Academic Journal of Nawroz University (AJNU), Vol.12, No.4, 2023

https://doi.org/10.25007/ajnu.v12n4a1116

A Systematic Roadmap on Privacy, Security, Trust, Identity Management, and Resilience: Wireless Sensor Networks and Internet of Things Architectures

Idrees S. Kocher

Energy Engineering Department, Technical College of Engineering, Duhok Polytechnic University, Duhok, KRG – Iraq

ABSTRACT: As everything around us will be linked to the net in many ways via the Internet of Things (IoTs) and compared to the standard Internet, new forms of problems and complications can arise. Huge IoTs experiments are currently under way, most of which concern its sight, supporting technology, software, or facilities. Recently, a limited studies have comprehensively defined the security requirements such as privacy concerns, security, and trusting in the IoTs that are deemed special to the future net, these terms need to be discussed and addressed via numerous scholars and research groups as well. This article surveyed through 102 references from popular literature databases to explore the features\ properties that define the distinctive IoT relating to forthcoming privacy, security and trust issues. Then created security requirements that were triggered by the mentioned properties. This article examined the privacy, security, trust and resilience components of the three most popular IoT architectures in consideration of the requirements as well. Also, this survey contributed to the state-of-the-art security issues for embedded devices in Internet of Things world including provide a comparative table of well-known secure routing protocols and their countermeasures to well-known attacks on Open Systems Interconnection (OSI) structure of Wireless Sensor Networks (WSNs) within Internet of Things world. Finally, this survey identifies a number of study gaps that will serve as the foundation for future research**.**

Keywords: Wireless Sensor Networks; Iots Properties; Iots Security Requirements; Iots Architectures; Attacks and Defenses

1. Introduction

The Internet of Things (IoTs) brings intelligent processing and communication capabilities to common items and equipment including conventional tools, sensors, cameras, vehicles, and utilities that aren't often thought of as smart devices. Enabling many entities to co-operatively collaborate and interact together to accomplish shared aims with limited human intervention (Köhler, 2014; Zanellaa et. al., 2014). To make our society simpler as well as better, such interactive appliances relate everyone's real world to the virtual world. IoTs becomes exponentially increasing, the amount of connected devices or computers surpassed the number of individuals on our planet in 2011 and every object of our daily life sis supposed to be linked to the digital environment by 2025, as reported for the US National Intelligence Council (NIC)[(Gubbi et. al., 2013; NIC, 2008). In several ways, it will change the lives, as IoTs incorporates a vast variety of different appliances which really produce and consume various set of valuable and useful data for substantial presence of important technologies that has never been discovered. These technologies can use the large size and varied kinds of data generated to deliver a new era of products. Numerous areas of our functional life, such as power and traffic management, house / building control, factory automation, battlefield, and hospitals, and many others, would include IoTs technologies and services (Bellavista et. al., 2013). IoTs diverse tools, software, and facilities, however, face many obstacles and problems, involving anonymity, security, and trust, which can also be regarded as significant obstacle seen between functional IoTs itself and its effective application, launch, and incorporation across our everyday lives. Therefore, numerous research works and efforts are still needed in several ways to completely adopt, implement, and use the IoTs principles for realistic life (Tan & Wang, 2010). Transportation, smart homes, mobility, smart industrial processes and smart energy grids are IoT`s applications. IoT architectures would address not just operational issues, but also security and privacy concerns. To gain societal approval, for example, social

system need to believe that the Internet of Things will manage such situations in a secure and private style. (Vasilomanolakis et. al., 2015; Gao & Bai, 2014).

By providing a systematic review of relevant work, this article outlines properties for the IoT ecosystem that, when combined, distinguish it from prior Information Technology (IT) architectures. A variety of security criteria are recorded in relation to these properties during construction. Moreover, the most prevalent IoT architectures are identified, and a detailed analysis is conducted by mapping them to the requirements. Lastly, the author of this article compares three architecture types of IoT then identifies research gaps as the actions required for a comprehensive IoT architecture in terms of security and privacy. Based on above facts, this systematic survey provides a major IoTs problems and state-of-the-art security issues which have to be resolved in order to satisfy a criteria for the fully functional and stable implementation of IoTs environments through the daily routines. Finally, updates the reader about what was achieved and/or recommended to resolve certain IoTs issues and concerns and also what needs to be tackled.

The remainder of this paper is structured as follows: Section 2 poses the key difficulties and problems of properties that restrict IoT's reliable use. In Section 3, a number of proposed security requirements that take into account these IoT properties, also several IoTs issues including its challenges and problems along with their security constraints, attacks, and IoTs countermeasures are presented. Section 4 addresses and provides an overview of the IoT architectures as well as a security and privacy analysis of them with respect to proposed requirements. In section 5, a comparative analysis of all IoT architectures with a focus on the fulfillment of the security requirements. Finally, Section 6 outlines a general results of work of such a systematic survey, concludes the survey, gives insights regarding current research gaps and possible future directions.

2. Unique Properties of Internet of Things

This section will look at the properties which distinguish the IoT in relation to security, privacy, and trust issues. As compared to conventional IT approaches such as big data, cloud computing, and business applications, the IoT is distinctive in relation to the issues that must be overcome due to a combination of properties. By examining relevant IoT researches in literature as in (Atamli & Martin, 2014; Babar et. al., 2010; Cirani et. al., 2013; Gazis et. al., 2014; Gubbi et. al., 2013; Mayzaud et. al., 2013; Miorandi et al., 2012;Ning et al.,2013 ; Roman et al., 2011; Web, 2010), these properties are identified. The identified distinguishing properties are introduced in the following subsections:

2.1 Limited resources

The IoT`s devices will have resource restrictions that must be addressed when designing security procedures. This covers both energy constraints, such as battery-powered devices, and limited processing power, such as micro sensors. As a result, costly computational encryption methods can't be used everywhere.

2.2 Unattended and uncontrolled environments

Micro sensors, such as traffic control camera systems and environmental tiny sensors, can be made publicly accessible via the Internet of Things. In such a setting, stable connected devices and steady presence are quite improbable. Because of the massive number of communicated devices among others and users in such an ecosystem, a priori trustworthy connections are also problematic (Roman et al., 2011). As a result, automated trust measurement and management methods for things, services, and consumers are essential again for IoT.

2.3 Interoperability and heterogeneity

Because it will have to incorporate a variety of items from diverse manufacturers, the Internet of Things is anticipated to be a very heterogeneous environment. As a result, model compatibility and interoperability must be taken into account.

2.4 Scalability

The IoT's enormous network of linked devices necessitates protocols that are extremely scalable. This would have implications for security measures. This would have implications for security measures. Centralized techniques, such as hierarchical Public Key Infrastructures (PKIs), and certain distributed approaches, such as pairs symmetric key exchange systems, for example, cannot grow with the Iot system.

3. Proposed Requirements of IoTs

This study synthesizes security requirements from the IoT domain, as well as associated IT sectors, and develops them in accordance with IoT properties to offer a thorough perspective. The next subsections divide the requirements into five sets of security needs, each with its own set of subcomponents:

3.1. IoT`s Privacy

The IoTs privacy main aim is to prevent the misuse and discloser of information. Several solutions had been made for identifying the IoTs privacy issues and find possible solution for them regarding either the personal or device specific privacy. In the following points, several privacy issues are listed as in (Bandyopadhyay & Se, 2011; Sarhan, 2018):

- Users generally do not want their data to be viewed by the public, thus there is a need for user control over their sensitive data to guarantee data privacy.
- A need for location privacy by controlling the user's physical location and movement so they won't be tracked without their permission.
- A necessity for privacy legislation as straightforward legal mechanisms to guarantee the right to privacy.
- Maintaining privacy management by providing standard, methodologies and tools to serve this purpose.

In addition, privacy considerations are being generalized to cover consumer's tools as done in (Said & Masud, 2013):

- Specify who is acquiring devices information.
- Specify how devices information is acquired.
- Specify the actual required time to acquire devices information.
- Specify the actual reasons from acquiring process of devices information.

Consequently, the collected user and device centric information should be kept in licensed servers and handled only by licensed individuals in (Chan & Perrig, 2003). In the context of IoT, a conflict of polices from the communicated and interacted systems will result and arise as an issue in this field, since each system has its own collection of privacy policies. Based on above mentioned facts, policies checking, notification and resolving processes required new approaches and solutions (Stankovic, 2014). Therefore, privacy rules were deemed a real challenge that might restrict the interaction of entirely different IoTs systems, there is still a need for scholars to develop a new standardized vocabulary in each system to describe privacy rules. For instance, a framework of Platform for Privacy Preferences (PPP) functions well enough as a tool to create privacy policies inside the conventional internet. Regrettably, there are many disadvantages of conventional online privacy languages within the IoT because they do not recognize dynamic shifts in policy in actual environments or communicate various forms of dynamic information and contexts (Olurin et al., 2012). The delegation process also as privacy protection strategy, however, is yet another possible resolution. The basic example of such a mechanism could be provided as a smart refrigerator coordination process corresponds to an individual consumer network domain and another distinct network domain refers to a smart search service. A selection of food products can be identified by the smart search service depend on the expiry date or accessibility inside the smart refrigerator. In order to do any of this, entry to the smart fridge requires the right. The legitimate right will be transferred from the consumer network domain to the application network domain to allow the service product to search the data presented by it to shape a list of recommendations in order to solve such problem (Roman et al., 2011). If an IoTs customer is able to search RFID tags inserted in items like visa card using only a Radio-Frequency Identification (RFID) reader on cell phones and import its privacy rules to use interact with them, this indicates that a fascinating strategy known as the privacy coach is implement (Broenink et al., 2010). For this approach, a consumer may opt to never use the entity if an entity's installed privacy policy may not meet the customer's expectation. But from the other side, the handset can verify the privacy rules of the reader and seek user permission if there is an attempt by an RFID browser to access details from the customer's cell phone. A further application of privacy coach is the security of the sensitive or private physical area like office. This method of security is accomplished by conducting a monitoring procedure without any of the consent of its owner for malicious insider devices, such as detectors placed in a building for doing monitoring (. Radomirovic, 2010). Subscribers often wish to share data about themselves, but

without revealing far too much. For instance, a user might notice somebody near his place whom enjoys that kind of music he enjoys without offering the close person his own location and music preferences (Oleshchuk, 2009). In relation to the abovementioned case, there would be a significant number of situations to gathering various forms of customer data. In highest point of all that, a small cost of processing data, that is around $0.03 / GBytes or much lower these days, making data effectively preserved. It would, however, not be necessary for consumers to directly handle their information (Atzori et al., 2010). Recording user records, however, poses many potential privacy issues as they're being used throughout many detrimental ways fraud or public reporting. A digital forget system is therefore required to deal with the problems throughout this regard via regularly removing customer data that is not necessary. Digital forget means that only when data specifically needed is memorized (Singh et al., 2015). So a guest pass function of a Flickr (https:/www.flickr.com) site, for instance, enables its members to access and distribute multiple forms of images files across the web, so that their files will expire at a given date and then to be removed (Thompson, 2021). This is apparent that digital forget has also been regarded as an important and required strategy for the protection of privacy. Regrettably, research related to such a methodology and realistic updates towards its growth are only at the starting stage (Mayar, 2009). Consumers do not restrict even control which knowledge is obtained from them in many different circumstances. Users go in to a house fitted with a sensor network, for instance composed of IoTs sensors like cameras. Such condition is mostly prevented through not going into the house, so no photo can be obtained with customers, but customers can access sensor-equipped houses in many other situations nowadays. Within that context, one possible approach is to restrict a capacity of the IoT system installed in these houses. Restrictions are also applied to the processing of information at a comprehensive level that would not in any way compromise privacy. For instance, distortion is added to people's photographs such that the necessary details in such images is protected, thereby preserving the privacy of individuals. Sometimes in critical cases, to provide some required facts or specifics for further procedures, a photo of a person belonging is always retrieved afterwards, although this must be accomplished exclusively via law enforcement personnel (Wickramasuriya et al., 2004).

Due to the engagement of people and more pervasive data gathering, such as in smart home situations, privacy is regarded to be one of the most prominent issues in the IoT (Medaglia & Serbanati, 2010). Depending on how an IT system viewed, a variety of privacy definitions exist.

• **Data privacy:** This term completes confidential transmitted data in that a database record really should not reveal unwanted properties, such as a person's identity. Since many sensing devices capture personal details, this is a huge problem with the Iot applications. When a large volume of such data is pooled, it creates Personally Identifiable Information (PII), which may be used to identify individuals (Daubert et al., 2015). There are techniques to "anonymize" such data records (Machanavajjhala et al., 2007; Sweeney, 2002 ; Xiao & Tao, 2007), however they have always proven inadequate. Furthermore, techniques to secure data privacy during data transmission among domains are mostly unknown and difficult to implement (Dwork & Lei, 2009).

• **Anonymity:** It refers to a single person's inability to be identified as the source of data or an action (Pfitzmann & Kohntopp, 2000). Anonymity is difficult to achieve because wearable and mobile devices may unintentionally reveal PII such as IP addresses and location. Although technologies like anonymous credentials (Camenisch & Herreweghen, 2002) and onion routing (Dingledine et al., 2004) are available in literature, they do not adapt effectively with the Internet of Things.

• **Pseudonymity:** This term is a tradeoff between anonymity and accountability. The activities of a person are tied to a pseudonym, a random identifier, rather than an identity, in pseudonymity. It can be used for a variety of objectives (Pfitzmann & Kohntopp, 2000), such as connecting numerous acts by the same individual or allowing for the graceful deterioration of anonymity in the event of misuse. Although pseudonyms can alleviate privacy issues and accountability in the IoT, consistent strategies that span various domains are necessary.

• **Unlinkability:** This term defines pseudonymity by stating that particular activities performed by the same person cannot be connected. In IoT, unlinkability guards against profiling. Although pseudonyms potentially address unlinkability by using a distinct pseudonym for each activity, cross-implications with anonymity, especially unknown meta-data, remain a difficulty. In addition, some entity may always trace every pseudonym to a person, and hence link all actions of that person.

It is worthy saying that privacy challenges within the traditional net almost exist only with people who

play active roles. On the other hand, people face privacy challenges in the IoTs sense, regardless of whether or not they use any program or service. Securing privacy and consumer consent is accepted as one of the major criteria for the widespread acceptance of IoT applications (Sarhan, 2018). To the best of author knowledge, privacy problems in the IoT must be taken seriously, researchers must pay greater attention to them, and they must be included and recognized in the development of any IoT-based strategy.

3.2. WSNs and IOTS Security Issues

In many ways, privacy and security in the Internet of Things overlap and support one other. For IoTs world such as Wireless Sensor Networks (WSNs) and RFID devices, the term security is a decisive issues because of the computing limitations, resource constraints, work nature, little storage capability, limited power, and restricted remote channel data transfer capacity of these devices. Although remote sensors and other elements of IoTs have been utilized at numerous touchy implementation fields, they still threaten by adversary in the event that they are used in unattended environments (Sarhan, 2018). Any compromised sensor device within the IoTs may lead to compromising entire system as well. However, programming and equipment improvements may address this issue partially. In general, to deal with the issue appropriately and exhaustively, refined countermeasures must be applied such as secured key management algorithms, adversary detection mechanisms and secured routing algorithms (Kocher et al., 2013). Table 1 summarizes WSNs threats with their suitable defenses which lead to meet secured WSNs in IoTs world (Zia & Zomaya, 2006; Zhao & Ge, 2013; Kocher, 2020; Gawdan & Sarhan, 2016; Gawdan et al., 2011a; Gawdan et al., 2011b; Kocher & Sarhan, 2017). For more details, Table 1 with its contents was introduced in details in my previous published work as in (Kocher, 2021).

Table 1. Threats with their suitable defenses in OSI WSNs layers within IoTs world

OSI WSN Layer Names	Possible Threats	Countermeasures Methods	Countermeasures Methods References.
Transport	Flooding De-synchronization	Client Puzzles Authentication	[47,49,96] [49,96]
Network	Hello Flood	{Authentication, Packet Leashes, Implementing Temporal and Geographic Data}	[47, 49,94, 97]
	{Selective Forwarding Spoofing and Alteration Attacks}	{Egress filtering, Authentication and Monitoring}	[97]
	Replayed Attack	counters or time-stamps	[47,49]
	Wormhole Attacks	{Authentication and Probing}	[47,49,97]
	Blackhole Attack	Enhanced path-finding	[98]
	Grayholes Attack	Isolate hostile node	[99]
	Sinkhole	Redundancy Check	[47,49,97]
	Sybil	{Redundancy Check, Authentication and Monitoring}	[100,101]
	{Acknowledgement Flooding}	{Authentication, Bidirectional Link Authentication Verification}	[48,49,97]
Link	Exhaustion	Rate Limitation	[96]
	Collision	Error Correction Code (ECC)	[96]
	Unfairness	Small Frames	[96]
Physical	Jamming	{Priority messages, Spread Spectrum, Low Duty Cycle and Mode Change}	[102]

In order to provide the world of IoTs with significant security answers, it's indeed imperative deal with the restrictive conditions presented through the following points for WSNs since those who lay a foundation for constructing IoTs systems (Kocher et al., 2013):

• **Unreliable Wireless Channel**: This is due to unreliable data transfer, data conflicts, and data processing latency for WSNs.

• **Limited Resources:** Examples of these are limited code storage space, limited data memory size, and limited battery energy.

• **Unattended Environment Operation:** An examples of these are unattended deployment, natural disasters.

Additionally, the need arise to new applications to instantly notify users if there should arise an occurrence of shifted object from any limited region with no permission. The warnings activated as output from these applications may take a numerous structures like SMSs, voice message and emails (Atzori & Morabito, 2010). For IoTs services and applications, they must have capability to achieve underlying tasks even with the present of attacks and furthermore ought to have the capacity to do recuperating from them continuously. Recuperating from security threats can be by many ways such as distinguishing the threats, analyze the attacks, and after that applying reasonable countermeasures against them or giving appropriate stand by solution. Thus, all steps must be carried out lightly putting in mind the security obligations set out as mentioned above. For unexpected threats happen, recouping and mending need re-program underlying elements. For doing as such, recuperating coding instructions should be safely applied to the suitable devices with the end goal to be executed inside them (Stankovic, 2014). Security requirements for network of (Schafer, 2021) can be incorporated to IoT architectures, with objects interconnecting to other entities or applications. Nonetheless, IoT characteristics such as constrained capacity must be taken into account.

Apart from what has already been discussed, data integrity, authentication, confidentiality and availability are the other key security challenges in the IoT, as proposed in the following subsections(Sarhan, 2018; Kocher et al., 2013).

3.2.1 Message Integrity

Message Integrity is refereeing to guarantee that message is not changed at all during its movement in the entire network. In general, inserting any message with extra information can control the underlying packets within entire network. Thusly, prior settling on the basic choice for gathered information, the need arises to verify that sent messaged are begun from the correct sources with no changing. RFID tags based applications utilized in numerous IoTs situations emerge new challenges, since their deployment nature are often unattended and they can't be empowered with abnormal state of intelligence (Juels, 2006). Thus, the stored information in RFID tags memory and RFID tags sending information within network can be altered by adversaries (Atzori et al., 2010). Thus, the need arises to protect stored data by applying programming errors algorithms and other memory protecting algorithms proposed as in (Kumar et al., 2007). To prevent the EPC global Class-1 Generation-2 tags from unauthorized objects, both the memory reading and writing exposure are controlled using passwords. Furthermore, the memory device in this sort of tags is separated into five zones, where each zone can be shielded and protected autonomously from adversary tasks by utilizing passwords process.

Although authenticity necessitates integrity, integrity alone may be necessary to identify and repair failures without authenticity. Routing approaches such as TCP and TLS may be sufficient. Nonetheless, IoT applications, like critical infrastructures, may demand business integrity, which should be included into the architectures as well.

3.2.2 Message Authentication

Data Authentication means to confirm that the IoTs information being sent to a destination node is delivered from a correct source sensor node. Since, the source of data won't have right to guarantee later that the sent information isn't from the source node. Manny efforts have been proposed in literature to deal with such issues. In this context, such issues can be accomplished by applying the well-known Hash Message Authentication Code (HMAC) algorithm (Krawczyk et AL., 1997). The algorithm utilizes the set of sharing security key between the participant parties like cryptographic checksum process that guarantees verification of underlying parties. Using hash function like Message Digest (MD5) or Secure

Hash Algorithm (SHA) is to play out the validation procedure for HMAC algorithm.

3.2.3 Message Confidentiality

Confidentiality of information means to guarantee secure data movement within entire network with the presence of adversary and keep messages from assaults.

An IoT necessitates architectures that can deal with the variety of things. Interconnecting objects may necessitate confidentiality, for example, to prevent confidential information from being eavesdropped during Internet transfer. This need can be met using technologies like IPSec (Kent & Atkinson, 2020) and Transport Layer Security (TLS) (Dierks & Rescorla, 2008). However, complexity may surpass the resource limits of objects, necessitating the development of secure network stacks for IoT (Bonetto et al., 2012).

Since, the IoTs contain a large number of WSNs nodes, it is important to ensure several sensor-related requirements as in (Sarhan, 2018):

- Information captured by such a specific sensor node should not be revealed with its neighboring sensor nodes.
- The need arises to provide a safe channel for communication, as sensor nodes may deal with secured sensitive data such as key distribution, clustered info and neighboring nodes info.
- To provide a secured network against adversaries and various types of traffic analyst attacks, the need arises to apply encrypting messages, keys, and sensor identities.

In order maintain privacy, several methods of network access related to research have been considered and proposed which fix this matter. Reference (Sandhu et AL., 1996) introduced the Role Based Access Control (RBAC) algorithm, role-related authorizations are used to enter specific IoTs devices and software. A function is assigned to each IoTs client and an entity is then generated as member with an acceptable level of authorization and access control. Every user understands precisely which and when to use specific IoTs services as well as administrations in this context. The RBAC offers a significant clear advantage from the IoTs point of view, as its entry gives consent and privileges could be progressively updated at whatever stage there is an adjustment in role assignments. To the best of author's knowledge, incorporating permission control methods, ongoing information stream management frameworks, secure protocols, applying encryption algorithm, and finally key management schemes plans can give an adequate level of secrecy in numerous IoTs scenarios (Miorandi et al., 2012).

For most applications based on IoTs, numerous cases need to update their existing code in sensor nodes either to add new code or to update the existing one with the end goal to address particular issues within the entire network. This updated approach is accomplished by applying the remote re-programming scheme for specific sensor nodes within network (Sarhan, 2018). In conventional systems, information dispersal algorithms are utilized for re-programming. In general, these algorithms broadcast raw information to specific sensor nodes within a particular network without considering any confirmation procedure, here, such case considered as a major security issue. Additionally, using cryptographic techniques cannot provide adequate protection for sensor node members from the inward malevolent adversaries in many cases. Thus, secure re-programming algorithms like Deluge scheme can be utilized to help the nodes to carry out confirmation process per each updated code (Gubbi et AL., 2013). An unattended deployment nature of sensor nodes within the IoTs application make them vulnerable to various sorts of physical threats (Gawdan & Sarhan, 2016; Wang et al., 2004). For a modern building or workplace whereby devices are discovered then by using signal-location schemes to identify the electronic signals. In this way, based on the characteristics of the collection signal, the position of the sensed sensors could be resolved. They will then be physically compromised, such as the use of physical control, the heating device, the bogus hardware on them, damaged, and even robbed. As the sensors are destroyed indefinitely, the damages arising from mechanically corrupted sensor nodes really aren't ready to have been repaired or modified. In addition, the physical compromised node lets opponents access the cryptographic data insider node and change the programming code or even eventually replace a few nodes with various harmful nodes that will also pose a major threat to IoTs applications security (Gawdan et al., 20011a; Kocher & Sarhan, 2017; Alsaadi & Tubaishat, 2015).

3.2.4 Availability

It guarantees that a thing's/service's connection is maintained even if a link fails. As a result, IoT architectures should make connection handover is a feasible case.

3.3 Trust Terminology Issues

In spite of the absence of an agreed definition of trust when used in IoTs world (Daubert et al., 2015), it may possible to state that it is the security policy along with the authorizations that control access processes to available resources (Blaze et AL., 1996)[64]. For that reason the trust mechanisms should guarantee these requirements in IoTs world (Roman et al., 2011):

- Recognizing the IoT's emotional impact on users during the execution for daily routines. The use of IoT software and facilities can even be significantly limited by some error in this understanding. Customers must therefore be able to manage one's own resources and have information at their disposal that explain all their experiences within IoT applications (Roman et al., 2011).
- Minimizing the degree of suspicion among the interacting objects.
- Aiding these objects in choosing a trusted partner for fulfilling their objectives.
- Guaranteeing active and cooperative trust environments for the objects.
- Supporting language for objects which helps building trust dialogue in simplifying dependable strategies along provisions in an easily and effectively manner.

To understand the trust term in IoTs world, it could usually be divided into groups as in the following subsections (Daubert et al., 2015):

3.3.1 Trust for Processing Steps

It means dealing only with significant and accurate information. This can be carried out by using precise data collection, appropriate data analytics, and data build up (Daubert et al., 2015).

3.3.2. Trust for Connection Ways

It means the exchanging of suitable data with only suitable service providers, this type can be achieved by recognizing some facts such as securing data reliability, integrity/validity, and confidentiality (Daubert et al., 2015).

3.3.3 Trust for Systems

In this type, the necessity of the presence of reliable general system is essential. To carry out this goal, presenting transparent workflows, protocols, and the current technology definition has to be provided and explained along its contexts (Daubert et al., 2015).

3.3.4 Trust for Devices

In this type, the communication and cooperation activities will be done among trusted devices and sensors, which can be achieved by using trusted programs and schemes (Daubert et al., 2015). In the IoT, this kind presents a difficulty since a prior device trust cannot always be created, for example, owing to excessive mobility and cross domain interconnections. To create device trust, methods such as trustworthy computing Iliev & Smith, 2005 and computational trust (Jøsang et AL., 2007) are necessary. Furthermore, because each entity assesses trustworthiness in a device differently, IoT designs must cope with non-singular perspectives on trust.

3.3.5 Entity Trust

In the Internet of Things, it refers to the expected activities of users such as people or services. Whilst trusted computing can build device trust, translating such techniques to device trust, like behavioral verification, is more difficult.

3.3.6 Data trust

In the Internet of Things, data comes from a variety of devices, some of which are potentially untrustworthy. As a result, using data aggregation and machine learning approaches, reliable data must be extracted from untrustworthy sources. Also, IoT services create new data by combining several forms of information. A fresh trust assessment, such as using computational trust, is needed for the freshly formed information.

3.3.7 Trust for Negotiation

Trust negotiating that is the credential interchange amongst users and devices which enables trustworthy control activities to also be carried out on resources and reducing misuse is also an important requirement, in addition with the above-mentioned trust categories (Miorandi et AL., 2012). Many current methods and frameworks for trust management are available in the literature. Many confidence qualities, such as honesty, teamwork, and others, are presented in reference (Bao & Chen, 2012). This protocol

requires each unit (node) to explicitly implement the trust detection function for interested devices. In addition, the proposed framework is based on an event-driven mode, therefore it automatically changes trust mechanisms amongst participating entities when a malicious or unwanted interaction event is encountered. In literature, the existing research efforts dealing trust management systems in the field of IoTs environments are fewer in comparison with the protocols. Reference (Chen et al., 2011) proposed trust protection strategy for dealing with IoTs environments focused on fuzzy credibility. This model focuses only on basic Quality of Service (QoS) upon WSNs confidence parameters, including the ratio of arrival packets, the ratio of forwarded packets, and the power consumed by the node.

3.4 Identity Management

Because of the massive number of devices, as well as the complicated interaction between equipment, applications, ownership, and consumers, identity management represents a great difficulty in the IoT (Medaglia & Serbanati, 2010; Suo et al., 2012).

• **Authentication:** In IoT applications, the vast number of devices exceeds the capability of direct authentication, such as when a user uses her service accounts to supply several devices. As a result, techniques for claiming ownership and controlling of a devices are needed.

• **Authorization:** Communications among devices in IoT situations may span several domains. Older authorization systems, such as Kerberos (Steiner et al., 1988), presume that all devices, owners, users, and services are contained inside a single domain. As a result, unified authorization systems that operate with untrusted objects, enable access delegation across domains, as well as provide fast revoking for malfunctioning or malicious equipment are needed.

• **Accountability:** This term guarantees that each activity can be traced back to a verified entity. Due to the widespread usage of devices, services, and data for a multitude of applications, accountability would be a major problem in the IoT. As a result, accountability must work with a wide number of entities, access delegation, cross-domain activities, and data derivation on a regular basis.

3.5 Resilience

The IoT's size in terms of devices combines to offer a wide surface for threats and malfunctions. As a result, the IoT requires resilience and robustness against threats and malfunctions as essential needs.

• **Robustness:** Architectures must enable effective selection of items, transmission routes, and services based on their robustness (failure/attack avoidance).

• **Resilience:** Fail-over and recovery methods must be available to sustain operations in the event of a failure or an attack, as well as to return to regular operations (failure/attack mitigation)

Table 2 shows the link among different IoT properties and security requirements. On the surface, it appears that restricted resources have the strongest relationship in terms of network security, owing to the limitations they impose on traditional security techniques such as encryption. The IoT's heterogeneity has an impact on identity management. As restrictions are placed on the technological choices that may be used, privacy is usually associated with scalability and limited resources. Additionally, the IoT's unpredictable environment and heterogeneity have a significant influence on trust.

Table 2. The influence level of security requirements on internet of things properties: the 'L' indicates low, 'M' indicates medium and 'H' indicates high

Internet of Things Properties	Network Security	Identity Management	Privacy	Trust	Resilience
Uncontrolled Environment	L	L	L	H	L
Heterogeneity	L	M	L	M	L
Scalability	L	L	M	L	H
Constrained Resources	M	L	M	L	L

4. Architectures of Internet of Things

The IoT infrastructure necessitates data management and coordination by establishing a link between physical objects and virtual entities (BETaaS, 2020), ensuring that information travels in a uniform manner. The subsections that follow offer an overview of three well-known ongoing research projects:

4.1 Internet of Things Architecture (IoT-A)

The IoT-A as in (IoT-A, 2021) would be an architectural standard framework that was created as part of an EU FP7 project till 2013 and is still being developed by the community. From business objectives to requirements, this architecture leverages the ideas of views and perspectives to drive the creation of architectural instances. A data view for static structures as well as dynamic data flows, a scalability and performance viewpoint, and even the security and trust viewpoint are examples of these views and perspectives (Bauer & Lange, 2013). IoT-A delivers solutions to fulfill security criteria in the following subsections:

• **Network Security Requirement:** The Key Exchange and Management (KEM) mechanism keeps track of this requirement. This mechanism handles cryptographic keys, which are utilized for confidentiality, integrity, and authenticity. The KEM employs IP Security (IPSec) bridges among (unrestricted) gateway as a well-integrated strategy for optimizing network security coverage across resource - limited equipment. All communications among restricted devices and the gateway, on the other hand, are unsecured. Moreover, throughout the context of network connectivity, the KEM mechanism does not tackle availability.

• **Identity Management Requirement:** This type is handled by 3 layers (modules) in IoT-A. The Identity Management (IM) module focuses on management, although it does not address a specific security requirement. Authentication (AuthN) is a module that includes users and services authentication, along with accountability with non-repudiation. Authorization (AuthZ) is a module that addresses service authorization needs using both Attribute-Based Access Control (ABAC) and Role-Based Access Control (RBAC) (Salinas et al., 2013). Revocation is determined by the access control model in use. To the best of his knowledge, the author of this work is unaware of any specific revocation modules in IoT-A.

• **Privacy Requirement**: Pseudonymisation (PN), a specialized module, tackles privacy by offering pseudonymization for devices, users, and services. Pseudonyms take the role of genuine identities received from KEM, but the identities and pseudonyms are still linked to guarantee accountability. Pseudonyms can also enable unlinkability if a different pseudonym is used for each action. PN, on the other hand, does not tackle complete anonymity and data privacy. AuthZ does, however, give some access granularity which might help with data privacy to some extent.

• **Trust Requirement:** The entity and device trust requirements are handled by Trust & Reputation (TAR) module. This module explains how to gather user reputation in order to determine service trust. However, it does not appear that data trust is handled.

• **Resilience Requirement:** The fault handling paradigm, or functional group, is outlined by IoT-A. Predicting prospective malfunctions, identifying current faults, reducing the impacts of faults, and restoring the system are all requirements and metrics of this model. As a result, the first strategy focuses on prevention, while the next three tackle mitigation over time.

4.2 Building the Environment for the Things as a Service (BeTaaS)

It presents an architecture for the Internet of Things (IoT) and Machine-to-Machine (M2M) interaction that allows applications to operate across a local cloud of gateways. Each BeTaaS instance creates one's own cloud of gateways which seamlessly connects several heterogeneous M2M systems. The Things as a Service (TaaS) reference model (BETaaS, 2021) is the foundation of BeTaaS. Domains, information, communication, security, and functions are all represented through architectural models. BeTaas delivers solutions to fulfill IoT security requirements in the subsections below:

• **Network Security Requirement:** The Key Management component of Network Security connects objects, conducts authentication, manages user requests, and offers encrypted messages. The BeTaaS utilizes a PKI including a Certificate Authority (CA) to handle keys and maintain confidentiality, authenticity, and integrity using secure channels of communication since BeTaaS instances comprises of numerous gateways.

• **Identity Management Requirement:** BeTaaS supports authentication via a specific architectural component for Identity Management. It distinguishes between two types of authentication: gateway level authentication, which occurs when a gateway joins a BeTaaS instance, and application or service level authentication, which occurs when a user interacts with an application. The authentication module in the first example employs key management, but in the second situation, OAuth may be used for authentication and authorization. Authorization is also handled by a distinctive element as in (BETaaS, 2021). The

necessity for accountability is still uncertain.

• **Privacy Requirement:** Although BeTaaS as in (BETaaS, 2020) mentions privacy as a critical component of the security measures, there is no proof that this requirement is achieved. The identity management module handles the control and management of the identities of sensors and gateways, however there is no mention of data anonymity or pseudonymity in such context.

• **Trust Requirement:** The trust and reputation module is in charge of handling the trust requirement. Particular trust features are gathered by the model such as security methods, the Quality of Service (QoS) fulfillment, dependability ability, energy load, and information stability. The ultimate trust value is calculated by aggregating these trust features.

• **Resilience Requirement:** Failure prevention, elimination, tolerance, and prediction are the essential elements that make up the resilience requirement. In reference (BETaaS, 2021), the Failure Analysis Approach component is in charge of identifying possible breakdown causes and developing solutions to successfully address them. On the system's functional items, a method called Failure Modes Effects and Critically Analysis is used.

4.3. Open Source Cloud Solution for the Internet of Things (OpenIoT)

An IoT architecture as in (OpenIoT, 2021) was founded by the EU FP7 OpenIoT research project (2012-2014). The IoT-A specified Architectural Reference Model (ARM) underpins OpenIoT. The fundamental ARM principles and functional building pieces are used. OpenIoT, on the other hand, focuses on offering an internet middleware architecture to enable on-demand connection to the Internet of Things (IoT) services, which might be provided by several service suppliers, such as cloud-based ones. The OpenIoT delivers solutions to fulfill IoT security requirements in the subsections below:

• **Network Security Requirement:** Three modules such as trustworthiness (trust), security, and privacy modules, are described in OpenIoT architectural standard as in (Gwadera, 2021). One sub module of the security module deals with secure messaging, while another deals with authentication and authorization. The public code lacks the privacy features, contrary to the specification. The module of trust assesses the reliability of sensor data input (data trust). To provide protected and encrypted communication, OpenIoT uses the HTTP with TLS protocol. Equipment with constrained capacity, such as Zigbee (IEEE 802.15.4), are also handled in part, with IPSec bridges formed by gateways to assure confidentiality, integrity and authenticity.

• **Identity Management Requirement:** OpenIoT makes use of a central security and privacy module which really leverages OAuth to give authentication and authorization. The RBAC paradigm would be used to handle authorization. Further criteria, such as accountability, are still not achieved.

Regarding the term "security & privacy," it appears that privacy concerns are not resolved.

• **Trust Requirement:** In OpenIoT, the trust module is a stand-alone module. The data and device trust requirements are both covered by the trust module. Records can be annotated with trust labels once device trust has been established. Nevertheless, entity trust is still an unknown.

• **Resilience Requirement:** Instead of focusing on robustness in terms of failure avoidance, OpenIoT focuses on resilience in terms of mitigation.

5. Comparative Security Analysis of IoTs

In general, recent surveys and security evaluations in the field of IoTs security have been published, such as (Al-Garadi et al., 2020; Francesca et al., 2019 ; Krishna et al., 2012; Ammar et al., 2018 ; Sharafi et al., 2021). Reference (Al-Garadi et al., 2020) aims to present a complete assessment of Machine Learning (ML) methods as well as recent developments in Deep Learning (DL) methods that can be applied to develop improved security solutions for IoT systems. The work then goes into the benefits, drawbacks, and advantages of each strategy in detail. The authors of (Francesca et al., 2019) conclude their paper with a rational comparison of the IoT technologies under consideration in terms of a set of eligible security attributes, including access control, integrity, anonymity, confidentiality, privacy, authentication, authorization, resilience, and self-organization. A five-layer and a seven-layer IoT architecture, in addition to the regular three-layer architecture, are provided in reference (Krishna et al., 2012). The communication

standards and the protocols, along with the threats and attacks corresponding to these three architectures, are discussed as well. The authors of (Ammar et al., 2018) look at the security of the most popular IoT frameworks, a total of eight. They explain the planned architecture, the fundamentals of developing third-party smart apps, suitable hardware, and security aspects for each framework. Reference (Sharafi et al., 2021) describes a rapid, resilient, and multilayer-based two-stage identification-authentication system for remote healthcare that uses an electroencephalogram (EEG) signal and fingerprints. Due to the dynamic nature of modified Euclidean distance pattern matching method, it is suggested to match the EEG signal in the identification step.

To the best of my knowledge, comparing security architectures reveals that the same standards are utilized for protecting communications, but different approaches are employed for delivering other security aspects.

The following subsections provide two comparative security analysis such as comparative security analysis of IoTs architectures and comparative security analysis of attacks and countermeasures for OSI of WSNs.

5.1 Comparative Analysis of IoTs Architectures

Based on above mentioned survey, this section compares the security requirements with respect to IoT architectures. The goal of this comparison is to give suggestions for choosing an architecture that meets specific criteria. Moreover, this research identifies security flaws in IoT architectures in general.

Table 3 highlights the study findings on the three IoT architectures as well as the security requirements. In general, it is clear that every architecture has a focal point. The OpenIoT, for example, is best used as an open sensor and service market. Both ToT-A and BeTaaS appear to meet the majority of requirements in a good manner. In general, both IoT-A and BeTaaS architectures are architectural platforms instead of architectures, and even the practical application is left to the developer.

Table 3. Internet of things architectures against security requirements: '✓' indicates satisfied, 'X' not satisfied, and '~' indicates a partial

IoT Security Requirements		**Internet of Things Architectures**		
		IoT-A	**BeTaas**	**OpenIoT**
Privacy	1.Data Privacy	~	X	X
	2.Anonymity	X	X	X
	3.Pseudonymity	✓	X	X
	4.Unlinkability	✓	X	X
Network Security	1.Confidentiality	✓	✓	✓
	2.Integrity	✓	✓	✓
	3.Authenticity	✓	✓	✓
	4.Availability	X	X	X
Trust	1.Device Trust	✓	✓	✓
	2.Entity Trust	✓	X	✓
	3.Data Trust	X	✓	X
Identity Management	1.Authentication	✓	✓	✓
	2.Authorization	✓	✓	✓
	3.Accountability	X	X	X
	4.Revocation	✓	X	X
Resilience	1.Robustness	✓	✓	X
	2.Resilience	✓	✓	✓

5.2 Comparative Analysis of Attacks and Countermeasures for OSI WSNs

Based on my previous published work, this section provides a comparative table of well-known secure routing protocols and their countermeasures to well-known attacks on OSI WSNs within IoTs world as shown in Table 4. More details for this table and its contents have been explained as in my published work (Kocher, 2021).

Table 4. A comparative table of well-known secure routing protocols and their countermeasures to well-known attacks on WSNs: '✓' indicates satisfied and 'X' indicate as not satisfied

Threats	NSKM [47,49] SecTAMP [86]	LKHW [87]	SecLEACH [88]	Ref. KeyChain [89]	EAP [90]	SecRoute [91]	SIGF [92]	TARF [94]	RLEACH [93]	SPINS [95]
Hello Flood	√	x	√	√	√	√	√	√	√	√
Eavesdropping	√	√	√	x	√	√	√	√	√	√
Rout Poisoning	√	√	√	√	x	√	√	x	√	√
Sinkhole	√	x	√	x	√	√	√	√	√	√
Blackhole	√	x	√	x	√	√	√	√	√	√
Grayhole	√	x	√	x	√	√	√	√	√	√
Wormhole	√	x	√	x	x	x	x	√	√	√
Sybil	√	x	x	x	√	√	√	√	√	√
Replay	√	√	√	√	√	√	√	x	√	√
Devic Replication	√	√	√	x	x	√	x	x	x	√
Device Impersonation	√	√	x	x	√	√	x	√	x	√

6. Conclusions, Gaps and Possible Future Works

6.1 Conclusions

This survey systematically reports the state-of-the-art contributions to the security issues for embedded wireless devices in Internet of Things world. In order to truly understand the concept of IoTs world, multiple security issues in WSNs and IoT`s tasks and issues have been recognized and discussed by this work. This study emphasized the IoT's unique properties in comparison to other technology advancements. To develop a common set of security, privacy and trust requirements for IoT technologies, this study compiled a complete list of security requirements based on these properties. Also this survey provides a comparative security analysis of IoTs architectures its embedded devices. Moreover, this research identifies security flaws in IoT architectures in general. Finally, to the best of my knowledge, comparing security architectures reveals that the same standards are utilized for protecting communications, but different approaches are employed for delivering other security aspects. This work is the most comprehensive study of its kind ever published in the field.

6.2 Gaps in IoT Architecture

The security aspects of the three most popular IoT architectures, namely IoT-A, BeTaaS, and OpenIoT, were examined in this study. As all of these architectures appear to meet some of the requirements listed in Table 3, there are a few holes to be filled:

- In very big deployments, access control models like CBAC and RBAC prove difficult to manage and provide needless access owing to a lack of context.
- In the IoT world, the acceptability of privacy and trust measures appears to be restricted. Instead of privacy-enhancing techniques, today's privacy is mostly reliant on fine-grained access control. Finally, for architecture, trust appears to be restricted to one method either cryptographic trust, ratings, or spatial correlation. Evolutionary computing trust methods, on the other hand, are able to combine a variety of distinct trust systems.
- Typically, network security simply handles a portion of data transmission, such as from a gateway to cloud architecture. Nevertheless, data transmission throughout cloud architecture and with resource-constrained equipment, such as IoT devices linked to a gateway, should also be taken into account.
- Many identity management platforms are confined to a single area and do not provide inter- area identity

management skills.

6.3 Possible Future Works

The key weaknesses found in particular places of identity management, privacy, and trust should be addressed, according to this study.

• Identity management: Higher accountability measures are necessary. Digital signatures (non-repudiation) and logs are often used methods. However, because of the digital signatures, such techniques give no privacy protection. This study proposes using methods like blind signatures in conjunction with threshold cryptography as in [85] for a best answer. Digital signatures enable revocable pseudonymity and assure accountability since no one entity may link the signature to an identity. As a result, the requirements for privacy and identity management may very well be matched.

• Privacy: Instead of providing security at only one level, a new framework is required to provide protection at the device, communication, and cloud. Both of anonymity and pseudonymity, for example, should be handled at the device level as soon as allowed to avoid the leaking of confidential information.

• Trust: The technologies under discussion only provide minimal reputation methods. Nevertheless, a true community of trust is necessary to properly fulfill the marketplace idea planned for the IoT. Instead of depending on a single perspective of trust, such a community could contain ideas like transitive trust, as in (if a trusted entity of mine trusts another entity, I also trust this entity).

References

[1]Köhler, M., Wörner, D., & Wortmann, F. (2014). Platforms for the internet of things–an analysis of existing solutions. *In Proceeding of the 5th Bosch Conference on Systems and Software Engineering (BoCSE`14)*, Ludwigsburg, 1-15.

[2]Zanellaa, A., Bui, N., Castellani, A., Vangelista, L., & Zorzi, M. (2014). Internet of things for smart cities. *IEEE Internet of Things Journal (IoT-J)*, 1 (1), 22-32.

[3]Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems*, 29(7), 1645-1660.

[4]National Intelligence Council (NIC) (2008). Disruptive civil technologies: six technologies with potential impacts on us interests out to 2025. Conference Report CR 2008-07, available at https://www.fas.org/irp/nic/.

[5]Bellavista, P., Cardone, G., Corradi, A., & Foschini, L. (2013). Convergence of MANET and WSN in IoT urban scenarios. *IEEE Sensors Journal*, 13(10), 3558-3567.

[6]Tan, L., & Wang, N. (2010). Future internet: The internet of things. *in Proceeding of the 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE)*, 5(15), 376-380.

[7] Vasilomanolakis, E., Daubert, J., Luthra, M., Gazis, V., Wiesmaier, A., & Kikiras, P. (2015). on the security and privacy of internet of things architectures and systems," *in proceeding of 2015 International Workshop on Secure Internet of Things (SIoT),* 49-57, doi: 10.1109/SIOT.2015.9.

[8]Gao, L., & Bai, X. (2014). A unified perspective on the factors influencing consumer acceptance of internet of things technology," *Asia Pacific Journal of Marketing and Logistics*, 26(2), 211–231.

[9]Atamli, A.W., & Martin, A. (2014). Threat-Based security analysis for the internet of things," *IEEE Secure Internet of Things (SIoT),* pp. 35–43.

[10] Babar, S., Mahalle, P., Stango, A., Prasad, N., & Prasad, R. (2010). Proposed security model and threat taxonomy for the Internet of Things (IoT). *in Proceeding of International Conference on Network Security & Applications (CNSA),* 89, 420–429,Springer Berlin Heidelberg.

[11] S. Cirani, G, F. and L. Veltri," Enforcing security mechanisms in the IP-based internet of things: An algorithmic overview," *Algorithms*, vol. 6, no. 2, pp.197–226, 2013.

[12] V. Gazis, C. G. Cordero, E. Vasilomanolakis, P. Kikiras and A. Wiesmaier," Security perspectives for collaborative data acquisition in the internet of things,"*in Proceeding of International Conference on Safety and Security in Internet of Things*, Springer, 2014.

[13] J. Gubbi, R, Buyya, S. Marusic and M. Palaniswami," Internet of Things (IoT): A vision, architectural elements, and future directions,"*Future Generation Computer Systems*, vol. 29, no. 7, pp. 1645–1660, September 2013.

[14] A. Mayzaud, R. Badonnel and I. Chrisment,"Monitoring and security for the Internet of Things," *in Proceeding of International Conference on Autonomous Infrastructure, Management, and Security (AIMS`13)*, vol. 7943, pp. 37–40, 2013.

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

[16] H. Ning, H. Liu, and L. T. Yang," Cyberentity security in the internet of things," *Computer*, vol. 46, no. 4, pp. 46–53, 2013.

[17] R. Roman, P. Najera and J. Lopez," Securing the internet of things," *Computer*, vol. 44, no. 9, pp. 51–58, 2011.

[18] R. H. Weber," Internet of Things – New security and privacy challenges," *Computer Law & Security Review*, vol. 26, no. 1, pp. 23–30, 2010.

[19] D. Bandyopadhyay and J. Sen, "Internet of things: Applications and challenges in technology and standardization", *Wireless Personal Communications*, vol. 58, no. 1, pp. 49-69, 2011.

[20] Q. I. Sarhan, "Internet of things: a survey of challenges and issues," *Int. J. Internet of Things and Cyber-Assurance*, vol.1, no. 1, pp.40–75, **2018**.

[21] Said, O. & Masud, M. 2013 "Towards internet of things: Survey and future vision", *International Journal of Computer Networks (IJCN)*, 5(1), 1-17.

[22] H. Chan and A. Perrig, "Security and privacy in sensor networks", *IEEE Computer*, vol. 36, no.10, pp. 103-105, 2003.

[23] J. Stankovic, "Research directions for the internet of things", *IEEE Internet of Things Journal (IoT-J)*, vol. 1, no.1, pp. 3-9, 2014.

[24] M. Olurin, C. Adams, and L. Logrippo, "Platform for privacy preferences (P3P): Current status and future directions", *in Proceeding of the tenth Annual International Conference on Privacy, Security and Trust (PST),* pp. 217-220, 2012.

[25] R. Roman, P. Najera and J. Lopez, "Securing the internet of things", *IEEE Computer*, vol. 44, no. 9, pp. 51-58, 2011.

[26] G. Broenink, J.-H. Hoepman, C. V. T. Hof, R. V. Kranenburg, D. Smits and T. Wisman, "The Privacy coach: Supporting customer privacy in the Internet of Things", *in proceeding of workshop on What Can Internet Things Do for the Citizen? (CIOT*), Radboud Univversity, pp. 1-10, 2010.

[27] S. Radomirovic, "Towards a model for security and privacy in the internet of things, " *in Proceeding of the 1st International Workshop Security of the Internet of Things (SecIoT)*, Network Information and Computer Security Laboratory, pp. 1-6, 2010.

[28] V. Oleshchuk, "Internet of things and privacy preserving technologies*", in Proceeding of the 1st International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology (VITAE)*, pp. 336-340, 2009.

[29] L. Atzori, A. Iera, and G. Morabito, "The internet of things: a survey", *Computer Networks: The International Journal of Computer and Telecommunication Networking*, vol. 54, no. 15, pp. 2787-2805, 2010.

[30] V. K. Singh, D. S. Kushwaha, S. Singh and S. Sharma, "The Next evolution of the Internet of Things", *International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)*, vol. 2, no. 1, pp. 31-35**, 2015**.

[31] C. Thompson, "25 Ideas for 2010: Digital Forgetting", Wired UK, 2009, available at http://www.wired.co.uk/magazine/archive/2009/12/features/25-ideas-for-2010-digital-forgetting, 2010, accessed in October 2021.

[32] V. Mayer-Schönberger, "Delete: The virtue of forgetting in the digital age", Princeton University Press, 2009.

[33] J. Wickramasuriya, M. Datt, S. Mehrotra and N. Venkatasubramanian, "Privacy protecting data collection in media spaces", *in Proceeding of the 12th annual ACM International Conference on Multimedia*, pp. 1-48, 2004.

[34] C. M. Medaglia and A. Serbanati," An overview of privacy and security issues in the internet of things," in The Internet of Things, pp. 389–395. Springer, 2010.

[35] J. Daubert, A. Wiesmaier and P. Kikiras,"A view on privacy & trust in iot," *in IOT/CPS-Security Workshop, IEEE International Conference on Communications, ICC 2015*, London, GB, pp. 2665-267, IEEE, 2015.

[36] A. Machanavajjhala, D. Kifer, J. Gehrke and M. Venkitasubramaniam," L-diversity: Privacy beyond kanonymity," *TKDD*, vol. 1, no. 1, 2007.

[37] L. Sweeney," k-anonymity: A model for protecting privacy," *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, vol. 10, no. 5, pp. 557–570, 2002.

[38] X. Xiao and Y. Tao," M-invariance: towards privacy preserving re-publication of dynamic datasets," *in Proceeding of Proceedings of the ACM SIGMOD International Conference on Management of Data*, Beijing, China, pp. 689–700. ACM, 2007.

[39] C. Dwork and J. Lei," Differential privacy and robust statistics," in Proceedings of the 41st Annual ACM Symposium on Theory of Computing, STOC 2009, Bethesda, MD, USA, pp. 371–380. ACM, 2009.

[40] A. Pfitzmann and M. Kohntopp," Anonymity, unobservability, and pseudonymity - A proposal for terminology," *in Proceeding of Designing Privacy Enhancing Technologies, International Workshop on Design Issues in Anonymity and Unobservability,* Berkeley, CA, USA, Proceedings, vol. 2009 of Lecture Notes in Computer Science, pp. 1–9. Springer, 2000.

[41] Camenisch, J. & and E. V. Herreweghen, E. V. 2002. Design and implementation of the idemix anonymous credential system. *in Proceedings of the 9th ACM Conference on Computer and Communications Security(CCS 2002)*, Washington, DC, USA, pp. 21–30. ACM.

[42] R. Dingledine, N. Mathewson and P. F. Syverson,"Tor: The second generation onion router," in Proceedings of the 13th USENIX Security Symposium San Diego, CA, USA, pp. 303–320, USENIX, 2004.

[43] I. S. Kocher, C-O. Chow, H. Ishii and T. A. Zia," Threat models and security issues in wireless sensor networks," *International Journal of Computer Theory and Engineering*, vol. 5, no. 5, 2013**.**

[44] T. A. Zia and A. Y. Zomaya, "Security issues in wireless sensor networks," *in Proceeding of the International Conference on Systems and Networks (ICSNC*), Tahiti, French Polynesia, 2006.

[45] K. Zhao and L. Ge, "A survey on the internet of things security, "in *Proceeding of the Ninth International Conference on Computational Intelligence and Security (ICCIS),* pp. 663–667, 2013.

[46] I. S. Kocher, "Software engineering methods to improve the design of software reliability systems: roadmap, "*Journal of Southwest Jiaotong University*, vol. 55, no. 3, pp. 1-9, **2020,**

[47] I. Gawdan and Q. I. Sarhan," Performance evaluation of novel secure key management scheme over ban wireless sensor networks," *Journal of University of Duhok*, vol. 19, No. 1, pp. 179-188, **2016**.

[48] I. S. Gawdan, C.-O. Chow, T. A. Zia and Q. I. Gawdan," Cross-layer based security solutions for wireless sensor networks," *International Journal of the Physical Sciences (IJPS),* vol. 6, no. 17, pp. 4245-4254, 2011a.

[49] I. S. Gawdan, C.-O. Chow, T. A. Zia and Q. I. Sarhan,"A novel secure key management module for hierarchical clustering wireless sensor networks," *in Proceeding of 3rd International Conference on Computational Intelligence, Modeling and Simulation (CIMSim 2011)*, Langkawi, Malaysia, pp. 312-316, 2011b.

[50] I. S. Kocher and Q. I. Sarhan,"Classifying routing algorithms upon clustered based wireless sensor networks: a survey," *ZANCO Journal of Pure and Applied Science (ZJPAS)*, vol. 29, no. 2, pp. 25-36, 2017.

[51] I. S. Kocher,"A systematical roadmap on various security vulnerabilities and countermeasures in routing algorithms upon wsns," *Academic Journal of Nawroz University (AJNU)*, vol. 10, no.4, 2021.

[52] G. Schafer,"Security in fixed and wireless networks – an introduction to securing data communications," Wiley, 2003, accessed in October 2021

[53] A. Juels, "RFID security and privacy: a research survey," *IEEE Journal on Selected Areas in Communications (J-SAC*), vol. 24, no. 2, pp.381–394, 2006.

[54] R. Kumar, E. Kohler and M. Srivastava, "Harbor: software-based memory protection for sensor nodes, "*The 6th International Symposium on Information Processing in Sensor Networks (IPSN),* pp.340–349, 2007.

[55] H. Krawczyk, M. Bellare and R. Canetti, "HMAC: keyed-hashing for message authentication," IETF RFC 2104, 1997.

[56] S. Kent and R. Atkinson. Security Architecture for the Internet Protocol. RFC 2401 (Proposed Standard), November 1998, Obsoleted by RFC 4301, updated by RFC 3168, accessed in October 2020.

[57] T. Dierks and E. Rescorla.,"The transport layer security (TLS) protocol version 1.2.," RFC 5246 (Proposed Standard), August 2008, Updated by RFCs 5746, 5878, 6176. 2008.

[58] R. Bonetto, N. Bui, V. Lakkundi, A. Olivereau, A. Serbanati, and M. Rossi,"Secure communication for smart IoT objects: Protocol stacks, use cases and practical examples," *in 2012 IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks, WoWMoM 2012 - Digital Proceedings*, 2012.

[59] R. Sandhu, E. Coyne, H. Feinstein and C. Youman, "Role-based access control models," *IEEE Computer*, vol. 29, no. 2, pp.38–47, 1996.

[60] D. Miorandi, S. Sicari, F. De PellegriniI and I. Chlamtac, "Internet of things: vision, applications and research challenges, "*Ad Hoc Networks,* vol. 10, no. 7, pp.1497–1516, 2012.

[61] X. Wang, W. Gu, K. Schosek, S. Chellappan and D. Xuan, "Sensor network configuration under physical attacks, "Technical Report (OSU-CISRC-7/04-TR45), Department of Computer Science and Engineering, Ohio State University, Ohio, USA, 2004.

[62] E. Alsaadi and A. Tubaishat, "Internet of things: features, challenges, and vulnerabilities," *IJACSIT,* vol. 4, no. 1, pp.1–13, 2015.

[63] Daubert, J., Wiesmaier, A. & Kikiras, P. 2015. A view on privacy & trust in IoT, "The *IEEE (ICCW)*, 2665–2670.

[64] M. Blaze, J. Feigenbaum and J. Lacy, "Decentralized trust Management, "IEEE Symposium on Security and Privacy, pp.164–173, 1996.

[65] A. Iliev and S. W. Smith,"Protecting client privacy with trusted computing at the server. *IEEE Security & Privacy*, vol. 3, no. 2, pp. 20–28, 2005.

[66] A. Jøsang, R. Ismail, and C. Boyd," A survey of trust and reputation systems for online service provision. *Decision Support Systems,* vol. 43, no. 2, pp. 618–644, 2007.

[67] F. Bao and I.R. Chen, "Trust management for the internet of things and its application to service composition," *in Proceeding of the IEEE International Symposium (WoWMoM)*, pp.1–6, 2012.

[68] D. Chen, G. Chang, D. Sun, J. Li, J. Jia and X. Wang, "TRM-IoT: a trust management model based on fuzzy reputation for internet of Things," *ComSIS* 11, vol. 8, no. 4, pp.1207–1228, 2011.

[69] H. Suo, J. Wan, C. Zou, and J. Liu,"Security in the internet of things: a review," *in Proceeding of Computer Science and Electronics Engineering (ICCSEE), International Conference*, vol. 3, pp. 648–651. IEEE, 2012.

[70] J. G. Steiner, B. C. Neuman and I. J. chiller,"Kerberos: An authentication service for open network systems," *in Proceedings of the USENIX Winter Conference,* Dallas, Texas, USA, pp. 191–202. USENIX Association, 1988.

[71] BETaaS Consortium," Building the environment for the things as a *service," http://www.betaas.eu/, 2012, accessed in 11. Feb. 2020.*

[72] IoT-A Consortium," IoT-A – Internet of Things Architecture," http: //www.iot-a.eu/, accessed in May 2021

[73] M. Bauer and S. Lange," Enabling things to talk," *Springer Berlin Heidelberg*, Berlin, Heidelberg, 2013.

[74] A. Salinas, Y. Ben-Saied and D. Level," Internet of things architecture concepts and solutions for privacy and security in the resolution infrastructure," (257521), 2013.

[75] BETaaS Consortium," D1.4.2 – TaaS Reference Model," http://www.betaas.eu/docs/deliverables/BETaaS%20-%20D1.4.2%.20 %20TaaS%20Reference% 20Model%20v1.0.pdf, October 2013, accessed in 11 Mar. 2014, accessed in October 2021.

[76] BETaaS Consortium,"BETaaS building the environment for the things as a service D2. 2. 2 – Specification of the extended capabilities of the platform, pp. 1–61, 2014, accessed in October 2021

[77] OpenIoT Consortium," OPENIoT D2.3 Detailed Architecture and Proof-of-Concept Specifications," http://openiot.eu/?q=node/49, 2013. Accessed in October 2021.

[78] OpenIoT Consortium," OPENIoT project description," http://www.openiot.eu/, 2013. accessed in October 2021

[79] R. Gwadera," D5.2.1 Privacy and security framework. 2013, accessed in October 2021.

[80] M. A. Al-Garadi, A. Mohamed, A. K. Al-Ali, X. Du, I. Ali and M. Guizani, "A Survey of Machine and Deep Learning Methods for Internet of Things (IoT) Security," in IEEE Communications Surveys & Tutorials, vol. 22, no. 3, pp. 1646-1685, **2020**, doi: 10.1109/COMST.2020.2988293.

[81] Francesca Meneghello, Matteo Calore, Daniel Zucchetto, Michele Polese and Andrea Zanella," IoT: Internet of Threats? A Survey of Practical Security Vulnerabilities in Real IoT Devices," IEEE Internet of Things Journal, vol. 6, no. 5, pp. 8182-8201, **2019**.

[82] Krishna RR, Priyadarshini A, Jha AV, Appasani B, Srinivasulu A and Bizon N," State-of-the-Art Review on IoT Threats and Attacks: Taxonomy, Challenges and Solutions. Sustainability**.** 13(16):9463, **2021**, https://doi.org/10.3390/su13169463.

[83] Ammar M, Russello G and Crispo B," Internet of Things: A survey on the security of IoT frameworks[J]. Journal of Information Security and Applications, vol.38, pp. 8-27, **2018**.

[84] Sharafi Afsaneh, Adabi Sepideh, Movaghar Ali and Al-Majeed Salah," A two-layer attack-robust protocol for IoT healthcare securityTwo-stage identification-authentication protocol for IoT," IET Communications, vol 15, no. 19, pp. 2390-2406, 7 September **2021.**

[85] D. Chaum," Blind signatures for untraceable payments," *in Proceedings of CRYPTO '82*, Santa Barbara, California, USA, pp. 199–203. Plenum Press, New York, 1982.

[86] Pecho, P., Nagy, J., Hanacke, P. & Drahansky, M. 2009 . Secure collection tree protocol for tamper-resistant wireless sensors. *Communications in Computer and Information Science*, 58, 217– 224, Springer-Verlag, Heidelberg, Germany.

[87] R. D. Pietro, L. V. Mancini, Y. W. Law, S. Etalle and P. Havinga, " LKHW: a directed diffusion-based secure multi-cast scheme for WSNs. ICPPW'03, pp. 397-406, IEEE Computer Society Press, 2003.

[88] Y-J. Han, M-W. Park and T-M. Chung, "SecDEACH: secure and resilient dynamic clustering protocol preserving data privacy in WSNs, "*in Proceedings of ICCSA'10*, pp. 142 – 157, 2010.

[89] D. Liu and P. Ning, "Efficient distribution of key chain commitments for broadcast authentication in distributed sensor networks, "*in Proceedings of the 10th Annual Network and Distributed System Security Symposium*, pp. 263 – 273, San Diego, CA, USA, 2003.

[90] S. Zhu, S. Setia and S. Jajodia, "LEAP: efficient security mechanism for large-scale distributed sensor networks, "*in Proceedings of the 10th ACM Conference on Computer and Communications Security*, pp. 62 – 72, New York, USA, ACM Press, 2004.

[91] J. Sen and A. Ukil,"A secure routing protocol for wireless sensor networks," *in Proceedings of* ICCSA'10, pp. 277 – 290, Fukuaka, Japan, 2010.

[92] A. D. Wood, L. Fang, J. A. Stankovic and T. He, "SIGF: a family of configurable, secure routing protocols for wireless sensor networks, "*in Proceedings of the 4th ACM Workshop on Security of Ad Hoc and Sensor Networks*, pp. 35 – 48, Alexandria, VA, USA, 2006.

[93] K. Zhang and C. Wang,"A secure routing protocol for cluster-based wireless sensor networks using group key management," *in Proceedings of WiCOM'08*, pp. 1-5, Dalian, 2008.

[94] G. Zhan W. Shi and J. Deng," TARF: a trust-aware routing framework for wireless sensor networks," *in Proceedings of EWSN'10*, pp. 65 – 80, Coimbra, Portugal.2010.

[95] Perrig, A., Szewczyk, R., Wen, V., Culler, D.E., & Tygar, J.D. (2002). SPINS: security protocols for sensor networks. *Wireless Networks*, 8 (5), 521-534.

[96] Wood, A.D., & Stankvic, J.A. (2002). Denial of service in sensor networks," *IEEE Computer*, 35(10), 54-62.

[97] Karlof, C., & Wagner, D. (2003). Secure routing in wireless sensor networks: attacks and countermeasures, "*in Proceedings of the 1st IEEE International Workshop on Sensor Network Protocols and Applications,* pp. 113-127.

[98] Deng, H., Li, H., & Agrawal, D. (2002). Routing security in wireless ad hoc networks. *IEEE Communications Magazine*, 40 (10), 70-75. DOI: 10.1109/MCOM.2002.1039859.

[99] Chandra, S.J., Harihara, S.G., Reddy, H., & Balamuralidhar, P. (2007). A mechanism for detection of grayhole attack in mobile ad hoc networks. *in Proceedings of the 6th International Conference on Information, Communication, and Signal Processing (ICICS'07)*, 1 – 5, Singapore.

[100] Newsome, J., Shi, E., Song, D., & Perrig, A. (2004). The Sybil attack in sensor networks: analysis and defenses. *in Proceedings of the 3rd International Symposium on Information Processing in Sensor Networks*, pp. 259-268, ACM Press.

[101] Kocher, I.S. (2021). An experimental simulation of addressing auto-configuration issues for wireless sensor networks. *CMC-Computers, Materials and Continua*, 71(2), 3821-3838. DOI:10.32604/cmc.2022.023478.

[102] Syeda, G.F., Syed, A.S., & Mohammed, S. (2018). Efficient Defense system for jamming attacks in wireless sensor networks," *in International Journal of Electronics and Communication Engineering and Technology*, 9 (4), 22–35. Manuscript ID:-00000-42994.