT global market is expected to witness a tremendous growth with the heterogeneous devices reaching 28 billion by end of 2020. The sheer amount of data generated by IoT objects can pose a serious threat to people's privacy and security because their activities can be monitored anytime, anywhere [7]. The potential security threats that can be used to harm consumers are: (1) unauthorized access and improper use of personal information; (2) promotion of attacks on other systems; and (3) the increase of security risks.

The research community is currently engaged in IoT research in several domains of which quite a number have been published [2], [8], [9]. However, several issues for further research. For instance, Atzori et al., [8], addressed authentication and data integrity concerns in IoT security and suggested the development of new software applications to control access to personal data during their life cycle. However, their work did not discuss other equally important security concerns such as trust, data privacy and access control. Meanwhile, Miorandi et al., [9] identified only three key security issues to be investigated: data confidentiality, privacy and trust. They did not give adequate attention to authentication, integrity and access control, which were only discussed superficially. Sicari et al., [10] divided the security aspects into three categories: security requirements (authentication, confidentiality and access control), privacy, and trust. The main limitation of this work is the taxonomy of the IoT, which remains unclear and, consequently, the lack of classification of the listed research activities according to a clear sorting logic. Riahi et al., [11] considered security issues that may occur due to interactions among all the system elements, and analyzed their consequences on the global system. They focused their analysis on specific interactions which are directly related to security: privacy, trust, identification, and access control. They however did not consider other interactions such as autoimmunity, safety, reliability and responsibility that are effected during the system design phase as they do not involve enhancing technologies. Farooq et al., [1] analyzed the security issues and challenges and provided well-defined security architecture to guarantee the user’s privacy and security to encourage wider adoption of IoT by masses. Specifically, they addressed authentication, integrity, data confidentiality and data privacy as elements of the IoT security. However, this was not comprehensive enough as they left out trust and access control. Neshenko et al., [12] while having nine IoT vulnerability classes only considered two main vulnerabilities, that is, unnecessarily open ports, and weak programming practices coupled with improper software update capabilities as being responsible for most IoT attacks. The other vulnerabilities were accorded lesser attention. This paper seeks to comprehensively address the main limitations of existing work which can be summarized as: identification, authentication, data integrity, trust, data confidentiality, access control, data privacy and data availability.

Therefore, the main objective of this paper is to provide the reader with a comprehensive discussion on the current state of the art of IoT, with particular focus on what have been done in the areas of privacy and security threats, attack surface, vulnerabilities and countermeasures and to propose a threat

taxonomy. This paper examines the privacy and security of the IoT from the users' point of view, addresses the security requirements on a wider dimension and frames the IoT security framework taking into account the resource constraints of the IoT devices. By fusing IoT architecture with privacy and security principles, the paper proposes IoT threat taxonomy. The paper brings out the latest developments in IoT privacy and security, highlighting the open issues and suggestions for further research. As a result, the contributions of this paper are as follows: The paper: a) provides an overview of Internet of Things concepts, architecture, technology and applications relating to IoT with intent to establish the connection between IoT privacy and security from the users' perspective; b) provides a systematic summary of IoT user security requirements and challenges and analyzes how the security and privacy of users is implemented within the IoT framework; c) tabulates known and documented attack surfaces, threats, vulnerabilities and recommended measures toward securing IoT devices; d) develops a threat taxonomy for the IoT system that classifies threats and vulnerabilities in categories of low, medium, and high with regard to their contribution to data privacy and security of IoT users; and finally, e) identifies countermeasures and links them to threats, vulnerabilities.

The rest of this article is organized as follows: Section 2 describes how the review was conducted. Section 3 describes the IoT concept and presents the need for user centric security and privacy design. Section 4 reviews current research on privacy and security of IoT and identifies threats and vulnerabilities. Section 5 highlights the mitigation measures against IoT vulnerabilities. Section 6 presents the proposed threat taxonomy while section 7 presents important research issues for future research. Finally, Section 8 concludes the survey.

2. Literature Survey Process

This survey adopts a mixture of qualitative and quantitative systematic literature review approach to the problem. According to [13], this method has advantages over the narrative style. It can also identify areas covered by existing studies and highlight gaps. Get closer to literature from various perspectives and promote new insights.

This IoT privacy and security survey uses an online database and other resources to find all articles that meet specific criteria, enter information about each study in a personal database and summarize the current state of the table. It was conducted through a systematic review of the literature [13], [14].

- **Identify Databases:** Published academic journals have become resources from which electronic databases such as Google Scholar, Web of Science, Research Gate and Science Direct are used for collection.
- **Choose Keywords:** Keywords used for the searches were 'Internet of Things', 'IoT', 'privacy', 'security', 'IoT Privacy', 'IoT Security', 'IoT Models', and 'IoT threat taxonomy'.
- **Choose Time Range:** The research was limited to articles published between 2010 and 2020.
- **Choose Exclusion Criteria:** Research focused on academic articles published in English. We also considered news articles, stories and annual reports touching on privacy and security of IoT.
- **Searching & Recording:** Each paper was recorded based on author of information, the year of publication and the journal in which the study was conducted. Subsequently, each article was classified according to the method used and whether the analysis was quantitative, qualitative or mixed. Privacy, threats, violations and awareness of the various technologies were also recorded.
- **Identifying Privacy and Security Gaps:** The analysis was performed to identify privacy and security gaps and make recommendations for future studies.

For this paper, all the scientific papers were accumulated from online resources. Digital databases such as IEEE Xplore, Google Scholar, Science Direct, ERIC and the ACM Digital Library are used to obtain scientific articles for this survey. The chosen literature, as well as the keywords used for search process was IoT Privacy, IoT Security, IoT Models, Principles, Requirements, Challenges, and IoT threat taxonomy. A total of 176 papers were retrieved with 133 of them reviewed (See Fig. 1).

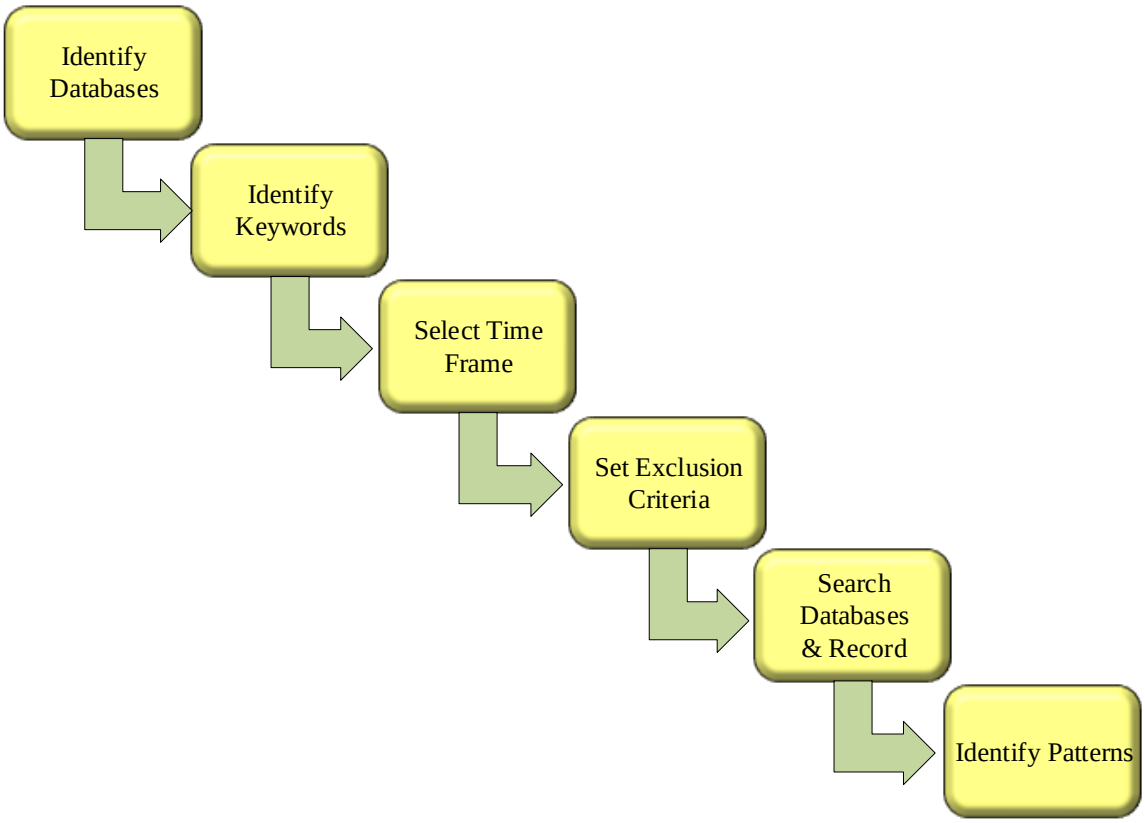

Figure 1: Systematic Literature Review Process

3. Internet of Things and User Centricity

3.1 Overview of IoT

The IoT is a technological phenomenon generated by innovative advancements in information and communication technologies related to ubiquity, pervasiveness and Intelligence [15]. The Internet of Things is a global concept that requires a general, specific, and acceptable definition. The ITU-T 13 research team explains Internet of Things (IoT) as *data that provides advanced services by connecting things (physical and virtual) based on existing and evolving communication and information technologies* [16]. Figure 2 shows IoT that connects people and things anytime, anywhere, anywhere, using any path / network and service [17].

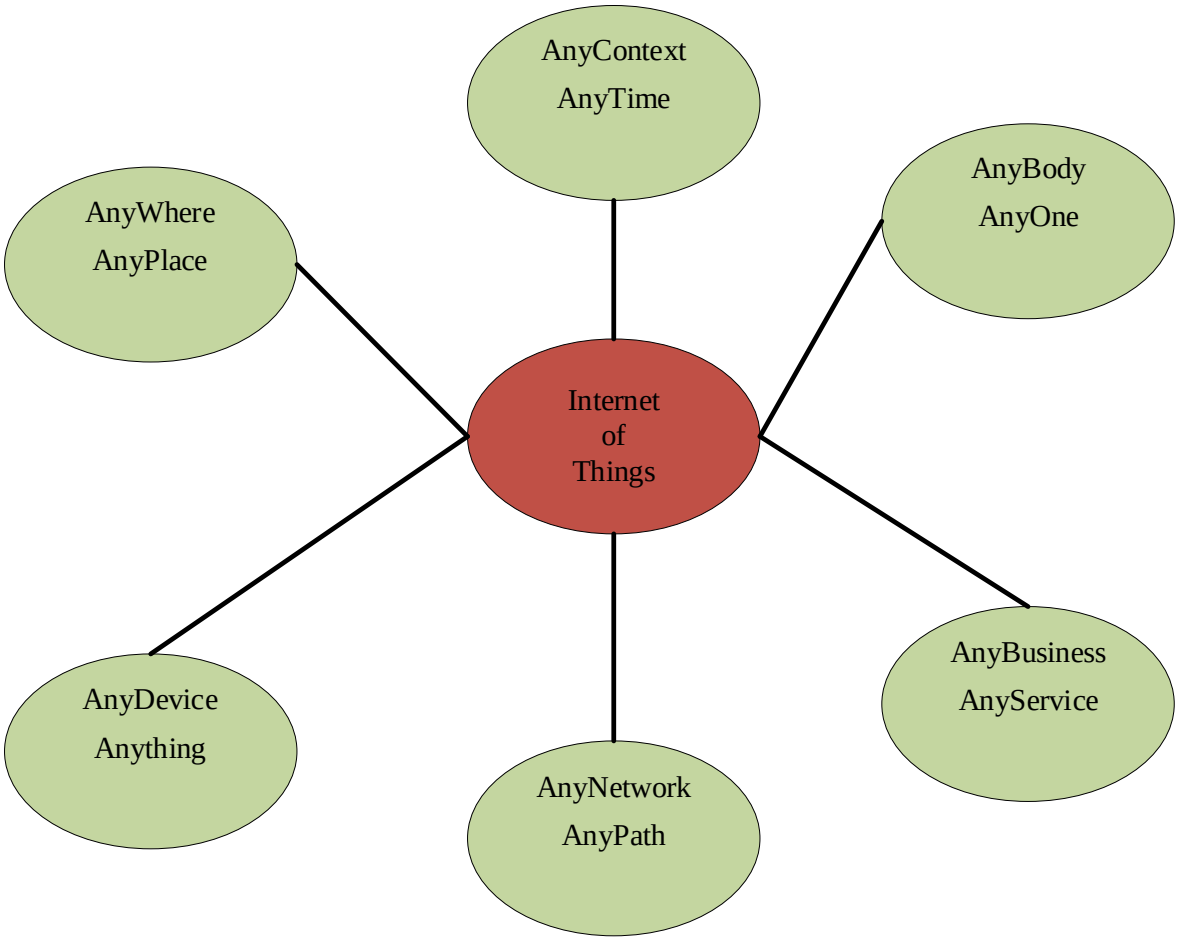

Figure 2: IoT Definition[17]

The IoT requires a seamless flow of information that is enabled by a secure environment between devices that ensure confidentiality, integrity and availability and that the information is not compromised. The information passes through the IoT architectural layers which include perception, network and application layers [16], [18], [19]. The IoT technology impacts several application areas. IoT is used in the design of smart environments and devices that include smart cities and smart health among others[20]. Applications can be classified according to network availability, coverage level, resolution, non-uniformity, repeatability, user engagement, and impact types. Some of the application domains include transportation, retail, healthcare, smart home and energy applications [21].

The deployment and implementation of IoT-based products and services rely on several technologies such as RFID, wireless sensor networks (WSN), middleware, cloud computing, and IoT application software [22]. The range of technologies that make up the IoT determine how users can come to interact with IoT devices. In the case of devices utilizing RFID, for example, identifying information can be shared in a similar way to reading a bar code. Other IoT devices, however, may require users to program their IoT devices using a mobile application. In this context, humans are increasingly incorporating Internet-enabled technologies into their everyday lives. For example, smart refrigerators allow individuals to use smartphones to schedule hot water to be dispensed, and a smart office building can

adjust lighting and temperature to suit workers' preferences based on input received from them or from sensors [2].

The number of actions that can be automated by different devices with distinct user populations is substantial. These devices can be referred to as being part of the "Internet of things" (IoT), a network in which objects share and communicate information with other elements [2]. Although the IoT allows for the transfer of data between devices and many other components, the interconnected nature of the IoT embeds security blind spots that can ultimately leave the devices in IoT susceptible to hacking thereby leading to security and privacy concerns for IoT users.

Researchers have suggested that security issues related to the IoT can be addressed by taking several countermeasures focused on securing accurate data and transferring these data with protection [23]. Such methods include, but are not limited to, performing a more thorough analysis of home router network traffic [24]and increasing device encryption efforts [25]. Unfortunately, most researchers fail to consider that users are regarded as the weakest link in the cybersecurity chain [26], and very few researchers have commented on the value of designing IoT devices with the user as an integral security component [23], [27]. This oversight can prove to be dangerous, as failing to consider the ever-present human component of the system has the potential to render any state-of-the-art security mechanism useless. As such, we argue that to ensure users' safety, researchers and designers must take a human factors approach to cybersecurity in which the human in the loop [28] is considered through-out the design and implementation process. Therefore, the current trends in Internet-enabled technologies need to be considered during the design process to ensure users' privacy and security is addressed. The insights in this paper will be useful to designers and developers who are expected to champion privacy by design principle so as to assure users that their information is secure from hackers.

3.2 Toward User-Centric IoT Security and Privacy

The IoT is a vision of ubiquitous connectivity. With sensors, code, and infrastructure, any object can become networked. Most of the discussion about IoT revolves around smart objects while the user is relegated to the periphery. Therefore, there is need to shift attention to smart people. This would potentially place users at the center of IoT solutions. The user is in this context a human, defined by different characteristics: name, age, job, school level, but also interests, domains of expertise and preferences. This builds the user's profile which could be represented in a computer system. The user is also represented by the context that evolves. A user context includes location, current activity, objects and other users in proximity but also social context. The social context of a user is represented by a set of social relationships with other users and forming the user's social networks.

In intelligent systems, the user plays several roles, i.e., the source of information, the provider of services, and the consumer. The user is therefore at the heart of these processes. That is why some paradigms have appeared giving focus to the user. Several works focus on detecting user profile [29], user social characteristics [30], [31] and to adapting treatments and processes to user context [32]. This paper posits that such works can be reused to achieve a user-centric IoT.

Miranda et al. [33] define the Internet of People (IoP) as bringing the IoT closer to people in order to easily integrate into it and fully exploit its benefits. This could provide a mechanism for serving user's contextual information as it places people at the center of innovation strategies. More than just smart applications and smart cities, the potential of IoP resides in smart people. IoP includes numerous topics, such as Biometric Sensors and Identification Technology, Wearable Technology, Brain Informatics

Processing, Body Area Network technology, Social Computing, and Collective Intelligence, Technology for Biomedical and healthcare application etc. Miranda et al. define a set of features they believe are essential foundations for any approach to the IoP: The features are: (i) IoP should be social and let devices interact with each other and with people more socially than does the IoT; (ii) IoP should be personalized which mean that interactions must be personalized to users sociological profiles and contexts; (iii) IoP should be proactive and not manually commanded by the user; (iv) IoP should be predictable which means that interactions must be triggered according to a predictable context that the user has previously identified, and for which a specific behavior has been defined.

In the IoT environment, user-centricity is concerned with empowering users to take control of their access control and privacy preferences to govern devices. This is because users express their fears about the privacy of their personal data and do not trust connected objects. On the other hand, IoP brings in the integration of technology into people's everyday lives. For example, the user must set parameters within the application, and when the person's context changes, they must manually reconfigure to reflect the new changes. User-centricity puts people (users) in control of their own information and contextual integrity. It allows the Internet to become an Internet, not of smart things, but of smart empowered people.

4. Recent Advances in IoT Privacy and Security

This section reviews the literature on the recent advances in IoT privacy and security focusing on the users of the IoT. The users of IoT systems and devices face various privacy and security challenges. While the research in IoT is still at infancy, there is literature to show that some significant research is going on in this field. This section therefore explores the state of the art in IoT privacy and security with a focus on the user.

4.1 IoT Security

How we deal with the security of the IoT will determine if it transforms the way we live and work. While security was a problem with the traditional Internet, security considerations in the IoT environment presented new and unique security challenges. Addressing these challenges and ensuring the security of IoT products and services should be a top priority. Users should be confident that IoT devices and related data services are safe from vulnerabilities, especially as this technology has become more prevalent and integrated in our daily lives. The main challenge is the integration of security mechanisms and user acceptance. The user should feel that he is controlling any information related to them instead of feeling that the system is controlling them. This integration generates new requirements that, to the best of our knowledge, have not been considered before.

The IoT is extremely vulnerable to attacks for several reasons. First, its components are always unattended making physical attack easy. Second, most of the communications are wireless, which makes eavesdropping extremely simple. Finally, most of the IoT components are characterized by low capabilities in terms of both energy and computing resources and, thus, they cannot implement complex schemes supporting security[8], [34].

In the context of the IoT, security concerns the protection of connected devices and networks. IoT protection protects against unauthorized access to data, Internet threats, denial-of-service attacks, unauthorized access to services, theft or alteration of data, malicious attacks and network security. However, IoT's ability to connect multiple networked automatic devices over the Internet and the ability to interact and manage remotely is likely to lead to the spread of malicious attacks [35]–[37].

In the IoT environment, as well as in traditional areas of the Internet, it is important to ensure the confidentiality, integrity, reliability and availability of data and information [38]. In this connection, the security requirements of IoT systems should provide data validation, intrusion resistance, access control and customer privacy. Relying on smart devices that are interconnected in all areas of our lives creates opportunities for intrusions and interventions that can compromise personal privacy or threaten public safety.

In recent years, a series of surveys covering the IoT research process have been published[2], [8], [9]. They focus on general IoT issues or models [11]. The survey of a broad number of published works led to the conclusion that despite numerous attempts in this field, many challenges and research questions remain open. In particular, Sicari et al., [10] stressed the fact that a systematic and a unified vision to guarantee IoT security is still lacking especially one that focuses on the human user.

4.1.1 IoT Security Concerns

In [8], the authors focused on authentication and data integrity concerns, and proposed research directions for problems, such as a proxy attack and man-in-the-middle attack. Concerning privacy, they suggested developing new software applications to control access to personal data during their life cycle. Although the survey is complete and interesting, it provides insufficient details about security challenges in the IoT. Miorandi et al., [9] said that many challenges arise in security but they identified only three key issues i.e. data confidentiality, privacy and trust. Conversely, they did not give adequate attention to authentication, integrity, and access control. In [2] the authors presented a cloud centric vision for the IoT and illustrated the enabling technologies and application domains of the future. They proposed many research issues based but did not discuss security research issues in depth and their discussions were limited to superficial questions regarding privacy and identity protection.

In [10], the authors adopted an open IoT vision and considered a set of intelligent objects that cooperate to accomplish a common objective. They averred that IoT deployments may involve diverse conceptions, technologies, implementations and architectures to build a communication or to perform a process. They divided the security aspects into three categories: security requirements (authentication, confidentiality and access control), privacy, and trust. The main limitation of this work is the taxonomy of the IoT, which remains unclear and, consequently, the lack of classification of the listed research activities according to a clear sorting logic. Riahi et al., [11] proposed a systemic and cognitive approach for IoT security to cover all that is consistent with the IoT framework. They considered security issues that may occur due to interactions among all the system elements, and analyzed their consequences on the global system. The authors focused their analysis on specific interactions which are directly related to security: privacy, trust, identification, and access control. They however did not consider other interactions that are effected during the system design phase as they do not involve enhancing technologies.

Farooq et al., [1] in their study analyzed the security issues and challenges and provided well-defined security architecture as a confidentiality of the user's privacy and security. They contend that because of the easy accessibility of the objects, they could be easily exploited by the evil-minded hackers. Further, Farooq et al., opined that since the devices have a direct impact on the lives of users, security considerations must be a high priority coupled with well-defined security infrastructure with new systems and protocols that can limit the possible threats related to privacy and security of IoT. Specifically, they addressed authentication, integrity, data confidentiality and data privacy as elements of the IoT security. Their study did not explore in detail authentications, risk assessment and intrusion

detection techniques. Meanwhile, Abdur et al., [39] focused on trust, access control and data privacy. However, their work did not bring out strongly the user centered element.

The following therefore highlights the various security concerns within the IoT environment as summarized in Table 1.

a) *Identification***:** It is most important for a smart device to know when it should or should not reveal its identity. Providing identity to an adversary can be a serious threat [10]. However, we must obtain a system that, at the same time, provides device identity to other qualified devices. Devices that interact with users (humans) must know their identity and be able to distinguish them too[8], [2]**,** [11].

b) *Authentication***:** Authentication is difficult as it usually requires appropriate authentication infrastructures and servers that achieve their goal through the exchange of appropriate messages with other nodes. In the IoT such approaches are not feasible given that passive RFID tags cannot exchange too many messages with the authentication servers. The same reasoning applies to the sensor nodes as well [8], [11]**,** [10]**,** [1].

c) *Data Integrity***:** Cybercriminals can be affected by a variety of other factors beyond their control, such as data changes during the transition and server outages and electromagnetic interference [11]. Data integrity is the use of common surveillance methods to protect this useful information from cybercriminals and to prevent external interference during transmission and reception. Thus, the system cannot change the data without identifying the threat [1]. Methods used to ensure data accuracy and reliability include checksums and cyclic redundancy checks (CRC) used through error detection mechanisms [8], [10]

d) *Trust***:** Trust is a multidimensional, multidisciplinary, and multifaceted concept. The concept of trust covers a bigger scope than security, thus it is more complicated and difficult to establish[8]. It is also related to the concept of privacy that is the ability of an entity to determine whether, when, and to whom personal information could be disclosed[11] [39]. A number of studies aim to improve identity trust and achieve privacy preservation in ubiquitous systems such as IoT. It is widely believed that a user will adopt and use the IoT technology based on the belief that the devices are secured by the manufacturers[9] [10].

e) *Data Confidentiality***:** Data confidentiality secures the user and ensures that confidential information is trusted by using various mechanisms to prevent unauthorized disclosure [1]. Security mechanisms that ensure data privacy include data encryption that protects data from unauthorized access, two-stage authentication that provides authentication by two dependent components, and biometric authentication, each of which is uniquely identified [1], [35]. For IoT-based devices, this ensures that sensor networks do not show the data of sensor nodes to neighboring nodes as well as transmitting the data of labels to an unauthorized reader [1], [9], [35], [40].

f) *Access Control***:** Access control refers to the permissions in the usage of resources, assigned to different actors of a wide IoT network. Access control should focus on IoT capabilities, rather than on a per-device granularity because factors affecting access-control decisions are heavily context-dependent. A number of steps should be taken to provide the requisite access control specification and authentication for the smart device[11][39] .

g) *Data Privacy***:** Due to the proliferation of increased amounts of data in an IoT environment, the existing challenge that data will be used for purposes in addition to or other than those originally specified becomes even more serious to consider. The IoT environment has devices, sensors, readers, and applications which have the potential to collect a multiplicity of data types of individuals as they move through such environments. There is a possibility of individuals being identified because of the aggregated data. The information collected based on object identifiers, sensor data and the connection capabilities of IoT systems might therefore reveal information on individuals, their habits, location, interests and other personal information and other preferences stored for ease of use in systems [8], [2]**,** [11]**,** [39], [9]**,** [10]**,** [1]**.**

h) *Data Availability***:** IoT provides data to its users when necessary. The availability of data allows the authorized person to have immediate access to information sources, not only under normal circumstances but also in catastrophic conditions [8], [41]. Implementing a firewall prevents denial of service (DoS) attacks and denies the availability of end user data. Backups and backup methods provide various system failovers to ensure system component replication in the event of a system failure or to ensure data reliability and availability [8].

Table 1: Summary of Surveys on Security of Internet of Things

Security Concerns	[8]	[2]	[11]	[39]	[9]	[10]	[1]
Identification	√	√	√	×	×	√	×
Authentication	√	×	√	×	×	√	√
Data Integrity	√	×	√	×	×	√	√
Trust	√	×	√	√	√	√	×
Data Confidentiality	×	×	√	×	√	√	√
Access Control	×	×	√	√	×	×	×
Data Privacy	√	√	√	√	√	√	√
Data Availability	√	×	×	×	×	×	×

Legend: √ Covers the security concern. × Does not cover the security concern

4.1.2 IoT Security Requirements

The IoT security requirements of researchers and security experts present a dilemma as authentication and trust directly conflict with confidentiality standards [42]. According to [1], the security requirements are best addressed using a generic IoT architecture at four key levels of *perception*, *network*, *middle-ware* and *application*. In this architecture security issues are identified as authentication, data privacy, routing security, data security, intrusion prevention, risk assessment, authentication and privacy of sensitive information. However, trust and identity management are lacking in the requirements. IoT security requirements such as integrity, information protection, confidentiality, disclaimer, freshness, authentication, authorization, access control, exception management, accessibility, fault tolerance and personal organization are highlighted in [43].

Babar et al., [43 claim that the most important security requirements include authentication and monitoring, data and information integrity, mutual trust and confidentiality]. IoT devices are mobile and often connect to the Internet through various wireless channels, such as Bluetooth, 802.11, WiMAX, Zigbee, GSM / UMTS. Using such a wireless connection, an attacker can block unique low-level identifiers such as Bluetooth and 802.11 device addresses [44].

Amine et al., [45] provide an overview of the authentication protocols used in the IoT context, including Machine Communication (M2M), Vehicle Internet of Things (IoV), Energy Internet of Things (IoE), and Internet Sensors (including IoS). Their research presented authentication protocols that did not solve authentication and privacy issues, but suggested the complexity and overhead of communication by using recommended methods or improving formal methods of security testing.

We note that human user security requirements have not been addressed in IoT security surveys thereby making the surveys incomplete. To provide a complete overview, we consolidate these IoT security requirements and divide them into four groups, namely: *network security*, *identity management*, *privacy*, and *trust*. Obviously, in terms of network security, constrained resources should have the strongest connection, mainly due to restrictions that apply to traditional security mechanisms, for example, encryption. Moreover, identity management is affected by the heterogeneity of the Internet of Things. Privacy is primarily related to scalability and limited resources as restrictions are placed on technology that can be used. Additionally, the uncensored environment and the heterogeneity of the Internet of Things have a serious impact on trust [40].

a) *Network Security*: Network security requirements are divided into confidentiality, authenticity, integrity, and availability. Interconnecting the devices require better confidentiality which could be accorded through IPSec and Transport Layer Security (TLS) [46]. Authenticity confirms that the connection established is with an authenticated entity and authenticity also includes integrity of data but can be required separately to detect and recover failures so mechanisms such as TCP and TLS suffice this requirement. Availability ensures that IoT service is available in case overhead exceeds the resource constraints of things. It also ensures the survivability of IoT services to authorized parties when needed despite denial-of-service attacks. It also ensures that it has the capability to provide a minimum level of services in the event of disruptions [43].

b) *Privacy*: Privacy is considered to be one of main challenges in IoT [47] due to the involvement of humans and increasingly ubiquitous data collection. Privacy of data includes transmitting and sharing of confidential information without exposing the user's identity. This requirement is considered as big challenge as almost every other sensing device collect personal information and large amount of such data becomes Personally Identifiable Information (PII) when combined together; enough to identify a person [47]–[49]

c) *Identity Management*: A comprehensive attention should be given for identity management in IoT due to the number of devices and the complex relationship between devices, services, owners and users [47], [50], [51]. Methods for authentication, authorization including revocation, and accountability or non-repudiation are required. There may be multiple domain scenarios in IoT, authorization solutions, e.g., Kerberos [44], [52], [53] assume a single domain that encloses devices, owners, users, and services. Therefore, new authorization solutions that work with untrusted devices, allow delegation of access across domains, and capable of quick revocation are needed.

d) *Trust Management*: Accountability in trust management ensures that every action is clearly bound to an authenticated entity. It must be capable to deal with huge amounts of entities, delegation of

access, actions that span organizational domains along with continuous derivation of data [10]. Trust management should act as self-organizing component in order to deal with the information flow and preventing the privacy information from leaking to untrusted devices. The authors in [54] make use of fuzzy set theory and formal semantics-based language to perform the layered trust mechanism, evaluated by using specific layer attributes (i.e., efficiency, risk, history). The user has access to the IoT only if security credential satisfies security policies, which are defined by means of a decision-making function according to user trust value.

From the surveyed literature, user IoT security requirements are partially covered under privacy, identity management and trust management. This is quite limiting considering that human users interact with the smart devices all the time. Confidentiality, integrity, authenticity and availability covered under network security with a bias toward device security, are equally important for user security and should have been discussed and analyzed. while users who are directly affected have not been considered

4.1.3 IoT Security Challenges

Although a number of studies have been conducted as shown in the literature to protect IoT applications, still there is a big security hole in IoT environment. IoT security issues and challenges have been analyzed in [1], [11], [60], [35], [43], [50], [55]–[59]. To successfully implement and deploy smart devices, trust in IoT must be assured. This therefore requires that the ecosystem employs a collaborative and unified approach to IoT security. This is subject to serious security challenges facing the ubiquity of this technology. A number of researchers have explored ways of making IoT safe for users. Nitti et al [34] conducted a study on the acceptance of IoT objects by users. 43% of users queried say they are afraid of the use that can be made of their personal data. 18 % find that the connected objects are not operational. 8% believe they are unreliable. Falcone and Sapienza [61] proposed a model for the users' acceptance of IoT systems. The proposed model uses the concepts of trust and control as a starting point, with particular reference to the feedback. The authors were able to precisely classify the tasks an IoT device can do according to the autonomy the user grants. They further provided a theoretical framework for the device–user relationship, formalizing their interaction. It is in fact a complex interaction: on the one hand, the device must adapt to the user, on the other hand, it must ensure that the user adapts to it. The realized model perfectly responds to these needs.

From the foregoing, this section therefore identifies a number of IoT security challenges, as defined by other researchers, which can be considered as open issues for future research directions. A summary of the related works found in literature is shown in Table 2.

Table 2: Identified IoT Security Challenges

Area	Challenges	References
Interoperability	Relevant security solutions should not interfere with the operation of many interconnected devices in the IoT network system.	[16].
Resource constraints	In IoT architecture, most nodes do not have storage capacity, power, and processor. They have a low speed connection. Therefore, it is impossible to use security methods such as frequency shutdown connection and public key cryptographic algorithms. It is very difficult to install a security system in such	[62]

	conditions	
Data volumes	Some IoT programs use short and sparse communication channels, but many IoTs, such as intuition, logistics, and large systems, require large amounts of data on a central network or server.	[63], [52]
Privacy Protection	Many RFID systems do not have an appropriate authentication mechanism, so anyone can control the labels and find the identifier of the items they are carrying. An attacker not only reads the data, but can edit or delete it.	[1].
Scalability	The IoT network consists of several nodes. The security mechanisms proposed in the IoT need to be expanded.	[64], [65].
Autonomic Control	Traditional computers require users to configure and modify different program areas and different communication environments. However, objects in the IoT network must configure and create the platform on which they work. This type of management includes methods and mechanisms such as self-organization, self-management, self-treatment, and self-defense.	[16].
Trust Management	The absence of central administration for IoT infrastructure makes trust management quite challenging.	[10], [54], [66]
Access Control	Access control is essential specially for IoT devices which may be located on open areas and physically under control of opponents. Contract management plays a centralized role for IoT systems in the future generations. Delegation of authority to IoT devices has to be considered by an access model to enable usability and flexibility of IoT systems.	[53], [67]–[71]
Intrusion Detection and Prevention	It includes abnormal network traffic monitoring. Adoption of intrusion detection and prevention is a challenge to avoid IoT botnet and DDoS attacks.	[12], [72], [73]

The works studied show that resource constraints play a critical role in the adoption of IoT. This is because it determines the slow speed and processing power affects the deployment of strong encryption solutions. Further, privacy protection through appropriate authentication mechanisms and trust management issues are considered critical. Users are apprehensive about devices that expose their data to unauthorized persons.

4.1.4 IoT Security Threats

Several studies have been conducted in the field of IoT primarily in the area of IoT security threats. However, there are still some open issues that need to be addressed. In this section we discuss some of the threats in each architectural layer that needs special attention as shown in Table 3 [35], [37], [41], [62], [74]–[76]. The identified threats at each layer are presented from the highest (High) to the lowest (Low). The threats at the perception layer are classified with the highest security risk level due to very

large hardware limitations that prevent the implementation of robust protection methods of the data collected, stored and transmitted. The risk level is also contributed by the heterogeneity of the devices within the perception layer which makes the establishment of security and the standardization of communication protocols more difficult [35]. At the network layer, threats are classified with risk levels ranging from Low-to-Medium due to the known disadvantages of wireless data transfer standards, as well as known threats in access networks [77], [81] . The threats at the application layer are classified with the Medium security risk level [82], [83]. This is because of the large number of users and the data to be stored and processed within the layer, as well as the known vulnerabilities of virtualization whose exploitation can cause extensive simultaneous damage to a large number of users.

Table 3: Threats and Security Concerns at each Layer of IoT

Layer	Threats and Security Challenges	Threat Level	References
Perception	**Eavesdropping**. Within the RFID technology, an attacker could easily sniff out the confidential information like passwords or any other data flowing from tag-to-reader or reader-to-tag which makes it vulnerable [84].	High	[1], [2], [35], [52], [78], [84]–[87]
	Spoofing. Spoofing is when an attacker broadcasts fake information to the RFID systems and makes it assume the information is from the original source [1], [35], [85]. This way attacker gets full access to the system making it vulnerable	High	
	RF Jamming. RFID tags can also be compromised by kind of a DoS attack in which communication through RF signals is disrupted with an excess of noise signals[52].	Medium	
Network	**Sybil Attack**. Sybil is a kind of attack in which the attacker manipulates the node to present multiple identities for a single node due to which a considerable part of the system can be compromised resulting in false information about the redundancy[77].	Medium	[1],[18], [77], [81]
	Sinkhole Attack. It is a kind of attack in which the adversary makes the compromised node look attractive to the nearby nodes due to which all the data flow from any particular node is diverted toward the compromised node resulting in packets drop i.e. all the traffic is silenced while the system is fooled to believe that the data has been received on the other side. Moreover this attack results in more energy consumption which can cause DoS attack [1].	Medium	
	Man-in-the-Middle Attack. This is a form of Eavesdropping in which target of the attack is the communication channel due to which the unauthorized		

	party can monitor or control all the private communications between the two parties hideously. The unauthorized party can even fake the identity of the victim and communicate normally to gain more information [1]. **Denial of Service (DoS) Attack**. The kind of attack in which the network is flooded with a useless lot of traffic by an attacker, resulting in a resource exhaustion of the targeted system due to which the network becomes unavailable to the users [1], [82], [88]. **Malicious code Injection**. This is a serious kind of attack in which an attacker compromises a node to inject malicious code into the system which could even result in a complete shutdown of the network or in the worst case, the attacker can get a full control of the network [1].	High High High	
Application	**Sniffing Attack**. An attacker can force an attack on the system by introducing a sniffer application into the system, which could gain network information resulting in corruption of the system [1] **Malicious Code Injection**. An attacker can leverage the attack on the system from end-user with some hacking techniques that allows the attacker to inject any kind of malicious code into the system to steal some kind of data from the user. **Denial-of-Service (DoS) Attack**. DoS attacks nowadays have become sophisticated, it offers a smoke screen to carry out attacks to breach the defensive system and hence data privacy of the user, while deceiving the victim into believing that the actual attack is happening somewhere else. This put the non-encrypted personal details of the user at the hands of the hacker **Spear-Phishing Attack**. It is an email spoofing attack in which victim, a high ranking person, is lured into opening the email through which the adversary gains access to the credentials of that victim and then by a pretense retrieves more sensitive information.	Medium High High Low	[1],[74], [82], [83]

From the literature, it is obvious that threats permeate every layer of the IoT architectural model. Of the threats mentioned, malicious code injection and denial-of-service attacks which have high threat levels are found in both application and network layers, respectively. Threats such as RF jamming, Sybil attack, sinkhole attack and sniffing attack have medium impact while spear phishing is considered to

have low impact. These threats could expose the vulnerabilities within the IoT systems and devices leading to successful attack on IoT assets. No layer is immune from threats. This means that safeguards to protect IoT must be adequately addressed across the architectural layer. At the application layer, the user is constantly under threat of malicious code injection, denial-of-service and spear-phishing attacks. While malicious code could be initiated from the user-end, denial-of-service targets the user data privacy. Spear-phishing on the other hand is used to lure unsuspecting user through email to allow access to user credentials.

4.1.5 IOT Attack Surface

Many Internet-connected smart devices do not have the proper level of security due to privacy protection and data access differences. Thus, the IoT attack zone represents all possible vulnerabilities in IoT devices and related programs and infrastructures in a particular network.

Assigning an IP address to a smart device connected to the Internet provides the function of transmitting network data. Deficiencies in these devices provide a platform through which hackers and government agencies can access the network, monitor users, and access other connected devices for a variety of purposes. The OWASP project has compiled a list of attack zones and their vulnerabilities in the IoT environment. This is shown in Table 4 below [89] [90].

Table 4: The OWASP IoT Attack Surface Areas [89][90]

Attack Surface	**Vulnerability**
Ecosystem Access Control	Authentication; Session management; Trust between components; Enrollment security; Cancellation system; Lost access procedures
Device Memory	Cleartext usernames; Cleartext passwords; Third-party credentials; Encryption keys
Device Physical Interfaces	Firmware extraction; User CLI; Admin CLI; Privilege escalation; Reset to insecure state; Removal of storage media
Device Web Interface	SQL injection; Cross-site scripting; Cross-site Request Forgery; Username enumeration; Weak passwords; Account lockout; Known default credentials
Device Firmware	Hardcoded credentials; Sensitive information disclosure; Sensitive URL disclosure; Encryption keys; Firmware version display and/or last update date
Device Network Services	Information disclosure; User CLI; Administrative CLI; Injection; Denial of Service; Unencrypted Services; Poorly implemented encryption; Test/Development Services; Buffer Overflow; UPnP; Vulnerable UDP Services; DoS
Administrative Interface	SQL injection; Cross-site scripting; Cross-site Request Forgery; Username enumeration; Weak passwords; Account lockout; Known default credentials; Security/encryption options; Logging options; Two-factor authentication; Inability to wipe device
Local Data Storage	Unencrypted data; Data encrypted with discovered keys; Lack of data

	integrity checks
Cloud Web Interface	SQL injection; Cross-site scripting; Cross-site Request Forgery; Username enumeration; Weak passwords; Account lockout; Known default credentials; Transport encryption; Insecure password recovery mechanism; Two-factor authentication
Third-party Backend APIs	Unencrypted PII sent; Encrypted PII sent; Device information leaked; Location leaked
Update Mechanism	Implicitly trusted by device or cloud; Username enumeration; Account lockout; Known default credentials; Weak passwords; Insecure data storage; Transport encryption; Insecure password recovery mechanism; Two-factor authentication
Vendor Backend APIs	Inherent trust of cloud or mobile application; Weak authentication; Weak access controls; Injection attacks
Ecosystem Communication	Health checks; Heartbeats; Ecosystem commands; Deprovisioning; Pushing updates
Network Traffic	LAN; LAN to Internet; Short range; Non-standard

From Table 4, an analysis of IoT attack surface areas and attendant vulnerabilities indicate that all of the major components of IoT systems can be exploited. Security should therefore be a priority in building and maintaining IoT systems. Regardless of the scale or the type of environment an IoT system is built into, security should be considered from the design phase to better integrate it in every aspect of the system. In this way, the IoT system, from its individual devices to its overall configuration, can be tailored to be both functional and secure. The discussed attack surface has critical vulnerabilities that users ought to be aware of in order to make the right choices when procuring smart devices. The users cannot be expected to perform positive actions to make up for security flaws.

4.2 IoT Privacy

IoT devices collect, analyse and transmit sensitive data across the network. This data requires adequate protection from adversaries while the user should be aware of what private data is being processed.

4.2.1 Privacy Definition

Privacy protection is very broad and multifaceted, from which literature review provides a variety of explanations and perspectives [41]. Privacy in the Internet of Things is the border where information from smart objects is exposed to the outside world. Therefore, privacy is threefold guarantee to the subject for [1], [23], [41], [76], [91]:

- Recognizing the risk of confidentiality imposed by data objects and services around a data object
- Individual management of personal data collection and processing in smart facilities

- Recognizing and managing the use and dissemination of personal information by individuals outside of personal management.

Regardless of the definition adopted, threats to privacy are generally one of the main concerns of users and can significantly affect the level of adoption of new technologies. Smart gadgets offer incredible value creation and capture opportunities, but their vulnerabilities might cause catastrophic disruptions, ranging from privacy breaches to breakdowns of public ecosystems.

4.2.2 Privacy Principles

To solve some of the problems that users of IoT products face, it is advisable to give the creators of the smart device a concept of privacy by design[92]. Ann Cavoukian [92] posited that privacy-by-design must be underpinned by the following seven principles presented in Table 5:

Table 5: Privacy Principles

Principle	**Explanation**
Proactive not reactive, preventative not remedial	It is designed to prevent the intrusion of privacy. We recognize the importance and benefits of routine early and consistent adoption of a strong personal life. This includes clear commitments at the highest level; privacy commitments clearly shared between the user community and stakeholders, and established means of recognizing poor privacy designs.
Privacy as the default setting	User does not need to take steps to protect your privacy. It will be notified by the following fair information practices: • Desired specifications • Limit collection • Restrictions on use, retention, and disclosure
Privacy is included in the design	It is an integral component of the basic functionality of the computer system, not an additional component which is then bolted to the system. This includes integration into information technology, operations, and architecture in a holistic, integrated, and creative way.
Full functionality – positive-sum, not zero-sum	It avoids compromises between different objectives and seeks to achieve all desired objectives (such as confidentiality and functionality) with a win-win approach.
End-to-end security – full lifecycle protection	It is integrated with IT systems before the first data record is collected and throughout the life of the data, ensuring that information is stored, processed, and destroyed securely at the end of the process.
Visibility and transparency – keep it open	It assures all stakeholders that information is managed in accordance with stated commitments and objectives and that its components are visibly transparent.
Respect for user privacy – keep it	It avoids compromises between different objectives and seeks

user-centric	to achieve all the desired (and apparently contradictory) objectives (such as confidentiality and functionality) with a win-win approach.

Cavoukian [92] takes a rather generalized concept of privacy by design and the approach lacks clear implementation strategies as part of the system design. This paper introduces the following additional principles postulated by Hustinx [93]to bridge the gap identified while evaluating the seven principles enumerated by [92].

1) *Data minimization*: Proactively prevent privacy risks by systematically minimizing the amount of data collected and processed. Therefore, software, information and communications technology and systems development should start by default with unidentified interactions and processes. Where possible, consistent identifiable and observable personal information should be kept to a minimum.
2) *Informed consent*: The terms are presented in a clear, relevant and transparent manner. This allows users to choose not to share certain information, except to the extent permitted by law. The confidentiality of the data determines the quality of the consent required.
3) *Transparency*: Provide users with an overview of how data is processed and used.
4) *Verifiable preventive protection*: Prevent threats with security measures that can be validated.
5) *Accuracy*: Keep accurate, complete and up-to-date personal information necessary to achieve the specified objectives.
6) *Possibility to withdraw consent*: Easily revoke user consent and give them the ability to delete shared information.

These principles may not ensure the inviolability of users 'personal lives, as the human-machine interface must be person-centered, and user-friendly in order to make personal decisions based on personal information. However, failure to apply and enforce privacy-by-design principles exposes the IoT environment to a wide range of privacy and security threats such as eavesdropping, spoofing, Sybil attack, man-in-the-middle attack, denial-of-service attack, profiling, inventory attacks and lifecycle transitions.

4.2.3 Privacy Threats

With the development of IoT and the diffusion of technology, confidentiality has become a major problem. The collection, use, and exchange of user data is common and continues in the Internet of Things environment. The review presented in [47]identifies the most common threats to Internet of Things privacy.

a) *Identification* is a major threat that associates identifiers such as names and addresses with individuals. Basically, we have experience in the back-end services of the reference model in the IT phase, with a large amount of information concentrated in a central location beyond the control of the subject. However, in IoT, the stages of interaction and data collection are also important, as the impact of emerging technologies and the nature of interactions and interactions increase the threat of identification.

b) *Location and tracking* are dangerous for the location of people using various tools such as GPS, Internet traffic, location of smartphone, etc. Privacy breaches have been identified, such as GPS tracking, disclosure of personal information such as illness or discomfort in monitoring or control.

c) *Profiling* is used to personalize electronic commerce (such as newsletters and advertisements). Organizations collect information of interest by communicating with other profiles and data sources. As IoT evolves, data sources explode every day. In addition, although data collection increases quantitatively, the data changes qualitatively due to the collection of previously inaccessible parts of an individual's personal life.

d) *Interactions and presentations* convey the number of smart items and new ways of communicating with the system and feedback to users. This threatens confidentiality, personal information between the system and the customer.

e) *Life cycle transitions* occur when IoT products are sold, used by their owners, and eventually destroyed. It has been established that objects destroy all data, but smart devices often store large amounts of historical data over their lifetime. This includes personal photos and videos that are not deleted during the transfer of ownership.

f) *Inventory attacks* are used to gather information about unauthorized use and access to personal items and features. Thieves can use inventory data to find safe time to identify and destroy property.

g) *Linking connections* between different systems increases the chances of unauthorized access and intrusion of personal data when systems are connected to individual data sources [23], [94].

The above identified threats confound users of IoT technology especially when users know that the devices collect and transmit personal data without their knowledge. Proper mitigation of the privacy threats would ultimately encourage users to adopt IoT technology.

4.2.4 Privacy Challenges

The evolving features and technologies of the IoT along with the emerging systems of the IoT interaction have led to specific privacy challenges. For the various threats identified by [47], a number of challenges were identified, discussed and classified as shown in Table 6.

Table 6: Privacy Challenges

Privacy Threat	***Threat Level***	***Challenge***
Identification	Medium	The design of the IoT system allows for centralized communication processing and horizontal communication. This reduces the identity data available outside the user's personal area and reduces the attack vector for identification. The challenge is related to associating the identity to a particular context that violates the individual's privacy by providing the identifying information to entities outside the user's personal sphere, increasing the possible cyberattack vectors[95].
Localization and tracking	Medium	The threat is related to the determination and recording of the individual's location across space and time

Privacy Threat	*Threat Level*	*Challenge*
		While localization and tracking are already possible through various means such as internet traffic and mobile phone GPs location, many users may perceive it as a violation of privacy if the data is used inappropriately or if they do not have any control of the sharing of their location data [95]. As such, the IoT faces a challenge in ensuring awareness of tracking and control of the localization data.
Profiling	High	There is a risk in the compilation of data about users so as to determine their interests through correlation with other sources of data and profiles [88]. Profiling could lead to privacy violations if the data is used for unsolicited ads, price discrimination, and social engineering. The challenge is in balancing the interests of the user with the requirements of the user's privacy when creating and analyzing data profiles. Gathering and sale of user profiles in the data marketplace without the individual's consent is also considered as a privacy violation[88].
Privacy-violating interaction and presentation	Medium	Majority of the mechanisms used to interact with the user and present feedback information are inherently public in nature, posing a threat to the individual's privacy in case other people can observe the data [39]. Thus, the IoT must solve the challenge posed by the easy visibility of personal user data.
Lifecycle transitions	Medium	The users' private information collected during the IoT device's lifetime may be disclosed during changes to the gadget's control spheres during their lifecycle [96]. The smart devices interact with numerous services and persons and amass the data on such interactions in their history logs. Considering that the lifecycle of most consumer goods is based on the customer owning the products forever, the sale or sharing of such devices could result in the buyer accessing sensitive data about the previous owner, thus violating the individual's privacy.
Inventory attack	Low	As the IoT interconnection capacities evolve with the development of end-to-end vision, the smart devices can be queried over the internet by both legitimate and non-legitimate parties. When the IoT gadgets are queried by the non-legitimate entities, the latter may exploit the device to collect unauthorized information regarding the characteristics and existence of the user's personal effects [59]. Thus, the IoT can allow for the disclosure of comprehensive data about the users' life and belongings, posing a threat to their privacy. A mechanism that provides tolerance to fingerprints is necessary to prevent passive inventory attacks based on fingerprints from something intelligent. It will certainly be difficult to resist

Privacy Threat	*Threat Level*	*Challenge*
		inventory attacks. Although PET was designed to protect privacy, the fact that it can make fingerprints even easier is currently not the most appropriate, but most appropriate, solution among the masses [93].
Linkage	Low	First, the transparency of the information that the system share is important for user approval. Second, adjusting the authorization and use management model is required for many stakeholders working in the respective system. Third, the data anonymization method should work for each system and be reliable for multiple combinations of different data sets [23], [94].

The seven privacy threats are classified based on threat levels from low to high. Privacy remains a major challenge on IoT that should be addressed if the technology is to gain acceptance from users. Among the privacy threats whose challenges have been enumerated, it is profiling that remains one of the most severe threats with a rating of high. Our analysis shows that it is greatly aggravated and that other threats like identification or tracking, though each provoking different and very specific privacy violations at medium level, add to its dangers by supplying even more linkable data. It is worth noting that business models that depend heavily on profiling have enjoyed tremendous success and so the trend for big data continues, fueled by the IoT's central promise for fine-grained and ubiquitous data collection. Here, the challenge consists in designing privacy-aware solutions for the IoT that allow balancing business interests and customers' privacy requirements. Privacy threats such as interaction and presentation, and lifecycle transactions are rated medium as they too have an effect on user profiling. Linkage and inventory attacks have low threat rating.

4.2.5 IoT Vulnerabilities

Vulnerabilities are flaws in systems or projects that allow illegal users to give instructions, access unauthorized data or perform denial of service attacks [97]. Vulnerabilities are present in various areas of the IoT system. This can be in hardware or software, system weaknesses and policies used by the system or users of the system itself [98].

Neshenko et al., [12] proposed nine IoT vulnerability classes. These classes include deficient physical security, insufficient energy harvesting, inadequate authentication, improper encryption, unnecessary open ports, insufficient access control, improper patch management capabilities, weak programming practices and insufficient audit mechanisms. However, the authors concluded that most IoT attacks are possible because of two main vulnerabilities in IoT, that is, unnecessarily open ports, and weak programming practices coupled with improper software update capabilities. They further point out that insufficient IoT access controls and audit mechanisms enable attackers to generate IoT-centric malicious activities in a highly stealthy manner.

Granjal et al., [99] performed exhaustive analysis on the security protocols and mechanisms available to protect communications on the IoT networks. They focused on vulnerabilities and attacks targeting the IoT networks. They also highlighted on ongoing work aimed at securing those protocols. The authors

identified some security challenges at each of the layers. At the physical layer, protocols (e.g., IEEE 802.15.4) do not specify a key model (i.e., a model for generating, distributing, storing, and replacing cryptographic keys), because it depends largely on the resources available on the IoT devices to support key management operations. At the network layer, routing protocols (e.g., Routing Protocol for Low-Power and Lossy Networks or RPL) offer security against external attacks only, and are not resilient against internal attacks. And finally, at the application layer, protocols (e.g., Constrained Application Protocol or CoAP) lack appropriate key management mechanisms for multicast communication.

Celik et al., [58] studied privacy and security issues related to IoT program analysis. They analyzed a number of systems for five major IoT programming platforms (Samsung's SmartThings, OpenHAB, Apple's HomeKit, Google's Android Things, and Amazon AWS IoT). The authors concluded that: (1) the dominant IoT programming platforms structure their apps around a sensor-computation-actuator idiom; (2) a suite of analysis tools and algorithms targeted at diverse IoT platforms is at this time largely absent; (3) because IoT applications control physical processes through devices, security and privacy issues are more subtle and difficult to identify than in related fields; (4) most approaches lack multiple analysis sensitivities such as path- and context-sensitivity; (5) most approaches often do not consider security and safety problems in multi-app environments and through information flows in trigger-action platforms; (6) members of the research community often use the SmartThings platform to evaluate their tools, as numerous open-source official and third-party apps are available; and (7) IoT systems often implement algorithms on the Abstract Syntax Tree (AST) of a SmartThings app because of the constraints on Groovy language and proprietary back-end libraries.

In 2018, The Open Web Application Security Project (OWASP) updated its top ten IoT vulnerabilities [100]. The list includes: a) weak, guessable, or hardcoded passwords; b) insecure network services; c) insecure ecosystem interfaces; d) lack of secure update mechanism; e) use of insecure or outdated components; f) insufficient privacy protection; g) insecure data transfer and storage; h) lack of device management; i) insecure default settings; and j) lack of physical hardening.

The OWASP project is intended to encourage and assist manufacturers to build their devices with security in mind and therefore make their devices secure by design. Its goal is to help organizations and individuals gauge the acceptable risk and take appropriate actions to mitigate them.

The OWASP top 10 IoT list of vulnerabilities does not come with separate guidelines for various stakeholders but instead takes a unified approach to address IoT vulnerabilities that might be affecting IoT devices. The OWASP IoT top 10 project team avoided specific IoT security vulnerability guidelines.

For this study, we consider and discuss the following key vulnerabilities which pose the highest security threat to IoT ecosystem:

a) Weak credentials and lack of strong authentication mechanisms

In 2010, Cui et al. [101] conducted Internet-scale probing and uncovered more than half a million embedded devices with default credentials. Most of these devices belonged to government organizations, large enterprises, Internet Service Providers (ISPs), and educational institutions. Two years later, in 2012, the Carna botnet revealed that there were more than 1.2 million devices online with no or default credentials [102].

b) Open Ports

A major concern to the security of IoT networks is the significant number of devices with unnecessarily open ports. Czyz et al. [103] showed that a large number of IoT devices are only reachable over IPv6, and various IoT protocols are more accessible over IPv6 than over IPv4 (e.g., 6LoWPAN). They discovered that a given IPv6 port is almost always more open than the same port is in IPv4. For example, IPv6 had 5% more open SSH ports, and 46% more open Telnet ports as compared to IPv4. They also concluded that there was a systemic failure in organizations to deploy consistent security policies for their devices as it pertains to port blocking. Lastly, the authors debunked the belief that the security threat of open ports in IPv6 is dampened due to the infeasibility of IPv6 network-wide scanning by discovering high-value hosts through scanning alone.

c) Weak programming practices

Although strong programming practices and injecting security components might increase the resiliency of the IoT, many researchers have reported that countless firmware are released with known vulnerabilities such as backdoors, root users as prime access points, and the lack of Secure Socket Layer (SSL) usage. Hence, an adversary might easily exploit known security weaknesses to cause buffer overflows, information modifications, or gain unauthorized access to the device[104][105][106].

d) Data Leakage

IoT applications are also prone to data leakage vulnerabilities. Celik et al. [107] conducted static taint analysis on 230 SmartThings applications, and found that 138 of the applications exposed at least one piece of sensitive data via the Internet or messaging services. Furthermore, the authors showed that half of the analyzed applications leak at least three different sensitive data sources, such as device info, devices state, user input, etc., to the Internet or messaging services.

e) Improper encryption

While it is clear that encryption can help to address some of the vulnerabilities presented in [108], complex cryptographic functions, such as those found in the Advanced Encryption Standard (AES), can result in large overhead for resource-constrained IoT devices. As a result, there is a growing interest in ultra-lightweight, but secure encryption algorithms optimized for low-powered hardware. However, as Singh et al. [109] pointed out, hardware-based encryption engines have a significant vulnerability: the power dissipation of the hardware can be measured while performing encryption, and later statistically analyzed to recover the secret key, thus compromising the device. Many countermeasures have been proposed to address this vulnerability in AES engines. Unfortunately, these countermeasures incur significant power and performance overheads, and therefore are not suitable for lightweight cryptographic primitives.

The reviewed literature has uncovered some inadequacies that this paper addresses. For instance, this paper addressed the entire spectrum of the listed IoT security concerns (identification, authentication, data integrity, trust, data confidentiality, access control, data privacy and data availability) unlike the existing papers. It is only Riahi et al., that covered seven out of eight security concerns leaving out data availability. Second, this paper comprehensively covered the IoT security requirements whereas the existing papers partially covered this under privacy, identity management and trust management. Third, we examined the vulnerabilities in IoT, but found out that most of the existing papers focused on just a

few specific areas such as hardware or software, system weaknesses and policies used by the system or users of the system itself. This was also not as comprehensive as has been articulated in this paper. Fourth, compared to existing works, this paper brings out the integration of privacy and security through the proposed threat taxonomy that is presented in Section 6.

5. Countermeasures

In this section, we describe countermeasures necessary to mitigate the IoT vulnerabilities, threats and attacks identified in section 3.

Bringing users into the fold requires designers and developers to understand that users hold the potential to be capable and informed about the elements of a system. Considering users and the various interactions they have with the system can allow designers to have a more well-rounded approach to understanding and ensuring IoT security [110]. To highlight the role users can play in protecting their privacy and minimizing their risk, we discuss steps that can be taken long before a cyberattack actually happens and what can be done when a hacking attempt occurs.

Working toward ensuring users' privacy and security should begin by considering what users are like before they begin to use an IoT device. Designers and developers should evaluate, among other factors, how users think about their safety, their motivation to be proactive in securing their information, and the trust they have in interconnected devices, as these factors will affect how users interact with their devices. For instance, the average user lacks an adequate understanding of the number and type of Internet-related risks to which he or she might be exposing him or herself [26] and the role he or she can play in securing his or her information [111]. This situation can be improved; an increased awareness of privacy threats and risks is correlated with the number of protective actions users report having taken [48]. We present below the countermeasures that include access and authentication controls, security protocols, intrusion detection, single sign-on, establishing trust, security awareness, privacy by design, and security tools:

5.1 Access and Authentication Controls

Access and authorization mechanisms are critical for the adoption of IoT technology. Therefore, systems access to authorized requests must be taken into account when developing IoT systems [112]. Authorizations techniques must verify if two objects participated in communication have been validated. The most common authentication techniques are a role-based access control (RBAC) and an attribute-based access control (ABAC). ABAC converts privileges to a set of attributes assigned to an object, whereas RBAC converts privileges to a set of roles assigned to an object. Another technique which can be used to ensure authorization for IoT objects is known as Authentication and Authorization for Constrained Environments (ACE) [113].

Martı´nez et al., [114] proposed SMARTIE, an integrating user-centric platform for efficient but secure dissemination of IoT data in smart cities. The authors' provided insights into the application of the IoT-ARM to generate this platform. The main goal of this platform is to empower users to take control of their access control and privacy preferences to govern devices. The SMARTIE that is based on the IoT-ARM guidelines on security and scalability provides architectural artifacts that enable easily and efficiently enforcing user access control policies. The proposed integrative approach is intended to give a user-managed, flexible, and scalable mechanism for access control to protect the access to smart meters' data through the use of the SMARTIE platform. In addition to manage information, the main

goal of this platform is to empower users with full control on their devices through a policy-based approach.

He et al., [53] in their study of access control and authentication in the home IoT noted that the current authentication methods for the home IoT appear transplanted from smartphone and desktop paradigms, which for the most part, assume a single-user-per-device environment. Through their online user study, they found major differences in the participants' desired access-control policies for different capabilities within a single device (e.g., updating software, turning lights on/off, turning cameras on/off, adding new user, etc.), as well as based on who is trying to use that capability (e.g., spouse, teenager, child, visiting family, babysitter, neighbor, etc.). they were able to pinpoint various contextual factors (e.g., time of day, location of user, location of device, who is nearby, etc.) that, along with capabilities and relationships, dictate the specification of more complex, yet desired, access-control policies.

Zeng & Roesner [115] used the access-control policies derived from [53], among other design principles from other studies, to create an access control system for the smart home. The application included four types of access controls:

- *Role-Based Access Control*: Each user is assigned a role — admin, child, or guest. Only admins are allowed to change access control policies, add new users, and organize the devices.
- *Location-Based Access* Control: Users can be restricted from using devices if they are not physically near the device.
- *Supervisory Access Control*: Allows a user who may be restricted from using a device, to use the device, if and only if another (authorized) user is nearby.
- *Reactive Access Control*: If a user attempts to use a device they do not have permission to use, the application will ask a more privileged user for permission in real-time, by sending a notification asking them to approve or deny the request.

For their work, the authors emphasized that the design of security and privacy features for a smart home must not limit a user's primary use case for the smart home. To them, the user's right to use the services is paramount.

Yang et al., [116] proposed RFID-based solutions to address specific IoT security issues such as device authentication, device privacy, and network integration. The possibility of a device being stolen, lost or damaged made the prospect of attaching an RFID tag to an IoT device chip desirable. Their solution comprises a unique set of tags and device identifier, a session key, and a power path. It is designed to ensure a safe and secure delivery platform. Meanwhile, Fernandes et al., [117] proposed a method of restricting access to IoT sensitive data. The authors have created a system called FlowFence that allows programs to control the use of data. The researchers achieved this by accessing sensitive data by blocking the flow of data identified by the user. The proposed solution allows programmers to divide the program into two modules. The first module manages sensitive IoT data in a test environment, while the second uses integrity constraints to coordinate the transmission of such sensitive data. An overview of FlowFence by IoT users has shown that data storage is minimized with limited growth.

Le & Mutka [67] proposed a lightweight authorization protocol that allows a user to easily transfer his/her access rights to smart home devices as a means of tackling the problem of delegating permissions. The protocol works by transferring access rights to a device in the form of a Bloom filter with the help of secured hashing to prevent the permission from being forged. The Bloom filters

prevents items from being removed and therefore, a user cannot recreate a permission higher than what he/she is holding but can still transfer lower permissions to other users.

Recent studies have focused on authentication mechanisms that mostly deal with biometric factors. For example, many papers [118]–[122] developed unique touch-based authentication mechanisms for wearable or smart home devices. Alternatively, [123] presented a continuous authentication system based on geometric and non-volitional features of cardiac motion.

Feng et al., [124] presented VAuth, the only system that we found that provides continuous authentication mechanism for voice assistants. VAuth collects the body-surface vibrations of a user and matches it with the speech signal received by the voice assistant's microphone. VAuth can fit inside things that people normally wear, such as eyeglasses, earbuds, and necklaces, Such a system can guarantee that the voice assistant only executes the commands that originate from the voices of authorized users. The authors evaluated the system on 18 users and 30 voice commands, and achieved a detection accuracy of 97% with less than 0.1% false positives, regardless of VAuth's position on the user's body, the user's language, the user's accent, or the user's mobility.

5.2 Security Protocols

A security protocol to support data exchange amongst objects was proposed by [125] and combined with a security framework for enhancing security, trust, and privacy for embedded systems. Lightweight symmetric encryption and asymmetric encryption in Trivial File Transfer Protocol (TFTP) were proposed to make the given protocol appropriate to the constrained nature of IoT devices. In [126], the authors propose mechanisms to ensure security at the network layer and at the application layer and perform an experimental study to identify the most appropriate secure communication mechanism for current sensing platforms.

Li et al., [127] proposed a key-free communication method for IoT networks, which they called HlcAuth. Essentially, HlcAuth utilized challenge-response mechanisms for mutual authentication between the gateways and smart devices without key management. Through real-world evaluation, the authors showed that HlcAuth can defend against replay attacks, message-forgery attacks, and man-in-the-middle attacks. However, for HlcAuth to work, the authors assumed that attackers are not within a certain range (at least 4.2 meters) of the gateway node.

In [42], authors proposed employment of hardware-based Physical Unclonable Functions (PUFs), to enhance and enable security-related operations to be handled at the sensor level in IoT. Usage of PUFs will help in increasing the security level of the IoT, by allowing low-level security implementations on the things and also by devising cryptography software to perform special tasks such as verification.

5.3 Intrusion Detection

Roman et al., [60] argued that a key component of a fault-tolerant IoT system includes objects that are able to defend themselves not only against network failures but also from outsider attacks. Items in the IoT should be able to use intrusion detection software and other tools to hold back attackers. IoT systems are susceptible to hacker infiltration thus exposing users of the systems to cyberattacks. Any abnormal activities or situations should eventually result in the degradation and gradual cessation of service. Users, however, should be made aware of critical events as they occur. For example, when a malware attack is identified in one given device, users should be notified immediately of the increased likelihood of an attack occurring to them. In such cases, users should be encouraged to change their

passwords or take other necessary precautions so as to prevent theft of their personal information and compromise to their privacy.

Although IoT users may be unaware of the large number of IoT interactions that take place behind the scenes, presenting warnings and sharing information about any potential cyber threats may allow users to jump back into the loop to make their own decisions about their safety. For example, a user who is warned that his smart meter has been hacked may decide to change his login credentials. For warnings to ultimately make a difference in protecting user information, users' actions must be congruent with any warnings they receive [128]. A warning should result in users' taking some action toward securing their information. Therefore, a hacking warning presented without useful information may be less effective than a warning presented with some insight on the state of the IoT system. For instance, a very basic warning may be ignored, whereas a warning about someone requesting remote access to a user's information may be more effective at eliciting action.

5.4 Single Sign-On

In certain IoT contexts, single-sign-on (SSO) mechanisms can be useful, since users need to authenticate only once to interact with various devices. Users can then access all resources for which they have access permission without entering multiple passwords. However, traditional Web 2.0 SSO such as OpenID and Shibboleth were not designed to fulfill certain IoT requirements,[43] such as giving the user control over the choice of identity provider. Other mechanisms force users to employ a particular protocol, which can be problematic in a heterogeneous environment. Another issue is the lack of support for directional identities, in which objects broadcast their identities[77].

5.5 Establishing Trust

Trust is essential to implement the IoT. It encompasses how users feel while interacting in the IoT. Feelings of helplessness and being under some unknown external control can greatly undermine the deployment of IoT-based applications and services. There must be support for controlling the state of the virtual world. Users must be able to control their own services, and they must have tools that accurately describe all their interactions so that they can form an accurate mental map of their virtual surroundings.

Since, devices in IoT can physically move from one owner to another, trust should be established between both owners to enable a smooth transition of the IoT device with respect to access control and permissions. Xie & Wang [129] presented the concept of mutual trust for inter-system security in IoT by creating an item-level access-control framework. It establishes trust from creation to operation and the IoT transmission phase. This trust is established by two mechanisms; the creation key and the token. Any new device which is created is assigned a creation key by an entitlement system. The device manufacturer must request for this key. The token is generated by the manufacturer or current owner, and this token is combined with the RFID identification of the device. This mechanism ensures that the permissions are changed by the same device if a new owner is appointed, or it will be used in a different department of the same company, thus reducing the overheads of the new owner. Owners can change these tokens, provided the previous token is availed, to replace permissions and access control to the previous token.

In addition to encouraging risk awareness, designers of IoT devices should focus on instilling trust among users [130]. All devices should be able to perform their basic functions reliably, but in the case of

smart, interconnect devices, users should be assured that their information will be handled properly and that they will have the ability to revoke access to this information at any time. IoT devices are designed specifically to work with large amounts of users' data, so a reduction in access to users' information can be counterproductive to the overall goals of an IoT device. As such, it is important to reassure users about their device's safety. Putting users at ease may involve including a certain level of transparency as to what steps are being taken to protect their personal information. Increasing overall levels of trust may lead users to be more inclined to allow IoT devices access to information they might not grant access to if there were doubts about the security capabilities of the IoT system [130].

5.6 Security Awareness

Another important security measure for the success and growth of the IoT framework is awareness among human users who are part of the IoT. In [131] the authors explained the consequences of not guaranteeing IoT using real numbers. They accessed the IoT devices (SCADA devices, web cameras, traffic controllers, and printers) that were publicly available using the default password or without a password. The recorded results showed that many of these devices were actually accessible. If people continued to ignore security and use minimal security like the default password that comes with the product, this may lead to more harm than good. Hackers can attack the entire network if one of the devices is unprotected.

5.7 Security Tools

Beyond training, users can be equipped with tools that help them determine the safety of an IoT device. Researchers have proposed a mobile app that supports users' privacy-related decisions[132]. A "privacy coach" in the form of a mobile app can inform users if an RFID privacy policy matches up with their preferred privacy settings. On the whole, these types of tools may make users more aware of their role in the system and what can be expected for their privacy.

5.8 Privacy by design

One viable solution is privacy by design, in which users would have the tools they need to manage their own data. The solution is not too far from current reality. Whenever users produce a data fragment, they can already use dynamic consent tools that permit certain services to access as little or as much of that data as desired.

6. Threat Taxonomy

In this section we propose threat taxonomy based on the security and privacy threats enumerated in sections 4.1.3 and 4.2.3, respectively. The taxonomy also captures the vulnerabilities and the mitigation strategies.

Threat taxonomy divides the types of threats into different levels of detail. The purpose of this taxonomy is to create a point for solving problems, the ability to mix, adjust, change, and mitigate threats. In order to expand it, the threat taxonomy is a living structure used on the basis of collected data, from a holistic point of view of threats [2],[133].

Based on the vulnerabilities and threats identified at various levels of the reference architecture, we have combined them to formulate a novel taxonomy of threats for an IoT System. The taxonomy is illustrated

in Figure 3. From Figure 3, one can deduce that an agent or attacker operating within the internal or external IoT environment attacks and exploits the threats which may fall under security or privacy domain as explained in sections 4.1.3 and 4.2.3 respectively. The IoT security threats as outlined in section 4.1.3 include eavesdropping, spoofing, RF jamming, Sybil attack, sinkhole attack, man-in-the-middle attack, denial of service (DoS) attack, malicious code injection, sniffing attack and spear-phishing attack. On the other hand, privacy threats enumerated in section 4.2.3 include identification, location and tracking, profiling and interactions and presentations. The threats expose the IoT system, devices and users to vulnerabilities. There are several vulnerabilities which have been identified and analyzed from literature. However, we concentrate on a few key ones as explained in section 4.2.5. The ones covered include open ports, weak credentials and lack of authentication mechanism, weak programming practices, data leakage and improper encryption. The IoT vulnerabilities are mitigated using effective countermeasure strategies. Most of the countermeasures explained in section 4 attempt to prevent, detect, and/or mitigate the vulnerabilities we described in section 4,2,5. They include access and authentication controls, security protocols, intrusion detection, single sign-on, establishing trust, security awareness, security tools and privacy by design.

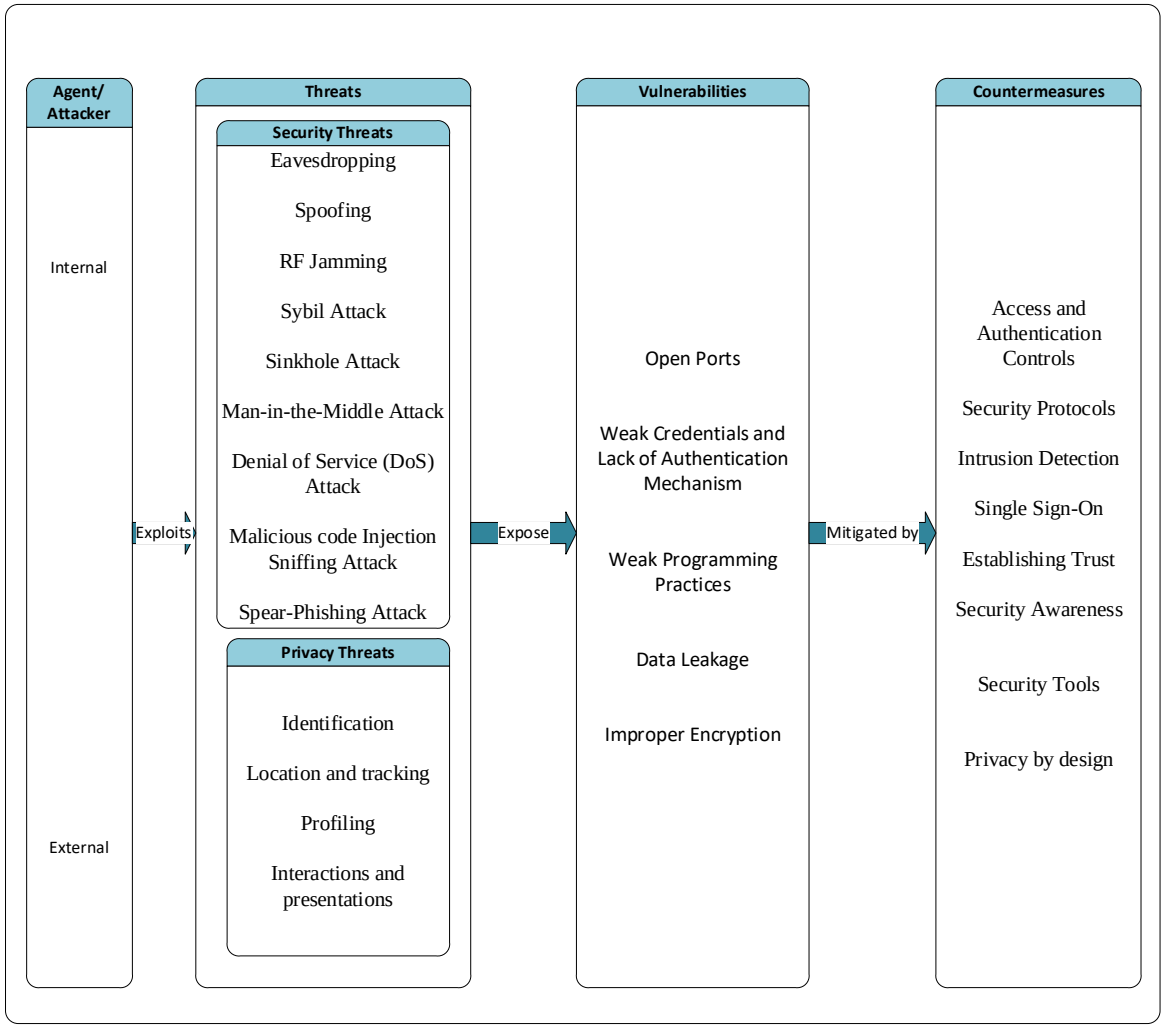

Figure 3: Threat Taxonomy

7. Open Research Challenges

With more IoT devices entering the uncontrolled, complex world and being deployed in hostile environments, securing IoT systems poses unique challenges. The survey identified a number of areas that still confound researchers in IoT privacy and security.

7.1 Security Research Issues

There are numerous reasons for IoT vulnerability. First, in most cases, the components have little control and are physically affected. Second, most communications are wireless. This will make it easier to listen to the secret messages. Finally, many components of the IoT have low capacity for energy and IT resources which prevent it from providing integrated security.

Despite significant efforts on the issue of IoT security, there are many issues that need to be addressed. First, the safety of the end-points of the IoT is important because of the variety of smart objects used. Later, integration, encryption, profiles and privileges, open trust, and labor-intensive protocols became important areas that required further research. Effective certification standards must also be considered. Second, we need to pay attention to the IoT ecosystem. It is very important for ecosystem data to facilitate monitoring of IoT system components throughout the life cycle. Third, we need to discuss IoT interactions from an IoT security perspective. The IoT security research is deficient in human user perspective when it comes to security requirements, threats, and vulnerabilities. This area needs further research to determine user specific IoT security requirements.

Fourth, while there exists a number of research efforts which propose IoT-tailored encryption schemes, we notice the shortage of studies which exhaustively and thoroughly assess and analyze their advantages and disadvantages under different malicious and benign IoT scenarios. Finally, we note the deficiency of remediation techniques concentrated on unnecessary open ports. These areas are fertile grounds for further research. Fifth, while we note that intrusion detection techniques in IoT realms demonstrate advanced progress, some of their methodologies leave the room for further research. Indeed, relying only on IDS mechanisms in an attempt to monitor intrusions seems to be not very effective, since they only detect limited attacks.

7.2 Privacy Research Issues

The security work of the IoT has shown great interest in protocols and planning. However, there are still some areas of interest in the area of privacy. First, start programs based on the principles of data minimization, to reduce the amount of personal data collected and to reduce storage needs, when a large amount of data is exchanged between IoT players. Second, researchers may try to standardize IoT security and safety mechanisms to meet the requirements of new circuits and algorithms. Third, instead of expecting IoT systems to meet their needs, new mechanisms need to be developed to allow users to manage their privacy settings.

The fourth issue concerns Limited Security-related Awareness Capabilities for IoT User. This challenge addresses secure access to IoT devices and their data. The possibility of an adversary gaining access to IoT devices by either brute-forcing their default credentials or by exploiting certain vulnerabilities remains a primary attack vector. This is possible with legacy IoT devices which are hard-coded or possess default credentials. We noticed that approaches which attempt to address this issue are rarely investigated in the literature. This challenge could be addressed by exploring techniques and methods to

increase users' awareness about the consequences of potential IoT threats and possible technical and non-technical strategies to reduce the risk of exposure.

8. Conclusion

The aim of this study was to provide a review of the most critical aspects of IoT with specific focus on the security issues and challenges involved with IoT devices with specific focus on the human user. We have identified many security and privacy issues that need to be addressed by the research community to make it a safe and secure platform that can enhance user adoption of the technology. Research focuses are much needed in this area to address these security issues and challenges in IoT heterogeneous environments so that users can confidently use IoT devices to communicate and share information globally with safety assurance.

In this paper we have identified threats and vulnerabilities that may hamper user adoption of IoT technology. The IoT security threats examined include eavesdropping, spoofing, RF jamming, Sybil attack, sinkhole attack, man-in-the-middle attack, denial of service (DoS) attack, malicious code injection, sniffing attack and spear-phishing attack. On the other hand, the privacy threats include identification, location and tracking, profiling and interactions and presentations. The paper also highlighted a few key vulnerabilities that may provide an attacker with the opportunity to infiltrate IoT systems or devices thus stealing personally identifiable information and other critical data. The three key vulnerabilities that may expose the devices include open ports, weak credentials and lack of authentication mechanism and weak programming practices. For this, the following key aspects should be considered to enhance security in IoT devices: access and authentication controls, single sign-on, establishing trust, security awareness and privacy by design.

The first contribution of this work is the analysis and classification of IoT security and privacy aspects. The security threats such as malicious code injection and denial-of-service attacks have high threat levels while RF jamming, Sybil attack, sinkhole attack and sniffing attack have medium impact. Spear phishing is considered to have low impact. These threats could expose the vulnerabilities within the IoT systems and devices leading to successful attack on IoT assets. In terms of privacy of IoT, profiling is the most severe threat with a rating of high with other threats like identification or tracking, which are at medium level of impact adding to its dangers by supplying even more linkable data. Privacy threats such as interaction and presentation, and lifecycle transactions are rated medium as they too have an effect on user profiling. Linkage and inventory attacks have low threat rating.

We also identified user requirements and challenges at the IoT architectural layers. We enumerated and discussed the threats, vulnerabilities and mitigation measures. We then proposed taxonomy of threats for IoT privacy and security. The model we have proposed integrates threats, vulnerabilities and countermeasures. We have also identified areas for further research. The research could focus on the safety of the end-points of the IoT, analysis of the advantages and disadvantages of various encryption technologies used in IoT, remediation techniques for the unnecessarily open ports. Additionally, researchers could explore techniques and methods to increase users' awareness about the consequences of potential IoT threats and possible technical and non-technical strategies to reduce the risk of exposure.

This paper has further determined that user-centricity is central to IoT privacy and security. Therefore, in terms of security, users expect (a) the devices to be secured at design and execution time (b) proactive identification and protection of IOT from arbitrary attacks (e.g. DoS and man-in-the-middle attacks) and abuse, and (c) proactive identification and protection of IOT from malicious software. In the domain of

user privacy, this paper determined that users want to have: (a) control over personal information (data privacy) and control over individual's physical location and movement (location privacy), and (b) methodologies and tools for identity management of users and objects. In the domain of trust, users desire to have: (a) easy and natural exchange of critical, protected and sensitive data, and (b) trust included as part of f the design of IoT.

REFERENCES

[1] M. Farooq, M. Waseem, A. Khairi, and S. Mazhar, "A Critical Analysis on the Security Concerns of Internet of Things (IoT)," *Int. J. Comput. Appl.*, vol. 111, no. 7, pp. 1–6, 2015, doi: 10.5120/19547-1280.

[2] 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, pp. 1–19, 2013, doi: 10.1016/j.future.2013.01.010.

[3] D. Bandyopadhyay and J. Sen, "Internet of things: Applications and challenges in technology and standardization," *Wirel. Pers. Commun.*, vol. 58, no. 1, pp. 49–69, 2011, doi: 10.1007/s11277-011-0288-5.

[4] T. V. N. Rao, "Design of Architecture for Efficient Integration of Internet of Things and Cloud Computing," *Int. J. Adv. Res. Comput. Sci.*, vol. 8, no. 3, pp. 392–396, 2017, [Online]. Available: www.ijarcs.info.

[5] A. McEwen and H. Cassimally, "The Internet of Things: An Overview," *Des. Internet Things*, no. October, p. 8, 2013.

[6] W.Mingjun *et al.*, "A research on experimental system for Internet of Things major and application project," in *3rd International Conference in System Science, Engineering Design and Manufacturing Informatization (ICSEM)*, 2012, pp. 261–263.

[7] R. Neisse, G. Baldini, E. Tragos, and I. N. Fovino, "Dynamic Context-Aware Scalable and Trust-based IoT Security , Privacy Framework," *Researchgate*, 2015.

[8] L. Atzori, I. Antonio, and M. Giacomo, "The Internet of Things: A survey," *Comput. Networks*, vol. Volume 54, no. Issue 15, p. Pages 2787-2805, 2010, [Online]. Available: http://dx.doi.org/10.1016/j.comnet.2010.05.010.

[9] D. Miorandi, S. Sicari, F. De Pellegrini, and I. Chlamtac, "Ad Hoc Networks Internet of things : Vision , applications and research challenges," *Ad Hoc Networks*, vol. 10, no. 7, pp. 1497–1516, 2012, doi: 10.1016/j.adhoc.2012.02.016.

[10] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-porisini, "Security , Privacy & Trust in Internet of Things : the road ahead," *Comput. Networks*, pp. 146–164, 2015.

[11] A. Riahi Sfar, E. Natalizio, Y. Challal, and Z. Chtourou, "A roadmap for security challenges in the Internet of Things," *Digit. Commun. Networks*, vol. 4, no. 2, pp. 118–137, 2018, doi: 10.1016/j.dcan.2017.04.003.

[12] N. Neshenko, E. Bou-Harb, J. Crichigno, G. Kaddoum, and N. Ghani, "'Demystifying IoT Security: An Exhaustive Survey on IoT Vulnerabilities and a First Empirical Look on Internet-Scale IoT Exploitations,'" *IEEE Commun. Surv. Tutorials*, vol. 29, no. 3, pp. 2702–2733, 2019, [Online]. Available: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8688434&isnumber=8809933.

[13] C. Pickering and J. Byrne, "Systematic quantitative literature reviews What are they and why use them ? Literature review Literature reviews ….. We all produce them … Common things in reviews going to review," pp. 1–17, 2016.

[14] B. Pejcinovic, "Using Systematic Literature Reviews to Enhance Student Learning," 2015.

[15] A. Dohr, R. Modre-Osprian, M. Drobics, D. Hayn, and G. Schreier, “The internet of things for ambient assisted living,” in *Seventh In- ternational Conference on Information Technology: New Generations (ITNG)*, 2010, pp. 804–809.

[16] ITU, “ITU-T Y.2060 Overview of the Internet of things. Available at https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-Y.2060-201206-I!!PDF-E&type=items internet of things reference architecture itu,” 2012.

[17] J. S. Kumar and D. R. Patel, “A Survey on Internet of Things : Security and Privacy Issues,” *Int. J. Comput. Appl.*, vol. 90, no. 11, pp. 20–26, 2014, doi: http://dx.doi.org/10.5120/15764-4454.

[18] R. Uttarkar and P. R. Kulkarni, “Internet of Things : Architecture and Security,” *Int. J. Comput. Appl.*, vol. 3, no. 4, pp. 12–19, 2014, [Online]. Available: http://www.rspublication.com/ijca/ijca_index.htm.

[19] X. Huang, P. Craig, H. Lin, and Z. Yan, “SecIoT : a security framework for the Internet of Things,” *Secur. Comm. Networks*, no. May 2015, pp. 3083–3094, 2016, doi: 10.1002/sec.

[20] M. Abomhara and G. M. Køien, “‘Security and privacy in the internet of things: Current status and open issues,’ in Privacy and Security in Mobile Systems (PRISMS), International Conference on.,” *IEEE*, pp. 1–8, 2014.

[21] S. M. P. Keyur K Patel, “Internet of Things-IOT : Definition , Characteristics , Architecture , Enabling Technologies , Application & Future Challenges,” *IJESC*, vol. 6, no. 5, 2016, doi: 10.4010/2016.1482.

[22] I. Lee and K. Lee, “The Internet of things (IoT): Applications, invest- ments, and challenges for enterprises,” *Bus. Horiz.*, vol. 58, pp. 431–440., 2015.

[23] N. Aleisa and K. Renaud, “Privacy of the Internet of Things: A Systematic Literature Review,” *Proc. 50th Hawaii Int. Conf. Syst. Sci.*, 2017, doi: 10.24251/hicss.2017.717.

[24] S. Notra, M. Siddiqi, H. H. Gharakheili, V. Sivaraman, and R. Boreli, “An Experimental Study of Security and Privacy Risks with Emerging Household Appliances (Position Paper),” *Commun. Netw. Secur. (CNS), 2014 IEEE Conf.*, pp. 79–84, 2014.

[25] G. Hernandez, O. Arias, D. Buentello, and Y. Jin, “Smart Nest Thermostat : A Smart Spy in Your Home,” *Black Hat USA*, pp. 1–8, 2014.

[26] M. Harbach, S. Fahl, and M. Smith, “Who’s afraid of which bad Wolf? A survey of IT security risk awareness,” *Proc. Comput. Secur. Found. Work.*, vol. 2014-Janua, pp. 97–110, 2014, doi: 10.1109/CSF.2014.15.

[27] K. Zhao and L. Ge, “A survey on the Internet of things security,” in *Proceedings of 9th International Conference on Computational Intelligence and Security (CIS)*, 2013, pp. 663–667.

[28] L. F. Cranor, “A Framework for Reasoning About the Human in the Loop,” *Proc. 1st Conf. Usability, Psychol. Secur.*, pp. 1:1--1:15, 2008, [Online]. Available: http://dl.acm.org/citation.cfm?id=1387649.1387650.

[29] R. Z. Rebaï, L. Ghorbel, C. A. Zayani, and I. Amous, “An adaptive method for user profile learning,” in *East European Conference on Advances in Databases and Information Systems*, 2013, pp. 126–134.

[30] M. Mezghani *et al.*, “Analyzing tagged resources for social interests detection To cite this version : HAL Id : hal-01178560,” in *16th International Conference on Enterprise Information Systems (ICEIS 2014)*, 2015, pp. 340–345.

[31] D. Tchuente, M.-F. Canut, N. Jessel, A. Péninou, and F. Sèdes, “Derivation of user profiles from social networks: a community approach of egocentric networks,” *Ingénierie des systèmes d’information*, vol. 18, no. 1, pp. 11–37, 2013.

[32] E. Khanfir, C. El Hog, R. B. Djmeaa, and I. A. B. Amor, “A web service selection framework based on user’s context and qos,” in *2014 IEEE International Conference on Web Services (ICWS)*, 2014, pp. 708–711.

[33] J. Miranda *et al.*, “From the Internet of Things to the Internet of People,” *IEEE Internet Comput.*, vol. 19, no. 2, pp. 40–47, 2015, doi: 10.1109/MIC.2015.24.

[34] M. Nitti, R. Girau, and L. Atzori, “Trustworthiness Management in the Social Internet of Things,” *IEEE Trans. Knowl. Data Eng.*, vol. 26, no. 5, 2014.

[35] E. Leloglu, “A Review of Security Concerns in Internet of Things,” *J. Comput. Commun.*, vol. 5, pp. 121–136, 2017, doi: 10.4236/jcc.2017.51010.

[36] M. Rimavicius, “Literature Review of the Internet of Things : Anticipating Tomorrow ’ s Challenges for Privacy and Security,” pp. 1–7, 2015.

[37] Wind River Systems, “Security in the Internet of Things,” 2015.

[38] K. (Ed) Kim and N. (Ed) Joukov, *Information Science and Applications*. 2017.

[39] M. Abdur, S. Habib, M. Ali, and S. Ullah, “Security Issues in the Internet of Things (IoT): A Comprehensive Study,” *Int. J. Adv. Comput. Sci. Appl.*, vol. 8, no. 6, 2017, doi: 10.14569/ijacsa.2017.080650.

[40] H. Sundmaeker, P. Guillemin, P. Friess, and S. Woelfflé, “Vision and Challenges for Realising the Internet of Things,” *Eur. Comm. Soc. Media*, 2010.

[41] F. Kamrani and M. Wedlin, “Internet of Things : Security and Privacy Issues,” no. December, 2016.

[42] T. Xu, J. Wendt, and M. Potkonjak, “Security of IoT Systems: Design Challenges and Opportunities.,” in *IEEE/ACM International Conference on Computer-Aided Design, Digest of Technical Papers*, 2014, pp. 417–423.

[43] M. Hossain, M. Fotouhi, and R. Hasan, “Towards an Analysis of Security Issues, Challenges, and Open Problems in the Internet of Things,” *2015 IEEE World Congr. Serv.*, no. June, pp. 21–28, 2015, doi: 10.1109/SERVICES.2015.12.

[44] S. Babar, P. Mahalle, A. Stango, and N. Prasad, “Proposed Security Model and Threat Taxonomy for the Internet of Things (IoT),” pp. 420–429, 2010.

[45] M. Amine, L. A. Maglaras, H. Janicke, and J. Jiang, “Authentication Protocols for Internet of Things: A Comprehensive Survey,” *Elsevier*, 2016.

[46] E. Rescorla, “The Transport Layer Security (TLS) Protocol Version 1.3,” *Netw. Work. Gr.*, 2018.

[47] J. H. Ziegeldorf, O. G. Morchon, and K. Wehrle, “Privacy in the Internet of Things : Threats and

Challenges," *Secur. Commun. Networks*, pp. 2728–2742, 2014.

[48] R. Kang, L. Dabbish, N. Fruchter, and S. Kiesler, "'My data just goes everywhere:' User mental models of the internet and implications for privacy and security," *SOUPS 2015 - Proc. 11th Symp. Usable Priv. Secur.*, pp. 39–52, 2019.

[49] H. A. Abdul-Ghani and D. Konstantas, "A comprehensive study of security and privacy guidelines, threats, and countermeasures: An IoT perspective," *J. Sens. Actuator Networks*, vol. 8, no. 2, 2019, doi: 10.3390/jsan8020022.

[50] A. M. A. Abuagoub, "IoT Security Evolution: Challenges and Countermeasures Review," *Int. J. Commun. Networks Inf. Secur.*, vol. 11, no. 3, pp. 342–351, 2019, [Online]. Available: https://search.proquest.com/docview/2354296086?accountid=8330%0Ahttp://jn8sf5hk5v.search.serialssolutions.com?ctx_ver=Z39.88-2004&ctx_enc=info:ofi/enc:UTF-8&rfr_id=info:sid/ProQ%3Atelecomms&rft_val_fmt=info:ofi/fmt:kev:mtx:journal&rft.genre=article&rft.jt.

[51] A. Zaslavsky, "Security and Privacy in the Internet of Things," pp. 1–2, 2015.

[52] F. Hu, *Security and Privacy in Internet of Things (IoTs): Models, Algorithms, and Implementations*. CRC Press Taylor & Francis Group, 2016.

[53] W. He *et al.*, "Rethinking access control and authentication for the Home Internet of Things (IoT)," *Proc. 27th USENIX Secur. Symp.*, pp. 255–272, 2018.

[54] J. P. Wang, S. Bin, Y. Yu, and X. X. Niu, "Distributed Trust Management Mechanism for the Internet of Things," *Appl. Mech. Mater.*, pp. 347–350, 2013.

[55] I. Andrea, C. Chrysostomou, and G. Hadjichristofi, "Internet of Things: Security vulnerabilities and challenges," in *Proceedings - IEEE Symposium on Computers and Communications*, 2016, vol. 2016-February, doi: 10.1109/ISCC.2015.7405513.

[56] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, and B. Sikdar, "A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures," *IEEE Access*, vol. 7, pp. 82721–82743, 2019, doi: 10.1109/ACCESS.2019.2924045.

[57] J. Bugeja, A. Jacobsson, and P. Davidsson, "On Privacy and Security Challenges in Smart Connected Homes," 2016, doi: 10.1109/EISIC.2016.21.

[58] Z. B. Celik, E. Fernandes, E. Pauley, G. Tan, and P. Mcdaniel, "Program analysis of commodity IoT applications for security and privacy: Challenges and opportunities," *ACM Comput. Surv.*, vol. 52, no. 4, 2019, doi: 10.1145/3333501.

[59] H. Lin and N. Bergmann, "IoT Privacy and Security Challenges for Smart Home Environments," *Information*, vol. 7, no. 3, p. 44, 2016, doi: 10.3390/info7030044.

[60] R. Roman, P. Najera, and J. Lopez, "Securing the Internet of Things," *IEEE Comput.*, vol. 44, pp. 51–58, 2011, doi: 10.1109/MC.2011.291.

[61] R. Falcone and A. Sapienza, "On the users' acceptance of IoT systems: A theoretical approach," *Inf.*, vol. 9, no. 3, 2018, doi: 10.3390/info9030053.

[62] A. Jain, B. Sharma, and P. Gupta, "Internet Of Things : Architecture , Security Goals , And Challenges- A Survey," *Int. J. Innov. Res. Sci. Eng.*, vol. 2, no. 4, pp. 154–163, 2016, [Online].

Available: www.ijirse.com.

[63] R. H. Weber, “Internet of Things – New security and privacy challenges,” *Comput. Secur. Rev. Sci. Elsevier*, 2010, doi: 10.1016/j.clsr.2009.11.008.

[64] S. Uludag, S. Zeadally, and M. Badra, “Techniques , Taxonomy , and Challenges of Privacy Protection in the Smart Grid,” 2015.

[65] W. Al-mawee, “Privacy and Security Issues in IoT Healthcare Applications for the Disabled Users a Survey,” 2012.

[66] J. Daubert, A. Wiesmaier, and P. Kikiras, “A View on Privacy & Trust in IoT,” 2015.

[67] T. Le and M. W. Mutka, “Access control with delegation for smart home applications,” *IoTDI 2019 - Proc. 2019 Internet Things Des. Implement.*, pp. 142–147, 2019, doi: 10.1145/3302505.3310076.

[68] B. Anggorojati, P. N. Mahalle, N. R. Prasad, and R. Prasad, “Capability-based access control delegation model on the federated IoT network,” *Wirel. Pers. Multimed. Commun. (WPMC), 2012 15th Int. Symp.*, pp. 604–608, 2012.

[69] B. Ur, J. Jung, and S. Schechter, “‘The current state of access control for smart devices in homes,’ .,” 2014.

[70] J. L. Hernández-ramos, J. B. Bernabe, M. V. Moreno, and A. F. Skarmeta, “Preserving Smart Objects Privacy through Anonymous and Accountable Access Control for a M2M-Enabled Internet of Things,” pp. 15611–15639, 2015, doi: 10.3390/s150715611.

[71] Z. Guoping and G. Wentao, “The Research of Access Control Based on UCON in the Internet of Things,” *J. Softw.*, vol. 6, no. 4, pp. 724–731, 2011, doi: 10.4304/jsw.6.4.724-731.

[72] N. Chaabouni, M. Mosbah, A. Zemmari, C. Sauvignac, and P. Faruki, “Network Intrusion Detection for IoT Security Based on Learning Techniques,” *IEEE Commun. Surv. Tutorials*, vol. 21, no. 3, 2019, doi: 10.1109/COMST.2019.2896380.

[73] I. Butun, P. Osterberg, and H. Song, “Security of the Internet of Things: Vulnerabilities, Attacks, and Countermeasures,” *IEEE Commun. Surv. Tutorials*, vol. 22, no. 1, pp. 616–644, 2020, doi: 10.1109/COMST.2019.2953364.

[74] J. Gupta, A. Nayyar, and P. Gupta, “Security and Privacy Issues in Internet of Things (IoT),” *IJRCS - Int. J. Res. Comput. Sci.*, vol. 3, pp. 18–22, 2015.

[75] L. Goeke, “Security Challenges of the Internet of Things,” 2017.

[76] D. Mendez, I. Papapanagiotou, and B. Yang, “Internet of Things : Survey on Security and Privacy,” pp. 1–16, 2017.

[77] A. Mohaisen, “The Sybil Attacks and Defenses: A Survey,” *Smart Comput. Rev.*, vol. 3, no. 6, 2013, doi: 10.6029/smartcr.2013.06.009.

[78] R. W. Anwar *et al.*, “Security Issues and Attacks in Wireless Sensor Network,” vol. 30, no. 10, pp. 1224–1227, 2014, doi: 10.5829/idosi.wasj.2014.30.10.334.

[79] J. Deng, R. Han, and S. Mishra, “Defending against Path-based DoS Attacks in Wireless Sensor Networks,” 2005.

[80] J. R. Douceur, “The Sybil Attack,” pp. 251–252, 2002.

[81] A. Singla, “Review on Security Issues and Attacks in Wireless Sensor Networks,” *IJARCSSE*, vol. 3, no. 4, pp. 529–534, 2013.

[82] B. Tuhin, K. Uday, and S. Sugata, “Survey of Security and Privacy Issues of Internet of Things,” vol. 6, no. 4, pp. 2372–2378, 2015.

[83] A. Kulshrestha and S. K. Dubey, “A Literature Review on Sniffing Attacks in Computer Network,” no. 2, 2014.

[84] B. Khoo, “RFID as an Enabler of the Internet of Things: Issues of Security and Privacy,” in *International Conference on Internet of Things and International Conference on Cyber, Physical and Social Computing (2011)*, 2011, pp. 709-712.

[85]] C Ramakrishna,] G Kiran Kumar,] A Mallikarjuna Reddy, and P. Ravi, “A Survey on various IoT Attacks and its Countermeasures,” *Int. J. Eng. Res. Comput. Sci. Eng.*, vol. 5, no. 4, pp. 2394–2320, 2018, [Online]. Available: http://ijercse.com/specissue/april-2018/27.pdf.

[86] T. Borgohain, U. Kumar, and S. Sanyal, “Survey of Security and Privacy Issues of Internet of Things,” vol. 2378, pp. 2372–2378, 2015.

[87] M. Premkumar, T. V. P. Sundararajan, and K. Vinoth Kumar, “Various defense countermeasures against DoS attacks in wireless sensor networks,” *Int. J. Sci. Technol. Res.*, vol. 8, no. 10, pp. 2926–2935, 2019.

[88] M. Abomhara and G. M. Køien, “Cyber security and the internet of things: Vulnerabilities, threats, intruders and attacks,” *J. Cyber Secur. Mobil.*, vol. 4, no. 1, pp. 65–88, 2015, doi: 10.13052/jcsm2245-1439.414.

[89] D. Miessler, “Securing the Internet of Things : Mapping Attack Surface Areas Using the OWASP IoT Top 10,” 2015.

[90] OWASP, “IoT Attack Surface Areas,” 2015. https://www.owasp.org/index.php/IoT_Attack_Surface_Areas.

[91] European Commission, “IoT Privacy, Data Protection, Information Security,” *Eur. Comm.*, pp. 1–9, 2013, [Online]. Available: http://ec.europa.eu/digital-agenda/en/news/conclusions-internet-things-public-consultation.

[92] R. Roman, J. Zhou, and J. Lopez, “On the features and Challenges,” *Comput. Networks*, vol. 57, 2013, [Online]. Available: http://ac.els-cdn.com/S1389128613000054/1-s2.0-S1389128613000054-main.pdf?_tid=62952796-1fb8-11e4-b600-00000aab0f6b&acdnat=1407583931_1fb78496c95511b61437402b5af0bd17.

[93] P. Hustinx, “Privacy by design : delivering the promises,” no. January, pp. 253–255, 2010, doi: 10.1007/s12394-010-0061-z.

[94] S. Fischer-Hübner, P. Duquenoy, M. Hansen, R. Leenes, and G. Zhang, “IFIP Advances in Information and Communication Technology: Preface,” *IFIP Adv. Inf. Commun. Technol.*, vol. 352 AICT, no. April, 2011, doi: 10.1007/978-3-642-20769-3.

[95] K. Rose, S. Eldridge, and L. Chapin, “The Internet of Things : An Overview,” *Internet Soc.*, no. October, 2015.

[96] G. Baldini, M. Botterman, R. Neisse, and M. Tallacchini, “Ethical Design in the Internet of Things,” *Sci. Eng. Ethics*, vol. 24, no. 3, pp. 905–925, 2018, doi: 10.1007/s11948-016-9754-5.

[97] E. Bertino, L. D. Martino, F. Paci, and A. C. Squicciarini, *“Web services threats, vulnerabilities, and countermeasures,” in Security for Web Services and Service-Oriented Architectures*. Springer, 2010.

[98] J. M. Kizza, *Guide to Computer Network Security*. Springer, 2013.

[99] J. Granjal, E. Monteiro, and J. Sa 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, doi: 10.1109/COMST.2015.2388550.

[100] OWASP, “OWASP Top Ten Vulnerabilities 2018 Project,” 2018. https://owasp.org/www-pdf-archive/OWASP-IoT-Top-10-2018-final.pdf.

[101] A. Cui and S. J. Stolfo, “A quantitative analysis of the insecurity of embedded network devices: Results of a wide-area scan,” *Proc. - Annu. Comput. Secur. Appl. Conf. ACSAC*, pp. 97–106, 2010, doi: 10.1145/1920261.1920276.

[102] Y. M. Pa Pa, S. Suzuki, K. Yoshioka, T. Matsumoto, T. Kasama, and C. Rossow, “IoTPOT: Analysing the rise of IoT compromises,” *9th USENIX Work. Offensive Technol. WOOT 2015*, 2015.

[103] J. Czyz, M. Luckie, M. Allman, and M. Bailey, “Don’t Forget to Lock the Back Door! A Characterization of IPv6 Network Security Policy,” *Netw. Distrib. Syst. Secur. Symp.*, no. February, pp. 21–24, 2017, doi: 10.14722/ndss.2016.23047.

[104] A. Furfaro, L. Argento, A. Parise, and A. Piccolo, “‘Using virtual environments for the assessment of cybersecurity issues in iot scenarios,’” *Simul. Model. Pract. Theory*, vol. 73, pp. 43–54, 2017.

[105] A. Tekeoglu and A. S. Tosun, “‘A testbed for security and privacy analysis of iot devices,’” in *2016 IEEE 13th International Conference on. IEEE, 2016 in Mobile Ad Hoc and Sensor Systems (MASS)*, 2016, pp. 343– 348.

[106] A. Cui, M. Costello, and S. J. Stolfo, “‘When firmware modifications attack: A case study of embedded exploitation.,’” *NDSS*, 2013.

[107] Z. Berkay Celik *et al.*, “Open access to the Proceedings of the 27th USENIX Security Symposium is sponsored by USENIX. Sensitive Information Tracking in Commodity IoT Sensitive Information Tracking in Commodity IoT,” *USENIX Secur. Symp.*, 2018, [Online]. Available: www.usenix.org/conference/usenixsecurity18/presentation/celik.

[108] J. Wurm, K. Hoang, O. Arias, A.-R. Sadeghi, and Y. Jin, “‘Security analysis on consumer and industrial iot devices,’” in *Design Automation Conference (ASP-DAC), 2016 21st Asia and South Pacific*, 2016, pp. 519–524.

[109] A. Singh, N. Chawla, J. H. Ko, M. Kar, and S. Mukhopadhyay., “Energy Efficient and Side-Channel Secure Cryptographic Hardware for IoT-Edge Nodes,” *IEEE Internet ofThings J.*, 2019.

[110] D. Jeske and P. Schaik, “Familiarity with Internet threats: Beyond awareness,” *Comput. Secur.*, vol. 66, pp. 129–141, 2017.

[111] S. Furman, M. F. Theofanos, Y. Y. Choong, and B. Stanton, “Basing cyber- security training on user perceptions,” *IEEE Secur. Priv.*, vol. 10, pp. 40–49, 2012.

[112] S. Cirani, G. Ferrari, and L. Veltri, “Enforcing Security Mechanisms in the IP-Based Internet of Things: An Algorithmic Overview,” pp. 197–226, 2013, doi: 10.3390/a6020197.

[113] S. Aragon, M. Tiloca, M. Maass, M. Hollick, and S. Raza, “ACE of spades in the iot security game: A flexible ipsec security profile for access control,” *2018 IEEE Conf. Commun. Netw. Secur. CNS 2018*, 2018, doi: 10.1109/CNS.2018.8433209.

[114] J. A. Martı´nez, J. L. Herna´ndez-Ramos, V. Beltra´n, A. S. Ruiz, and P. M, “A user-centric Internet of Things platform to empower users for managing security and privacy concerns in the Internet of Energy,” *Int. J. Distrib. Sens. Networks*, vol. 13, no. 8, 2017, doi: 10.1177/1550147717727974.

[115] E. Zeng and F. Roesner, “Understanding and improving security and privacy in multi-user smart homes: A design exploration and in-home user study,” *Proc. 28th USENIX Secur. Symp.*, pp. 159–176, 2019.

[116] K. Yang, D. Forte, and M. M. Tehranipoor, “‘Protecting endpoint devices in iot supply chain,’” in *2015 IEEE/ACM International Conference on Computer-Aided Design (ICCAD)*, 2015, pp. 351–356.

[117] E. Fernandes, J. Paupore, A. Rahmati, D. Simionato, M. Conti, and A. Prakash, “‘Flowfence: Practical data protection for emerging iot application frameworks,’” 2016.

[118] W. Chen *et al.*, “Taprint : Secure Text Input for Commodity Smart Wristbands,” *ACM Int. Conf. Mob. Comput. Netw.*, 2019.

[119] Z. Yan, Q. Song, R. Tan, Y. Li, and A. W. K. Kong, “Towards touch-to-access device authentication using induced body electric potentials,” *Proc. Annu. Int. Conf. Mob. Comput. Networking, MOBICOM*, 2019, doi: 10.1145/3300061.3300118.

[120] X. Li, F. Yan, F. Zuo, Q. Zeng, and L. Luo, “Touch Well Before Use: Intuitive and Secure Authentication for IoT Devices,” *Proc. 25th Annu. Int. Conf. Mob. Comput. Netw.*, pp. 1–17, 2019, doi: 10.1145/3300061.3345434.

[121] V. Nguyen *et al.*, “Body-guided communications: A low-power, highly-confined primitive to track and secure every touch,” *Proc. Annu. Int. Conf. Mob. Comput. Networking, MOBICOM*, pp. 353–368, 2018, doi: 10.1145/3241539.3241550.

[122] B. Hutchins, M. Zhou, A. Reddy, M. Li, W. Jin, and L. Yang, “Beat-PIN: A user authentication mechanism for wearable devices through secret beats,” *ASIACCS 2018 - Proc. 2018 ACM Asia Conf. Comput. Commun. Secur.*, pp. 101–115, 2018, doi: 10.1145/3196494.3196543.

[123] F. Lin, C. Song, Y. Zhuang, W. Xu, C. Li, and K. Ren, “Cardiac scan: A non-contact and continuous heart-based user authentication system,” *Proc. Annu. Int. Conf. Mob. Comput. Networking, MOBICOM*, vol. Part F1312, pp. 315–328, 2017, doi: 10.1145/3117811.3117839.

[124] H. Feng, K. Fawaz, and K. G. Shin, “Continuous authentication for voice assistants,” *Proc. Annu. Int. Conf. Mob. Comput. Networking, MOBICOM*, vol. Part F1312, pp. 343–355, 2017, doi: 10.1145/3117811.3117823.

[125] M. A. M. Isa, N. N. Mohamed, H. Hashim, S. F. S. Adnan, J. Manan, and R. Mahmod, “A

lightweight and secure tftp protocol for smart environment," in *2012 IEEE Symposium in Computer Applications and Industrial Electronics (ISCAIE)*, 2012, pp. 302–306.

[126] J. Granjal, E. Monteiro, and J. S. Silva, "On the effectiveness of end- to-end security for internet-integrated sensing applications," in *2012 IEEE International Conference in Green Computing and Communications (GreenCom)*, 2012, pp. 87–93.

[127] C. Li *et al.*, "HlcAuth: Key-free and secure communications via home-limited channel," *ASIACCS 2018 - Proc. 2018 ACM Asia Conf. Comput. Commun. Secur.*, pp. 29–35, 2018, doi: 10.1145/3196494.3196499.

[128] I. Chong, A. Xiong, and R. W. Proctor, "Human Factors in the Privacy and Security of the Internet of Things," *Ergon. Des.*, vol. 27, no. 3, pp. 5–10, 2019, doi: 10.1177/1064804617750321.

[129] Y. Xie and D. Wang, "An Item-Level Access Control Framework for Inter-System Security in the Internet of Things," *Appl. Mech. Mater.*, pp. 1430–1432, 2014.

[130] K. A. Hoff and M. Bashir, "Trust in automation: Integrating empirical evidence on factors that influence trust," *Hum. Factors*, vol. 57, no. 3, pp. 407–434, 2015, doi: 10.1177/0018720814547570.

[131] M. Patton, E. Gross, R. Chinn, S. Forbis, L. Walker, and H. Chen, "Uninvited Connections: A Study of Vulnerable Devices on the Internet of Things (IoT)," in *Joint Intelligence and Security Informatics Conference (JISIC)*, 2014, pp. 232–235.

[132] Z. Zhang, "RETRACTED ARTICLE: Research on RMB internationalization path," *Proc. 2nd Int. Conf. Artif. Intell. Manag. Sci. Electron. Commer. AIMSEC 2011*, pp. 578–581, 2011, doi: 10.1109/AIMSEC.2011.6010224.

[133] S. Ferdous, R. K. Hussein, O. Madini, A. Alharthi, R. J. Walters, and G. Wills, "Threat Taxonomy for Cloud of Things," in *Internet of Things and Big Data Analytics*, United Scholars Publications, USA, 2017, pp. 1–27.