CAPITAL UNIVERSITY OF SCIENCE AND TECHNOLOGY, ISLAMABAD

A Comprehensive Ontology of Information Disruption Attacks for IoT based Health Care Systems

by

Rizwana Jamshed

A thesis submitted in partial fulfillment for the degree of Master of Science

in the

Faculty of Computing
Department of Computer Science

2021

This research is proudly deditaced to all my beloved family (my mother, my father, my brother all my friends). Thank you for your constant compassion, encouragement, sacrifices, guidance and support.

CERTIFICATE OF APPROVAL

A Comprehensive Ontology of Information Disruption Attacks for IoT based Health Care Systems

by

Rizwana Jamshed

(MCS191031)

THESIS EXAMINING COMMITTEE

S. No.	Examiner	Name	Organization
(a)	External Examiner	Dr.Tariq Ali	UIIT, PMAS Rawalpindi
(b)	Internal Examiner	Dr.Aamer Nadeem	CUST, Islamabad
(c)	Supervisor	Dr.Qamar Mahmood	CUST, Islamabad

Dr. Qamar Mahmood
Thesis Supervisor
April, 2021

Dr. Nayyer Masood
Head
Dept. of Computer Science
April, 2021

Dr. Muhammad Abdul Qadir
Dean
Faculty of Computing
April, 2021

Author's Declaration

I, **Rizwana Jamshed** hereby state that my MS thesis titled "**A Comprehensive Ontology of Information Disruption Attacks for IoT based Health Care Systems**" is my own work and has not been submitted previously by me for taking any degree from Capital University of Science and Technology, Islamabad or anywhere else in the country/abroad.

At any time if my statement is found to be incorrect even after my graduation, the University has the right to withdraw my MS Degree.

(Rizwana Jamshed)
Registration No: MCS191031

Plagiarism Undertaking

I solemnly declare that research work presented in this thesis titled "**A Comprehensive Ontology of Information Disruption Attacks for IoT based Health Care Systems**" is solely my research work with no significant contribution from any other person. Small contribution/help wherever taken has been duly acknowledged and that complete thesis has been written by me.

I understand the zero tolerance policy of the HEC and Capital University of Science and Technology towards plagiarism. Therefore, I as an author of the above titled thesis declare that no portion of my thesis has been plagiarized and any material used as reference is properly referred/cited.

I undertake that if I am found guilty of any formal plagiarism in the above titled thesis even after award of MS Degree, the University reserves the right to withdraw/revoke my MS degree and that HEC and the University have the right to publish my name on the HEC/University website on which names of students are placed who submitted plagiarized work.

(Rizwana Jamshed)
Registration No: MCS191031

Acknowledgement

I would like to thank the Most Merciful and Most Beneficent of **Allah** the Almighty, who has bestowed upon me the talents, wisdom and eternity of my efforts to arrive here and to accomplish my study goal. I am very thankful to **Dr. Qamar Mahmood**, supervisor of my research thesis, who directed me to complete my research thesis.

(Rizwana Jamshed)

Abstract

A large number of research papers related to the IoT attacks based on healthcare system are published on a regular basis. Authors of different research paper concentrated only on a certain number of attacks related to IoT based healthcare system. The number of attacks is dispersed in various research papers. There was no comprehensive classification available for these IoT attacks. One of the solutions for this problem can be the development of a comprehensive ontology for IoT attacks. We have developed a comprehensive ontology to solve this problem. In our proposed ontology, we gathered information related to information disruptions IoT based attacks from different research papers. This ontology has been conceptualized on the basis of acquired knowledge and implemented using protégé. This ontology is evaluated according to standard evaluation criteria which are completeness, consistency and accuracy. The result of this evaluation is based on user evaluation method and tool evaluation method. This ontology will be improvised by the feedback from community.

Contents

List of Figures

List of Tables

Abbreviations

DDoS	Distributed Denial of Services
DoS	Denial of Services
DNS/NTP	Domain Name Service/Network Time Protocol
DHCP	Dynamic Host Configuration Protocol
FMS	Fluhrer, Mantin and Shamir
IDS	Intrusion Detection System
IoT	Internet of Things
ITU	International Telecommunication Unit
M2M	Machine to Machine
ML/DL	Machine learning/Deep learning
PTW	Pychkine,Tews,Weinmann
RFID	Radio Frequency Identification
RPL	Routing Protocol for Low
SOA	Service Oriented Architecture
TCP/UDP	Transmission Control Protocol/User Datagram Protocol
TLS	Transport Layer Security
WSN	Wireless Sensor Network
XSS	Cross-Site Scripting

Chapter 1

Introduction

1.1 Background

The Internet of Things (IoT) [1] is a term which mean connected collection of anyone, anything, anytime, anyplace, any service, and any network. Kevin Ashton [2] first used the word Internet of Things (IoT) as a concept in 1999. In 2005, the International Telecommunication Union (ITU) issued an annual report on 'Internet of Things' [3]. According to the ITU study, RFID and intelligent computing technologies have brought a new age of global interconnection. As IoT is becoming common in different fields of life, one of the most important accomplishments of IoT is in the medical sector. One of the most appealing IoT technology fields is clinical consideration and medical treatment. The IoT has the ability to build many medical applications, such as remote monitoring of healthcare, fitness applications, chronic diseases, and caring for the elderly [4]. Therefore, it is possible to see various clinical devices, sensors, and imaging devices as a smart device or objects that form a central part of the IoT. An important factor is the flexibility of cost effective interactions across individual patients, hospitals, and healthcare organizations through smooth and safe connectivity [5]. In order to improve IoT based healthcare services, it is important to minimize costs, improve the quality of life and enhance the experience of the customer.

According to our observation, we have not found comprehensive classification of IoT attacks in healthcare domain. At that time, some of the approaches were used which are based on RFID [6],[7]. Now a days these approaches are rarely used in the healthcare domain. RFID systems [8] are vulnerable to a wide variety of malicious attacks. Wired networks (WSN) [9],[10],[11],[12],[13],[14],[15], where computer systems usually have both centralized and host-based protection (e.g. Firewalls). RFID readers and RFID tags operate in an inherently unstable and potentially noisy environment. Several researchers have concentrated on this since 2012 [6],[12]. They focus only on a certain number of attacks in each research paper. The numbers of IoT attacks related to the healthcare domain are scattered in numerous research papers. There was no comprehensive classification/ontology available for these attacks. The ontology[16] is designed to be efficient in order to make classification easier and more accurate. The ontology is being generated using a knowledge-driven approach [17] to capture the majority of the key concepts and their relationships in the IoT domain. New researchers need to gather all those research papers which is relevant to the IoT based healthcare attacks to find out the pros and cons of this area from a healthcare point of view.

1.2 Motivation

The Internet is the core of IoT. With the rapid development in IoT a lot of IoT devices in medical field invented. IoT devices includes almost all the attacks that lie within the Internet also falls in IoT. The fast development and wider adoption of IoT devices in our lives increase the need of addressing these attacks and their countermeasure before deployment. Several scholars suggest a classification [2], [12], [13], [14], [18], method in which they attempt to cover a particular feature of the health care system in IoT domain. There is no comprehensive ontology from which the research community will gain benefits because the classification in the research paper focuses on some particular aspect. Conceptualizing all these attacks in one classification would give the reader or researcher a detailed summary of the attacks.

1.3 Problem Statement

Attacks on the IoT healthcare domain are very important, but if researchers want to know what kind of attack or hierarchy is, there is no comprehensive hierarchy/ontology for future researchers. Our research work is based on a classification of IoT attacks in healthcare domain and prepare one comprehensive ontology which contains almost all attacks that occur on IoT.

1.4 Research Questions

From this problem statement some research questions have been raised.

1. Why the information disruption attacks related to IoT are more critical / dangerous?
2. Does there any taxonomy/classification exist which have modeled IoT attacks?
3. Is there any comprehensive classification/ontology available for IoT attack?
4. Is comprehensive ontology being developed?
5. Is comprehensive ontology being evaluated?

1.5 Research Methodology

Brief Research Methodology of our research is discussed below:

1. Different research papers were explored and downloaded by different citation indexers (ACM etc.).
2. Selection of research papers in the IoT domain that involve information disruption attacks.

3. Research various classifications relevant to the attacks on information disruption and find the frequency of occurrences.

4. Summarize number of attacks in tabular format.

5. Graphical representation of these attacks.

6. Hierarchy of these attacks in which we classify these attacks from base class.

7. Develop an ontology for classification of attacks in protégé.

8. Evaluate our ontology using standard evaluation methods and then we will publish this ontology to get feedback from the community.

The first 3 research methods will answer our first 2 research questions. The remaining steps will answer our 3 research questions, which are 3, 4, 5.

1.6 Thesis Organization

This thesis is organized in the following chapters. Chapter 2 surveys existing classification related to IoT based healthcare system. It is further divided into sub parts in which classification in different surveyed techniques has been discussed. This chapter will answer our 1st, 2nd and 3rd research question. Proposed ontology has been discussed in chapter 3 which is divided into three steps such as knowledge acquisition, conceptualization and implementation. Ontology evaluation is explained in Chapter 4. Chapter 3 and 4 will answer our 4th and 5th research question.

Chapter 2

Literature Review

This chapter discusses the research work on the bases of the existing classification related to IoT base healthcare system. We have divided this chapter into the three sections. Section 2.1 shows the survey of IoT attacks. Section 2.2 shows the classifications in different surveyed techniques. Section 2.3 concludes this chapter.

2.1 Survey of IoT Attacks

IoT has a variety of application domains such as retail, industrial, smart infrastructure, etc. There were twenty papers in which classification of healthcare system based on IoT attacks were discussed, ten papers were related to general IoT domain and its attacks, remaining papers were related to RFID and WSN [11],[12],[13],[14],[15],[19],[20].

One of IoT domains is the healthcare system. From the healthcare point of view, the author [5] focuses on some specific parameters such as protection and privacy features, security requirement, threat models, and attack taxonomies. To mitigate security risk, they proposed an intelligent collaborative security model. The strategies explored in this paper are how various technologies can be leveraged in a healthcare context, such as big data, ambient intelligence, and wearable. The

author also discusses several IoT and eHealth policies and regulations worldwide. This also poses a lot of obstacles that are still available for future researchers.

Since IoT uses a network architecture which is close to traditional network architecture for interaction between different machines. Vulnerabilities of traditional network architecture are inherited into IoT network as well. Different vulnerabilities are found when research takes place in the area of the Internet of Things (IoT), which will hold IoT at risk. As a consequence, there are too many IoT attacks that were invented before actual product deployed. The author [2] addresses the frequency of various IoT attacks, also describes them and their countermeasures and considers the most noticeable attacks in IoT. These attacks are based on various categories. At least one attack is discussed from each category which is the most dangerous of all those particular attacks. There is still no final solution to these attacks. Efficient and safe solutions are still needed.

IoT based healthcare and their infrastructure are vulnerable to a number of major security threats and malicious activity. In terms of methodologies, motivations and implications, IoT based healthcare suffers from many security challenges that differ from other domains due to the difficulty of the environment and the design of devices deployed. The most recent security issues for the IoT based healthcare system are addressed in [3]. This paper includes the classification related to IoT based healthcare Infrastructure. It focused on three layers (Application layer attack, Network layer attack, Perception layer attack). There is still a need for future work to protect patient safety data, linked medical devices within critical healthcare infrastructure.

In terms of comfort and efficiency, one of the aims of smart environments is to enhance the quality of human life. In any real-world smart environment based on the IoT model, confidentiality and privacy are key issues. Vulnerabilities in IoT based systems generate security threats that affect applications in smart environments. Intrusion detection systems (IDSs) designed for IoT environments are therefore a critical need. However, this IDS has limitations and, because of this, author presents a detailed survey of the latest IDSs intended for the IoT model,

concentrating on the required methods, features and mechanisms [21]. The author gave some suggestions that should be taken into consideration when developing an IDS for an IoT. There is the need for an efficient, lightweight framework with an effective placement strategy that does not adversely affect the IoT environment's integrity, confidentiality, and availability.

Without proper consideration of the deep security objectives and challenges involved, IoT has been quickly established over the past decade. The author [4] discusses IoT's security goals and objectives and then presents a new classification of various forms of security and privacy threats and their countermeasures. The author captures a wide variety of security vulnerabilities in IoT systems and attacks. The author claims that their classification is unique as compared to other classifications as it has four distinct classes: Physical, Network, Software and Encryption attacks. IoT is implemented by means of similar current network technologies (Wireless Sensor Network, Networks, RFIDs, the Internet and so on). The author also highlighted the required security countermeasures which is needed for successfully secure IoT system and its future direction is also discussed.

The author [22] proposes several IoT security issues that occur in the three-layer system structure and offer its solutions. However, IoT as a large framework involves the integration of many layers. Many security issues arise as a result of System Integration, so there are many security issues that aren't exclusive to any one layer, such as privacy protection. In the IoT based healthcare system privacy and security in each layer is a big issue. They concentrated and expanded in depth only on perception layer. They are intended to use combined technologies in the IoT environment to solve the security issue.

Since IoT provides organizations with a huge business value and creates opportunities for many existing applications such as energy, healthcare and other sectors. It also suffers from a variety of security problems that, as opposed to other fields, are the most challenging. In [23] author offers a detailed top down survey of the most recent IoT security and privacy solution in term of flexibility and scalability. The author also addresses new approaches to IoT protection and privacy in terms

of flexibility and scalability, such as blockchain and Software Defined Networking (SDN).

Since IoT's significant growth is a new technological paradigm that may include security-critical operations and putting online of sensitive data, its security aspect is important. The author discusses the issues of network protection in the domain of smart home, healthcare and transportation. During operation, it is likely that the interruption may occur in IoT devices that cause them to be in shutdown mode. Security attack taxonomy within IoT networks is designed to help IoT developers become more aware of the possibility of security vulnerabilities in order to implement better defences. The author [24] also addresses attacks on five layers, namely physical, data link, network, transport and application layer. These taxonomies are intended to help potential developers discover their safety measures.

In [25], the author focuses on all IoT security issues and all the challenges. The author also focuses on the design of three layers, i.e. perception, transport and application layer. They evaluate each layer and try to find their solution and their security issue. They also evaluate in depth the cross-layer heterogeneous integration problems and according to author safety concerns and lightweight security solutions are effective for them.

As the digital world is rising day by day, so is cyber crime in the healthcare system centered on IoT. In [26] author analysis IoT-enabled cyber-attacks, found in all application domains since 2010. They concentrated on recent and verified attacks based on incidents in the real world and proof-of-concept attacks.

The Internet of Things (IoT) has tremendous safety risks with patient health tracking sensors. Advanced security and privacy threats, including data breaching, data integrity, and data collusion, are also its main concerns. In [27] the author studies privacy and security issues regarding the data acquisition and then transmission of healthcare data. They suggest a four-layer system which are IoT network sensors/devices, Fog layers, the layer of cloud computing, and the layer of healthcare providers. They present an algorithm then run on a special platform that indicates

that when applied to attacks, this method can be effective in terms of frequency, energy cost, and overall computing cost, but its detailed implementation is still in progress.

The author focuses on ever changing IoT vulnerabilities in [28]. They include a unique taxonomy that sheds light on IoT vulnerabilities, their attack vectors, impacts on various security goals, vulnerability-exploiting attacks, effective remediation methodologies, and operational cyber security capabilities currently provided to detect and track such weaknesses.

The Internet of Things (IoT) connects billions of smart devices that, with minimal human interference, can interact with each other. IoT, with an estimated 50 billion devices by the end of 2020 is one of the fastest growing areas in the history of computing. Since ML/DL plays a vital role in transforming IoT system security between communication and security-based intelligence systems. A detailed survey of ML methods and recent developments in DL methods is given in [29] by the authors, which can be used to establish improved security methods for IoT systems. Authors often address opportunities and problems in it that can serve as possible future studies.

Networks with a non-wired infrastructure and dynamic topology are like wireless sensor networks. Each layer in the OSI model is vulnerable to multiple attacks, stopping a network's performance. In [13] authors address multiple attacks on four layers of the OSI model and their protection mechanism on how to avoid network layer attacks, but the key focus is a wormhole attack as the most dangerous wireless network attack. The authors also recommend the method of promiscuous mode to detect and isolate the malicious node during wormhole attacks.

Due to the tremendous amount of applications, the wireless sensor network (WSN) has become the research field of today's worlds. WSN has been very common in the research field since 2015, so there is a lot of work done on it as well as a lot of security problems arise. In [9] author presents various types of attacks encountered during transmission or communication over the network of wireless sensors and gives some ideas to resolve these attacks. These attacks are divided

into two categories: active attacks and passive attacks. The author explains just how these attacks are carried out and what their countermeasures are to help future scholars.

The type of interaction we see now is either human-human or human-device. Human-human needs alot of resources while human-device needs alot of parameters to keep in view. The IoT promises a great future for the internet where the communication is based on machine-machine (M2M). It is cost effective, and gives alot of oppurtunites in IoT field. In [30] author provides the IoT scenario which is comprehensively summarized and its supporting technologies and sensor networks are reviewed. IoT is defined as a six layered architecture by the author. They just addressed certain WSN-related problems. Research is still being carried out for its wide-range acceptance, however, it is highly doubtful that it would be an omnipresent application without resolving the obstacles in its creation and providing user privacy and security confidentiality. IoT implementation requires exhausting efforts to resolve and present solutions to threats to its security and privacy.

The Internet of Things (IoT) and cloud computing have exposed devices to vulnerabilities. The increased deployment of IoT devices in the healthcare system renders patient information subject to malicious attacks centered on the IoT devices, protection and privacy. Although such security issues have been discussed by several researchers in IoT, there is an unfortunate lack of a systematic review of IoT's security issues for eHealth. In [31] author performs a detailed IoT security vulnerability review. They propose a solution of using distributed security architecture in both devices and cloud application layers. Cloud computing provides numerous other services that are booming in IoT based telemedicine practices around the world. A lot of security problem arises in it. If security problems are not addressed, practical adoption of telemedicine in the cloud can be greatly disrupted. The author [32] describes possible attacks that can be carried out on the cloud. In the cyber industry, the Intrusion Detection System (IDS) is quite a good solution for tackling these attacks. To achieve great results, they use multiple algorithms like RandomForest, J48 etc., but future work involves proposing an effective security solution using IDS as a defender for cloud environments.

A generic interpretation of IoT is that in several domains it provides multiple facilities, using typical internet infrastructure by allowing various communication patterns such as human-to-object, object-to-object. In terms of computing power, memory and bandwidth, IoT objects have their own limitations. Therefore, IoT vision has suffered from unparalleled attacks targeting not only people but also businesses. Some instances of these attacks are loss of privacy, organized crime, mental illness, and the likelihood of endangering human lives. The author [18] proposes a new four-layered IoT reference model based on the strategy of building blocks, in which a detailed IoT attack model consisting of four main phases is created. It will allow the prospective investigator to create a better approach to these attacks.

In today's emerging environment, all devices are getting smarter and can also connect with other devices. Due to heterogeneity existence, it also has to face certain difficulties in securing overall privacy. The author [33] proposes several forms of DDoS-focused vulnerability. It requires mechanisms to avoid such an attack that can detect and prevent it from attacking, but it has limited power capacity due to small devices. So the process must be added at the entrance of the network. They only address common attacks on DDoS so that it can be useful to potential researchers when developing their countermeasure.

Cyber security has to contend with a wide range of potential threats, appearing at a higher number every day. Therefore, evaluation of future attacks and risks is critical. As the domain information is complicated and quickly expanding, ontology can be helpful in integrating and sharing the knowledge needed for cyber security assessment and for prioritized countermeasures. In [34] author model known attacks and it's products with an ontology that is capable of providing a full understanding of threats, but flexible to add new threats and reason what threats are important to a particular IoT configuration. Evaluation of ontology is important which is its future phase and many researcher are working on it.

The IoT is the new subject of analysis and the security problems are a more powerful aspect, too. The author [35] concentrated on devices that are not endorsed

by their manufacturers and their updates may not be available for those devices. Another IoT security challenge is to approve the signal via the web connection. Many IoT devices do not encrypt the message until it is transmitted over the network. Due to a lack of safety mechanisms in IoT devices, a large number of IoT devices have become targets of cyber attacks. The author discusses twelve different kinds of attacks long with their behavior.

The Internet of Things (IoT) brings a lot of advantages to our lives. Removing menial duties and enhancing the daily effectiveness of things. The Internet of Things might not be as safe as you think because several variables limit the devices used. In [1] the author looks at the latest developments in IoT protection and the most successful strategies for securing IoT devices. They address the IoT architecture based on three layers, i.e. perception layer, network layer and application layer.

Safe routing is important for accepting and using of sensor networks for many applications, but the author [12] has shown that the presently suggested routing protocols are unreliable for these networks. The author proposes security objectives for routing sensor network, illustrate how attacks against ad-hoc and peer-to-peer networks can be adapted to effective sensor network attacks. It implements two classes of novel sensor network attacks, i.e. sinkhole and hello flood, and examine the security of all major routing protocols of the sensor network. The author identifies threats and propose countermeasures for construction.

With the rapid growth of internet technology and communications technology, our lives are increasingly being led into a fantasy space of virtual worlds. In addition to the advantages of IoTs, there are also protection and security benefits and privacy issues at various levels, such as front end, back end and the network. The author introduced architecture to the Internet of Things in [8] and design and resolve those protection and privacy issues at various layers of IoTs. Several open issues were also found by the author, the protection and privacy issues that need to be resolved are targeted by the research community to build a healthy and trustworthy platform for delivery of the future of the Internet of Things. There are a lot of twist questions facing researchers to work with.

The Internet of Things (IoT) has received substantial academic interest in recent years. The internet's future would comprise of heterogeneously interconnected devices that will further expand the world's boundaries of physical entities and interactive parts. The Internet of Things (IoT) can provide new functionality to connected objects. The Author's [36] address the role of SOA (Service Oriented Architecture) in it as well as related enabling technologies for SOA implementation. The concepts, design, basic technology, and implementations of IoT are evaluated by author in [36].

Radio Frequency Identification (RFID) technology can be commonly used in production, retail, logistics, transportation, medical, and protection in different industries. It is one of the most promising and fastest developing technology. Despite the enormous business potential, the RFID has certain inherent shortcomings. RFID system security threats directly impact the rapid growth of RFID technology and limit it. In [6] the author addresses some risks and attacks to the protection of the RFID system that will increase and become more and more complicated. The author also provides the security threats for RFID systems and gave an appropriate solution for it. Therefore, security in RFID is an open issue so, scholars and researchers must always focus to find the protection for RFID technology.

2.2 Classifications in Different Surveyed Techniques

In this section we are going to discuss the classification published in different surveyed papers. These survey paper contain classification which is related to different aspect of IoT attacks. We ensured that there is no comprehensive classification exist in these surveyed techniques. For this purpose we want to review these classifications.

In this classification author [2] discuss attacks according to the common architecture of the IoT which contains only three layers i.e. perception layer, network layer

and application layer. This classification is divided into four categories, i.e. physical attack, network attack, software attack and encryption attack and it cover 25 attacks.

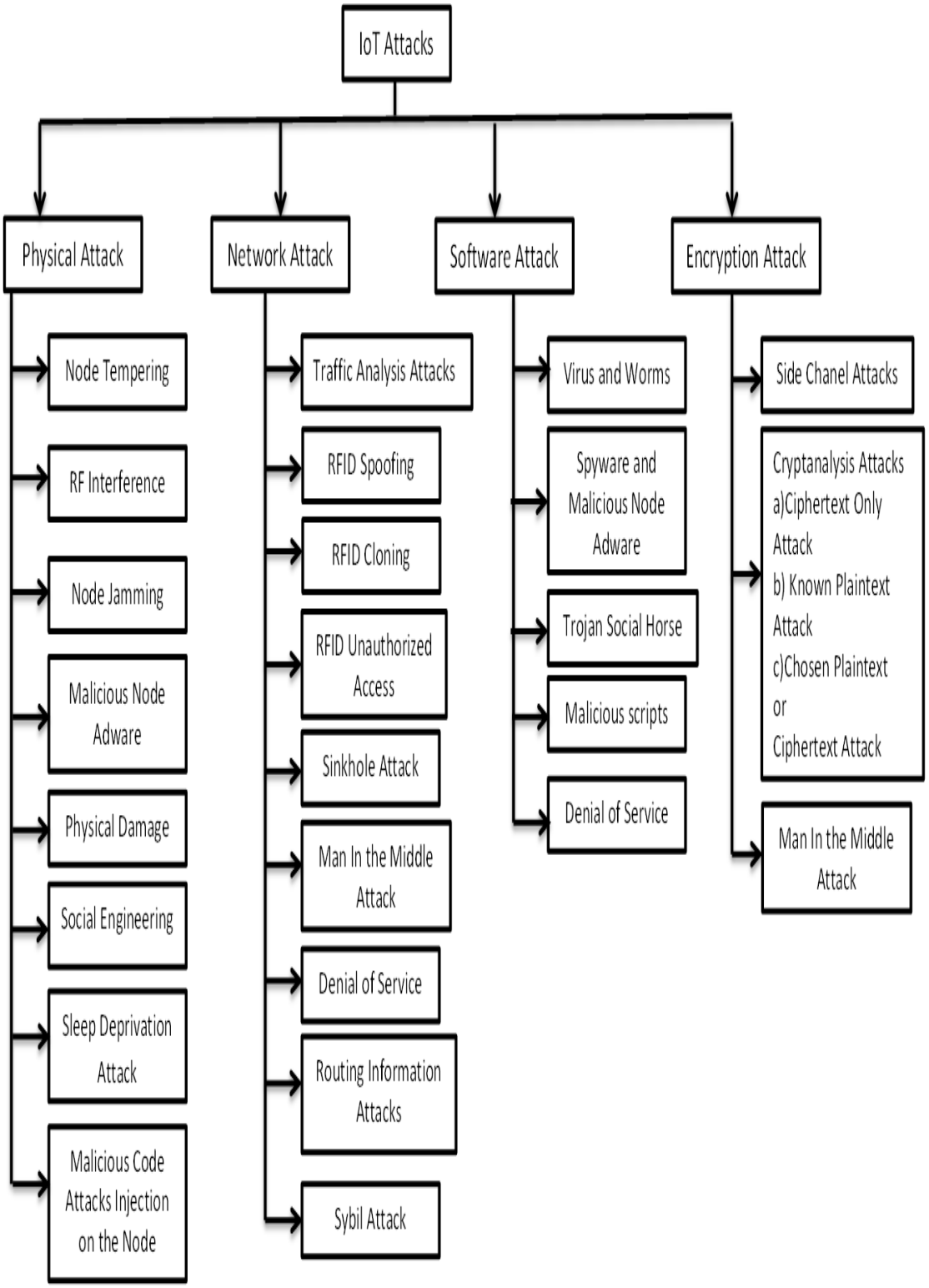

FIGURE 2.1: IoT and its security attacks [2]

In this classification author [3] draw a map of cyber attacks to know the threats, vulnerabilities and expected risks within IoT based healthcare. In this classification, author spilt these attacks into three layer attacks, i.e. application layer attacks, network layer attacks and perception layer attack and cover only 21 attacks.

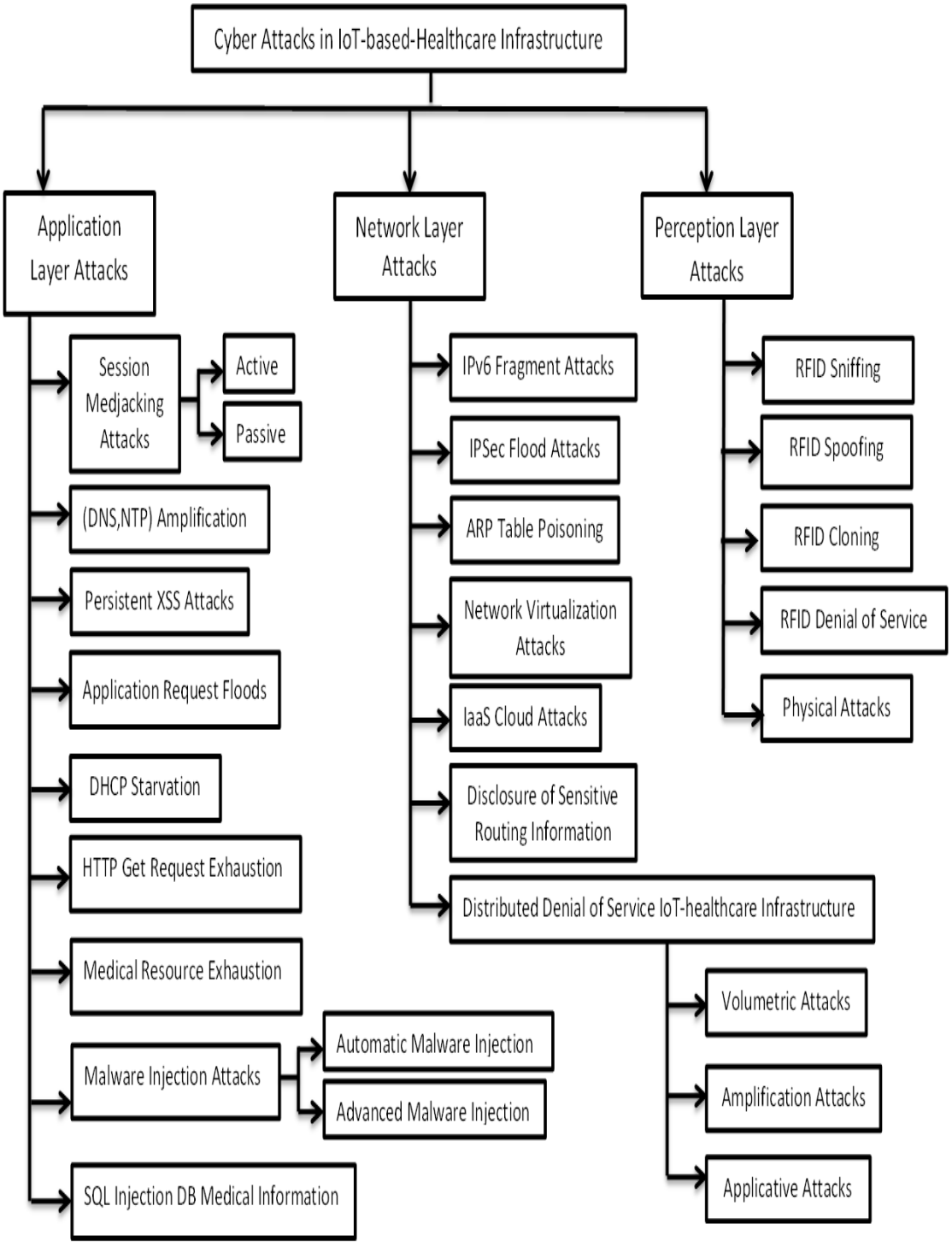

FIGURE 2.2: Cyber attack classification in IoT based healthcare [3]

The author [4] of this research paper claims that their classification is specific to other classifications based on IoT since their classification is divided into four groups, i.e. physical attacks, network attacks, software attacks, and encryption attacks and it covers 25 attacks.

Physical Attacks	Network Attacks	Software Attacks	Encryption Attacks
Node Tampering	Traffic Analysis Attacks	Virus and Worms	Side Channel Attacks
RF Interference	RFID Spoofing		Cryptanalysis Attacks: a)Ciphertext Only Attacks b)Known Plaintext Attacks c)Chosen Plaintext or Ciphertext Attack
Node Jamming	RFID Cloning	Spyware and Adware	
Malicious Node Injection	RFID Unauthorized Access		
Physical Damage	Sinkhole Attack	Trojan Horse	
Social Engineering	Man In the Middle Attack		
Sleep Deprivation Attack	Denial of service	Malicious Scripts	Man In the Middle Attack
Malicious Code Injection on the Node	Routing Information Attacks		
	Sybil Attack	Denial of Service	

FIGURE 2.3: Classifications of IoT attacks [4]

The author [24] provide this classification which will allow the scholar to understand different kinds of attacks in this taxonomy. This classification consists of eight categories, i.e. device property, location, strategy, information damage level, host based, access level, protocol based, communication stack protocol and it covers 23 attacks.

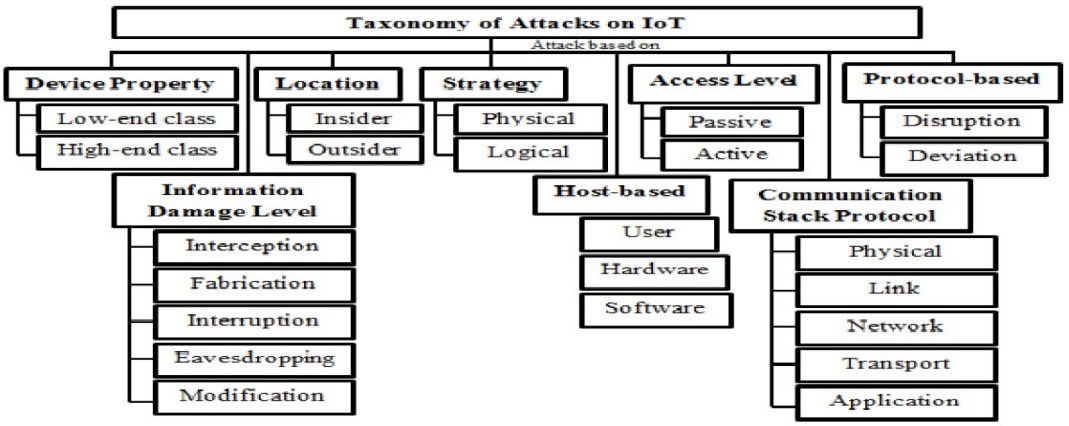

FIGURE 2.4: Taxonomy of security attacks on IoT [24]

In this figure author [24] discuss layer based attacks with its techniques so that future researchers/scholar can get help through this and design its countermeasure. It consists of five layers, i.e. physical layer, data link layer, network layer, transport layer, application layer and 16 attacks.

Layer	Attacks	Methods/ Strategies attacks
Physical	Jamming	Creates radio interference and exhaustion on IoT devices.
	Tampering	Creates compromised nodes.
Data Link	Collision	Simultaneously transmit two nodes of the same frequency.
	Exhaustion	By repetitive collision the nodes.
	Unfairness	Using above link layer attacks.
Network	Spoofed, altered or replayed routing information	Creates routing loops, extend or shortening sources routes, attracting or repelling network from select nodes.
	Selective forwarding	Choose what information that gathered before transmit it.
	Sinkhole	Monitoring, Redundancy, Authentication
	Sybil	Single node duplicates its node to be in multiple locations.
	Wormholes	Selectively tunneling or retransmit information to the IoT devices.
	HELLO flood	Uses HELLO packets as weapon to launch the attack on IoT system.
	Acknowledgement spoofing	Spoof the link layer acknowledgements for overhead packets.
Transport	Flooding	Repeat the request of a new connection until the IoT system reach maximum level.
	De-synchronization	Disruption of an existing connection.
Application	Attacks on reliability and clone attack: Clock skewing, Selective message forwarding, Data aggregation distortion	The adversaries usually masquerade like normal behavior in IoT system. Attackers also can still choose a message that he/she intend in the IoT system and launched their own malicious activites.

FIGURE 2.5: Layered based attacks with their attack strategies in IoT System [24]

The author [28] constructs and observes IoT vulnerabilities in this taxonomy within the range of layers, security effects, and attacks, method of remediation and awareness capabilities of the situation and then describes each of them.

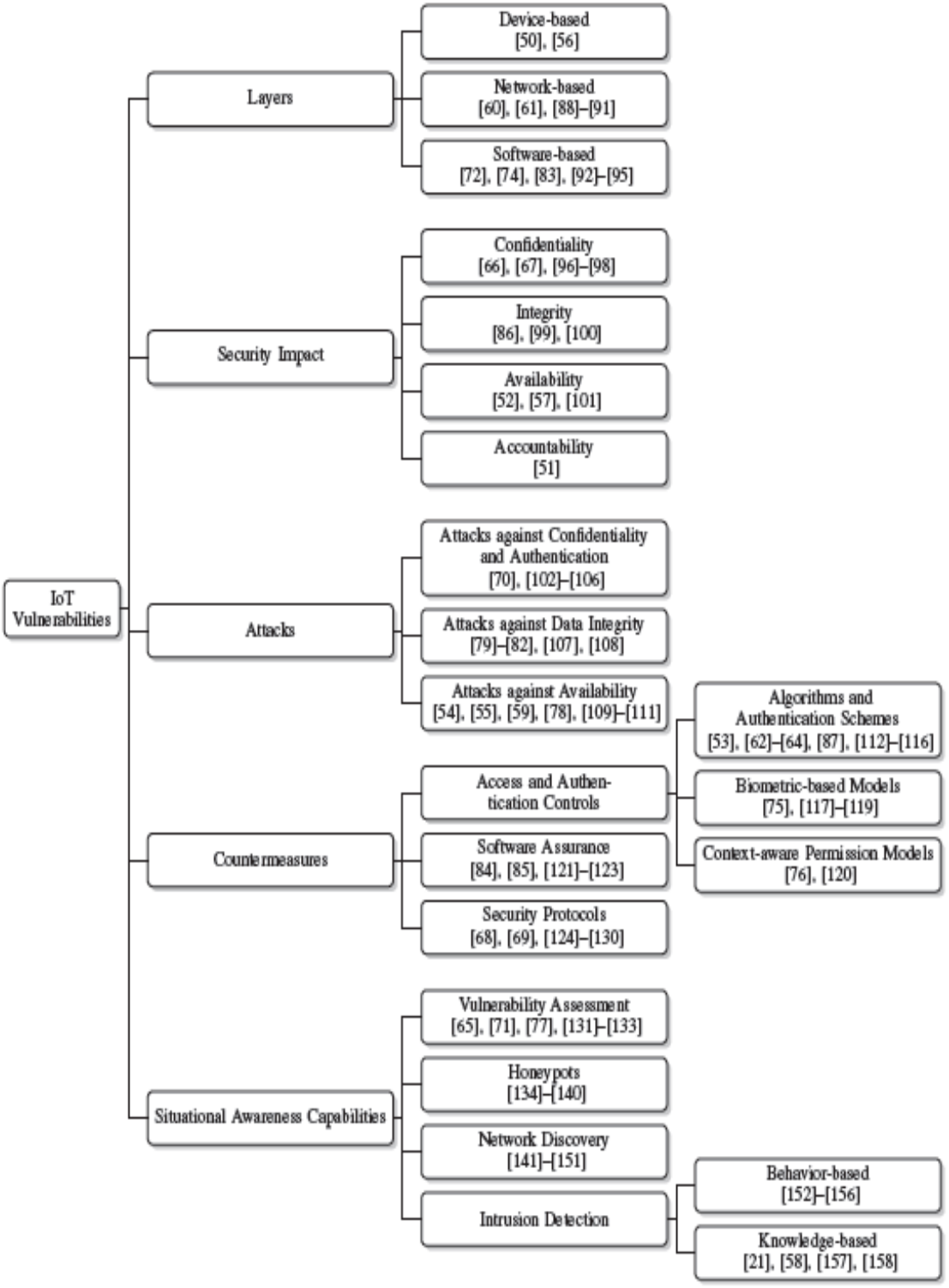

FIGURE 2.6: A categorization of IoT vulnerabilities [28]

Author [29] presents this taxonomy for IoT security using machine learning or deep learning ML/DL. In this taxonomy IoT security is classified into five categories i.e. IoT system, IoT security threats, learning methods for IoT security, ML/DL for layers security and challenges and future directions. In this classification, author discuss how ML/DL methods use to secure the communication between IoT based system based on the traditional architecture of IoT which consist of three layers i.e. application layer, network layer and perception layer.

FIGURE 2.7: Thematic taxonomy of ML/DL for IoT security [29]

In this diagram author [29] discuss basic attacks which can affect its basic security requirement. In this diagram threats are divided into two categories, i.e. active threat and passive threat. These active and passive attacks are related to the basic security of IoT system which is confidentiality, integrity, authentication, authorization, availability and non-repudication.

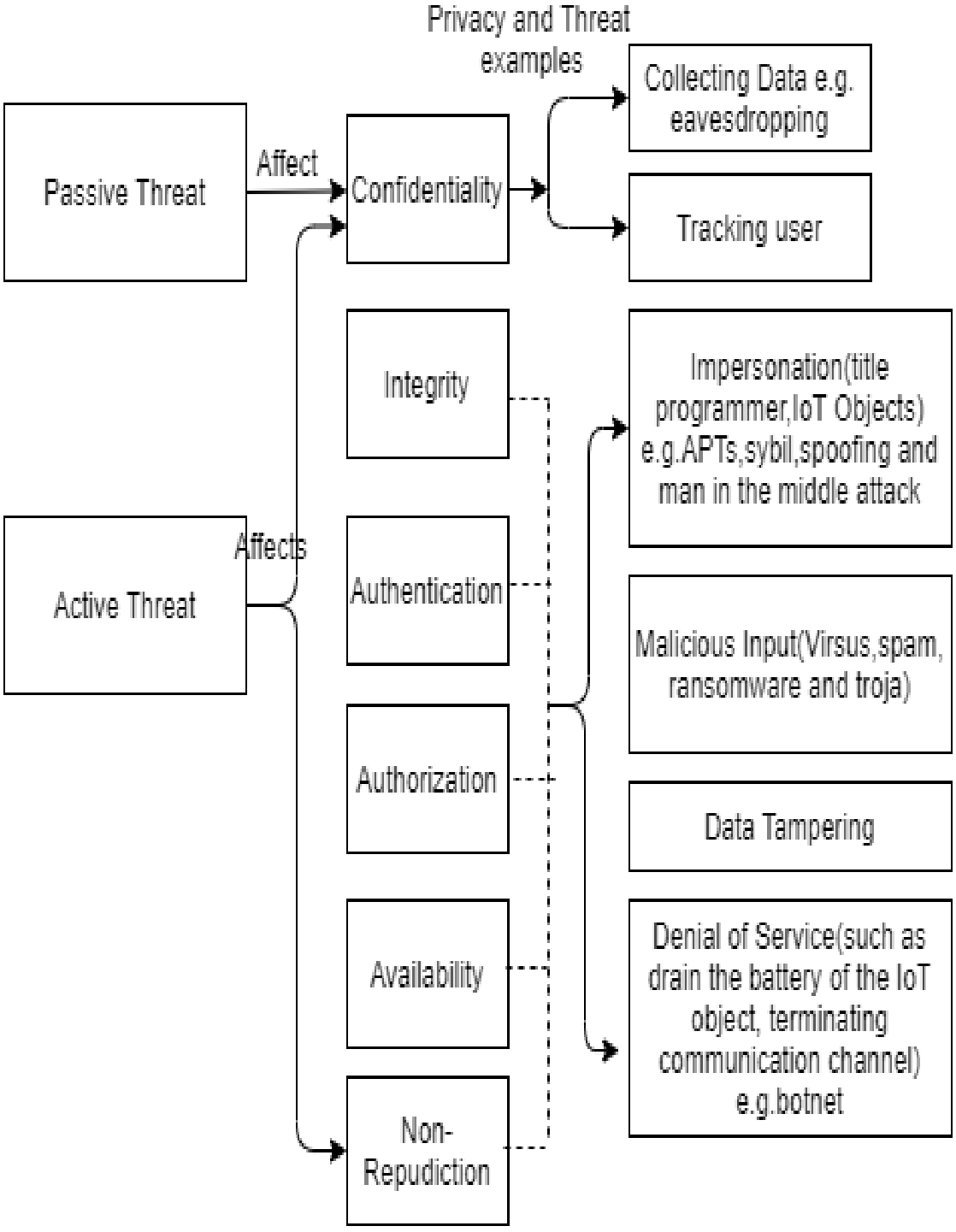

FIGURE 2.8: Potential threats in the IoT system [29]

The author [13] addresses attacks on WSNs in this diagram. These attacks are defined by the author on the basis of the OSI model. These attacks affect four layers: the physical layer, the MAC layer, the network layer and the application layer and it cover 13 attacks.

OSI Layers	Attacks
Application Layer	Clock Skewing, Selective Message Forwarding, Data Aggregation Distortion.
Network Layer	False Routing, Packet Replication, Blackhole, Wormhole, Sinkhole
MAC Layer	Traffic Manipulation, Identity Spook
Physical Layer	Device Tampering, Eavesdropping, Jamming

FIGURE 2.9: OSI layer attacks [13]

Based on WSN technology, the author [9] addresses different vulnerabilities. These attacks are split into two categories: active and passive attacks and it covers 18 attacks.

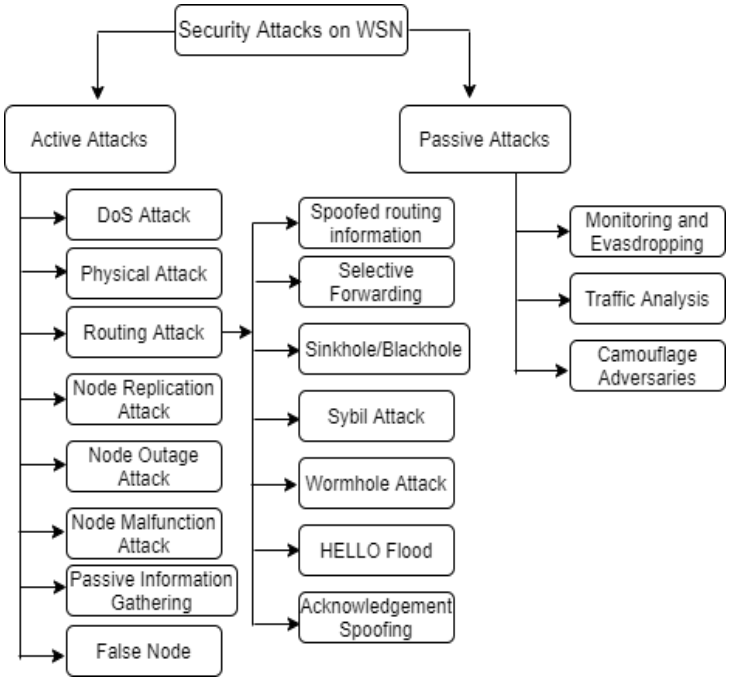

FIGURE 2.10: Security attacks on wireless sensor network [9]

In this taxonomy author [18] addresses hardware attacks of IoT objects. It covers 18 attacks.

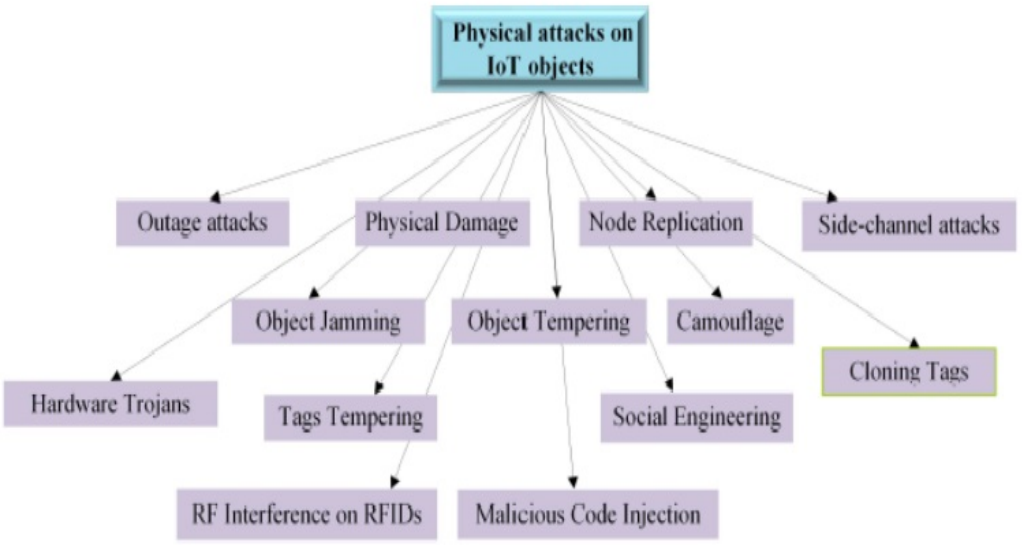

FIGURE 2.11: Taxonomy of physical attacks against IoT objects [18]

The author addresses [18] attacks that target only the network protocols in this taxonomy. It is divided into two groups, i.e. RPL attack-based (low power and lossy network routing protocol), 6loWPAN-based attacks and it cover 10 attacks.

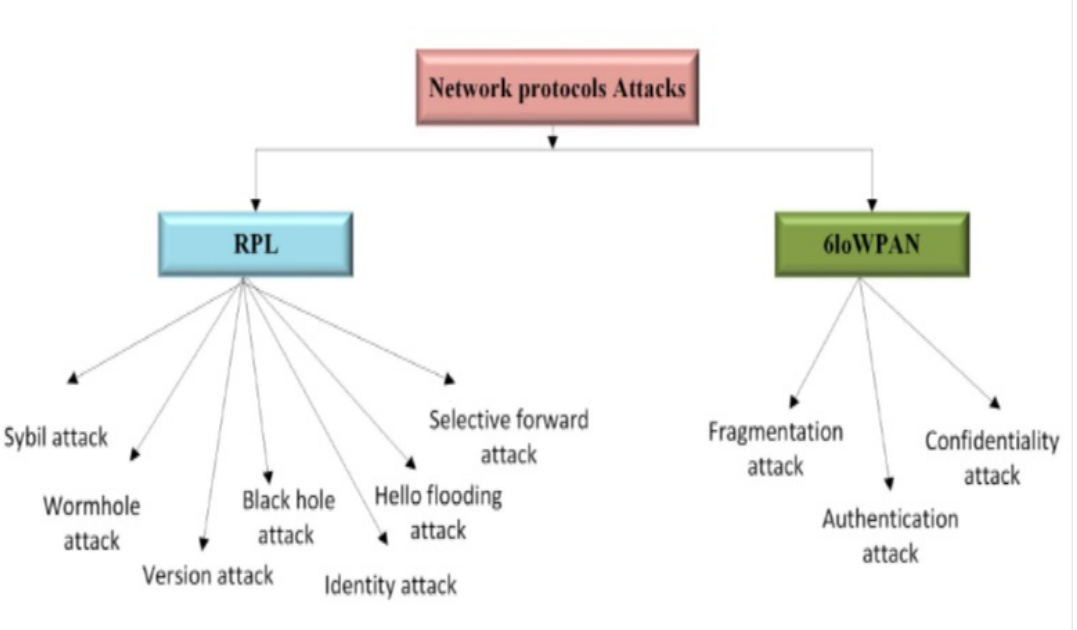

FIGURE 2.12: Taxonomy of network attacks against IoT objects [18]

The author addresses [18] communication protocol-based attacks over networks. It is categorized into three classifications, i.e., TLS, attacks against the application protocol, attacks based on TCP/UDP and it cover 21 attacks.

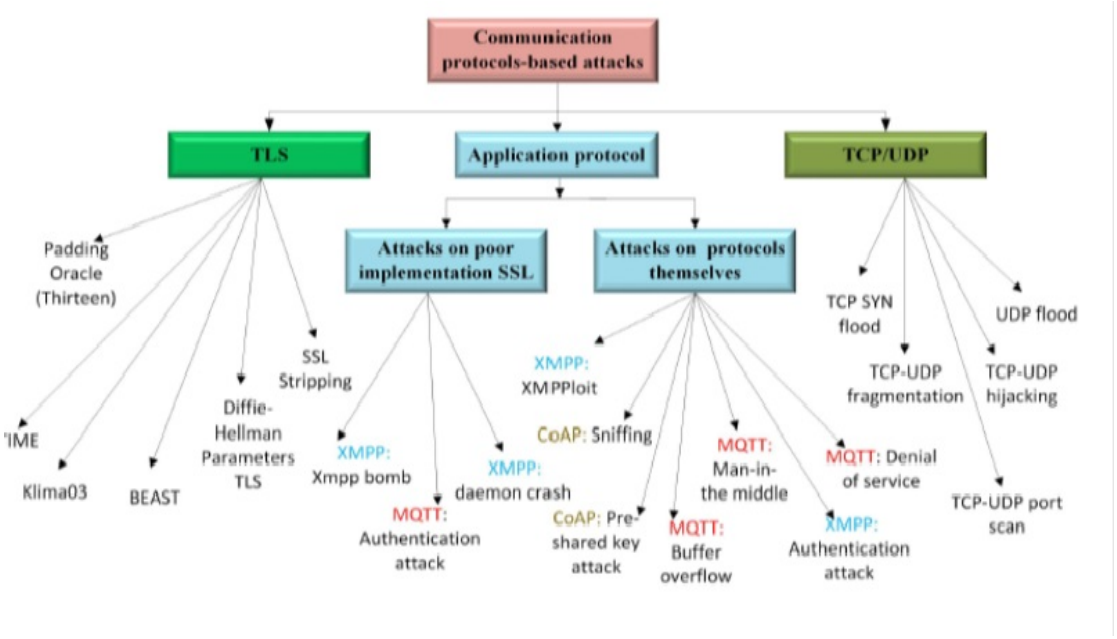

FIGURE 2.13: Taxonomy of communication protocol attacks [18]

The authors [18] discuss certain attacks related to data in this taxonomy, i.e. placed on IoT objects locally or remotely placed on the cloud and it cover 13 attacks.

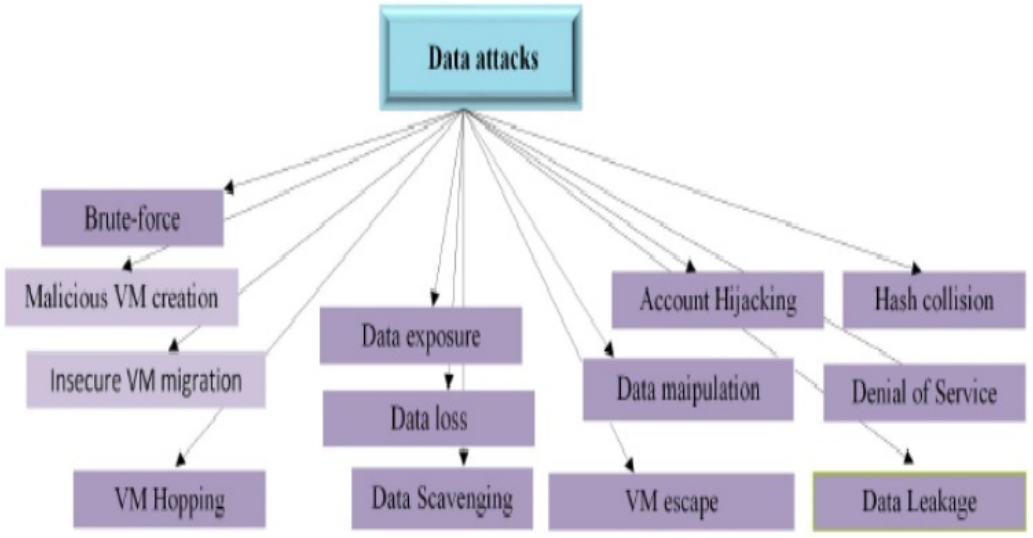

FIGURE 2.14: Taxonomy of data at rest attacks [18]

The author [18] addresses those attacks in this taxonomy in which the attacker does not damage data, but can do other harm to it, such as software attacks, etc.. It covers 19 attacks

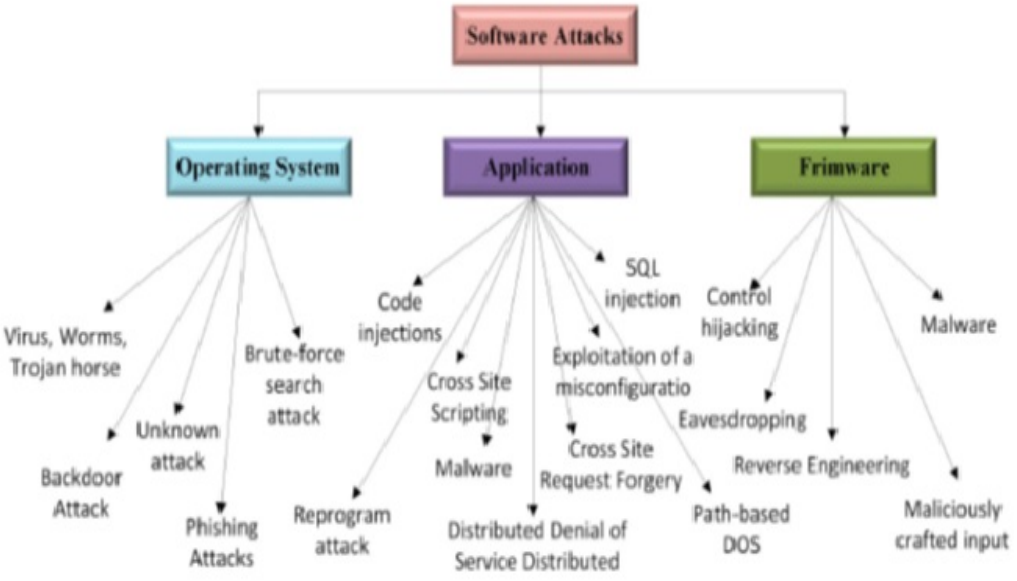

FIGURE 2.15: Taxonomy of IoT software [18]

The authors present different classifications based on their perspectives on various surveyed techniques. Those methods were limited to a few basic criteria. We couldn't find a comprehensive classification that listed all of the attacks in one place.

2.3 Conclusions

Various techniques and their classifications have been surveyed in this chapter. It was observed that each of the classifications focused on particular classes (physical attacks, network attack, software attack, encryption attack etc.) for IoT attacks. According to our acquired knowledge, it has been found that there is no comprehensive IoT related attack classification available that can model all the different attacks. In the next chapter, we will propose a comprehensive ontology related to IoT based healthcare system and the steps to develop this ontology.

Chapter 3

Proposed Ontology

After carrying out a detailed survey in chapter 2 on the classification of IoT attacks in the healthcare domain, we conclude that there is no comprehensive classification of IoT attacks available in the healthcare system. Proposed ontology is my contribution in this IoT base healthcare domain. This chapter is divided into 2 sections. In section 3.1 our proposed ontology development is divided into four stages which are knowledge acquisition, conceptualization, implementation and evaluation. We discussed three stages here in detail. Ontology evaluation will be discussed in the next chapter. In section 3.2 we conclude this chapter.

3.1 Proposed Ontology Development

We are going to propose one comprehensive ontology which contain information regarding disruption attacks that occur in IoT based environment in general and specific in the healthcare domain. We have studied various attacks from various papers and then we have conceptually modeled them in the form of ontology by implementing that ontology by using protégé software [37].

Ontology development lifecycle has many methodologies such as feature driven development, TOVE [38] etc. To develop this ontology we have adopted the following steps:

1. Knowledge acquisition
2. Conceptualization
3. Ontology Implementation
4. Ontology Evaluation

3.1.1 Knowledge Acquisition

To provide an ontology for the attacks which is related to IoT base healthcare system, we need to acquire the knowledge in this domain. From the surveyed techniques in literature review we have gathered knowledge which is modeled in tabular form. Each table consists of five research papers. In these tables, each row consists of different types of attack and each column consists of published techniques in which these types of attack exist. Tick means that the attack is included in the published techniques in these tables, while empty cells imply that there is no attack in this technique. The numbers of attacks which occur in these research papers are shown in 3.1, 3.2, 3.3, 3.4.

TABLE 3.1: Information disruption attack classification

No.	**Attack name**	**Riaz, 2015**	**Jyoti, 2015**	**Djenna, 2018**	**Elrawy, 2018**	**Loannis, 2015**
01	H/W Compromise	✓			✓	
02	S/W Compromise	✓			✓	
03	Standard protocol compromise	✓				
04	Network Protocol Stack Attack	✓				
05	Node Tempering		✓			
06	RF Interference on RFIDs		✓			✓
07	Node Jamming in WSNs		✓			✓
08	Malicious Node Injection		✓		✓	✓
09	Malicious Node Adware	✓				
10	Physical Damage		✓		✓	✓
11	Social Engineering		✓			✓
12	Sleep Deprivation Attack		✓			✓

13	Malicious Code Injection	✓		✓	✓
14	Sinkhole attack	✓			✓
15	Traffic Analysis Attacks	✓			✓
16	RFID Spoofing	✓	✓		✓
17	RFID Cloning	✓	✓		✓
18	RFID Unauthorized Access	✓	✓		✓
19	Man in the Middle Attacks	✓			✓
20	DoS/DDoS Attack	✓	✓	✓	✓
21	Routing Information Attacks	✓			✓
22	Sybil Attack	✓			✓
23	Phishing Attacks	✓			✓
24	Virus, Worms, Trojan horse, Spyware and Aware	✓		✓	✓
25	Malicious Scripts	✓			✓
26	Side-channel Attacks	✓			✓
27	Cryptanalysis Attacks	✓			✓
28	Session Medjacking		✓		
29	Ransomware		✓		
30	Timing Attacks				✓
31	Mass Node Authentication Problem				✓
32	DNS, NTP Amplification		✓		
33	XSS Attacks		✓		
34	Application Request Flood		✓		
35	DHCP Starvation		✓		

In table 3.1 some number of attacks are removed because these attacks do not occur in these five published techniques. The number of attacks which we removed in this tables are (Device tempering, Physical attacks, Ip address spoofing, Session hijacking, Cross site scripting, DNS spoofing, FMS attack, Korek attack, Chop-chop attack, Fragmentation attack, PTW attack, Google replay attack, Micheal attack, Ohigashi-Morii attack, Dictionary attack, ZED sabotage attack, Selective forward attack, Zigbee attack, Homing attack, Flooding attack, Eavesdropping, Sql injection, Node replication attacks, Node outage attacks,Object replication attack, Camouflage). These attacks are covered in next tables.

TABLE 3.2: Information disruption attack classification

No.	Attack name	Zao, 2013	Djamel, 2018	Nawir, 2016	Jing, 2014	Stellios, 2018
01	Node Temparring	✓				
02	Malicious Node Injection	✓				
03	Sinkhole Attack			✓		
04	RFID Spoofing			✓		
05	DoS/DDoS Attack	✓		✓		
06	Routing Information Attacks	✓		✓		
07	Sybil Attack			✓		
08	Virus, Worms, Trojan horse, Spyware and Aware			✓		
09	Side-channel Attacks	✓				

In table 3.2 only nine attacks are presented. Remaining 58 attacks are not presented in published techniques which we surveyed in literature review. They are presented in other published techniques.

TABLE 3.3: Information disruption attack classification

No.	Attack name	Daman, 2014	Wahid, 2015
01	Device Temparing	✓	
02	Eavesdropping	✓	
03	Node Jamming in WSNs	✓	
04	Malicious Node Injection		✓
05	Node Replication Attacks		✓
06	Node Outage Attacks		✓
07	Sinkhole Attack		✓
08	Traffic Analysis Attacks	✓	✓
09	DoS/DDoS Attack		✓
10	Routing Information Attacks	✓	✓
11	Blackhole Attack	✓	✓
12	Sybil Attack		✓
13	Virus, Worms, Trojan horse, Spyware and Aware	✓	✓
14	Hello Flood		✓
15	Timing Attacks	✓	
16	Physical Attacks		✓

In table 3.3 only sixteen attacks are presented. Remaining 51 attacks are not presented in these published techniques. They are presented in other techniques.

TABLE 3.4: Information disruption attack classification

No.	**Attack name**	**Gill, 2019**	**Hezam, 2018**	**Sonar, 2014**
01	H/W Compromise		✓	
02	Eavesdropping		✓	
03	Sql Injection	✓		
04	Object Replication Attack		✓	
05	RF Interference on RFIDs		✓	
06	Node Jamming in WSNs		✓	✓
07	Camouflage		✓	
08	Malicious Node Injection		✓	
09	Social Engineering		✓	
10	Sinkhole Attack		✓	
11	RFID Spoofing			✓
12	De-synchronizing Attack			✓
13	Man in the Middle Attacks	✓	✓	
14	Network Sniffing	✓		
15	Drown Attack	✓		
16	Bootstrapping Attack			✓
17	DoS/DDoS Attack	✓	✓	✓
18	Blackhole Attack		✓	
19	Sybil Attack		✓	
20	Virus, Worms, Trojan horse, Spyware and Aware		✓	
21	Hello Flood		✓	✓
22	Side-channel Attacks		✓	
23	Session Hijacking	✓		
24	Physical Attacks		✓	
25	Ip Address Spoofing	✓		
26	Cross-site Scripting	✓		
27	DNS Spoofing	✓		
28	FMS Attack		✓	
29	Korek Attack		✓	
30	Chopchop Attack		✓	

31	Fragmentation Attack	✓	
32	PTW Attack	✓	
33	Google Replay Attack	✓	
34	Micheal Attack	✓	
35	Ohigashi-Morii Attack	✓	
36	Dictionary Attack	✓	
37	ZED Sabotage attack	✓	
38	Selective Forward Attack	✓	
39	Zigbee Attack		✓
40	Homing Attack		✓
41	Flooding Attack		✓

In table 3.4 some number of attacks is removed because these attacks do not occur in these published techniques. The number of attacks which we removed in this tables are (s/w compromise, standard protocol compromise, device temparing, network protocol stack attack, traffic analysis attack, RFID cloning, routing information attack, phishing attack, DNS, NTP amplification, XSS attacks, application request flood, DHCP starvation, RFID unauthorized access, malicious node adware, sleep deprivation attack, malicious code injection, node replication attacks, node outage attacks, physical damage, node temparring). These attacks are covered in previous three tables.

3.1.1.1 Frequency of Attack Occurrence in Different Surveyed Techniques

Several attacks from the acquisition of knowledge have been grouped into five different tables 3.5, 3.6, 3.7, 3.8, 3.9 in this section. Each table includes the names and frequencies of these attacks. In various published techniques, these frequency numbers indicates the number of occurrences of each attack. These numbers of attacks are grouped in different tables. Each group is represented by Group A, B, C, D, E respectively. Each group contains attacks which are organized in previous section 3.1. Each group contains 15 attacks, according to these table 3.1, 3.2, 3.3, 3.4. Node jamming in WSNs, malicious node injection, sinkhole attack, RFID

spoofing, man in the middle attack, DoS/DDoS attack, routing information attack, sybil attack, virus, worm, trojan horse, spyware and adware, side-channel attack has higher frequencies.

Table 3.5: Group A

Attack name	**Frequency**
H/W Compromise	3
S/W Compromise	2
Standard Protocol Compromise	2
Device Tempering	1
Eavesdropping	2
Sql Injection	1
Object Replication Attack	1
Network Protocol Stack Attack	1
Node Tempering	3
RF Interference on RFIDs	3
Node Jamming in WSNs	5
Camouflage	1
Malicious Node Injection	6
Malicious Node Adware	1
Node Replication Attacks	1

Table 3.6: Group B

Attack name	**Frequency**
Node Outage Attacks	1
Physical Damage	3
Social Engineering	3
Sleep Deprivation Attack	2
Malicious Code Injection	3
Sinkhole Attack	5
Traffic Analysis Attacks	4
RFID Spoofing	5
RFID Cloning	3
RFID Unauthorized Access	3
De-synchronizing Attack	1
Man in the Middle Attacks	4
Network Sniffing	1
Drown Attack	1
Bootstrapping Attack	1

Table 3.7: Group C

Attack name	**Frequency**
DoS/DDoS Attack	10
Routing Information Attacks	6
Blackhole Attack	3
Sybil Attack	5
Phishing Attacks	2
Virus, Worms, Trojan horse, Spyware and Aware	7
Hello Flood	3
Malicious Scripts	2
Side-channel Attacks	4
Cryptanalysis Attacks	2
Session Medjacking	1
Session Hijacking	1
Ransomware	1
Timing Attacks	2
Mass Node Authentication Problem	1

Table 3.8: Group D

Attack name	**Frequency**
Physical Attacks	2
Ip Address Spoofing	1
Cross Site Scripting	1
DNS Spoofing	1
FMS Attack	1
Korek Attack	1
Chopchop Attack	1
Fragmentation Attack	1
PTW Attack	1
Google Replay Attack	1
Micheal Attack	1
Ohigashi-Morii Attack	1
Dictionary Attack	1
ZED Sabotage Attack	1
Selective Forward Attack	1

TABLE 3.9: Group E

Attack name	**Frequency**
Zigbee Attack	1
Homing Attack	1
Flooding Attack	1
DNS, NTP Amplification	1
XSS Attacks	1
Application Request Flood	1
DHCP Starvation	1

Group A, B, C have the number of attacks which have higher frequency while group D and E contains low frequency. This number of frequencies indicate that which attacks are more critical in this domain. We plot graphs using the frequency of these attacks.

3.1.1.2 Plots for Frequency of Surveyed Attacks

Graphical representations of different attacks will be addressed in this section. By viewing these plots researcher/ scholar can find out which attack is very critical or repeated. These attacks are grouped by the frequency of attacks that helped me to generate charts from Microsoft Excel. These charts are created on the basis of two parameters, the number of attacks and their frequency level.

Figure 3.1 consists of the group A attacks that we have randomly put together. In it the highest frequency of attack is malicious node injection and node jamming in WSNs.

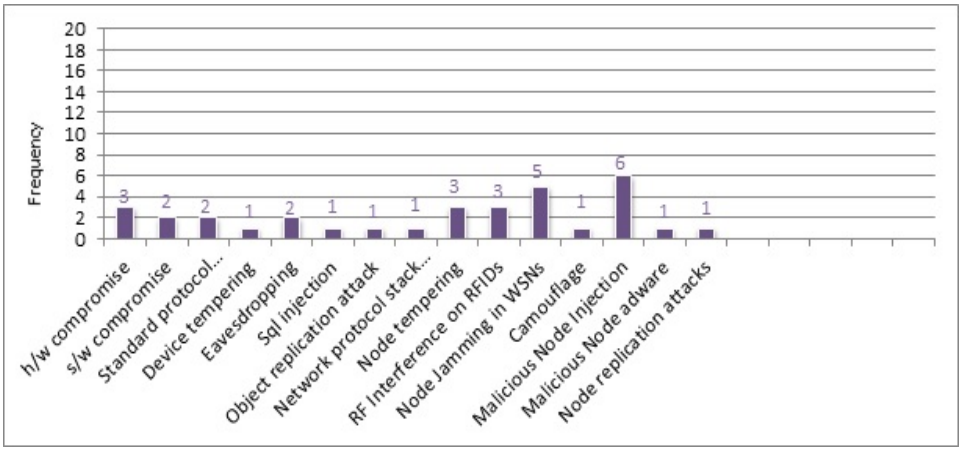

FIGURE 3.1: Group A

Figure 3.2 includes the group B attacks focused on an IoT based healthcare system. The highest frequency of attacks is sinkhole attack, traffic analysis attack, RFID spoofing, man in the middle attack.

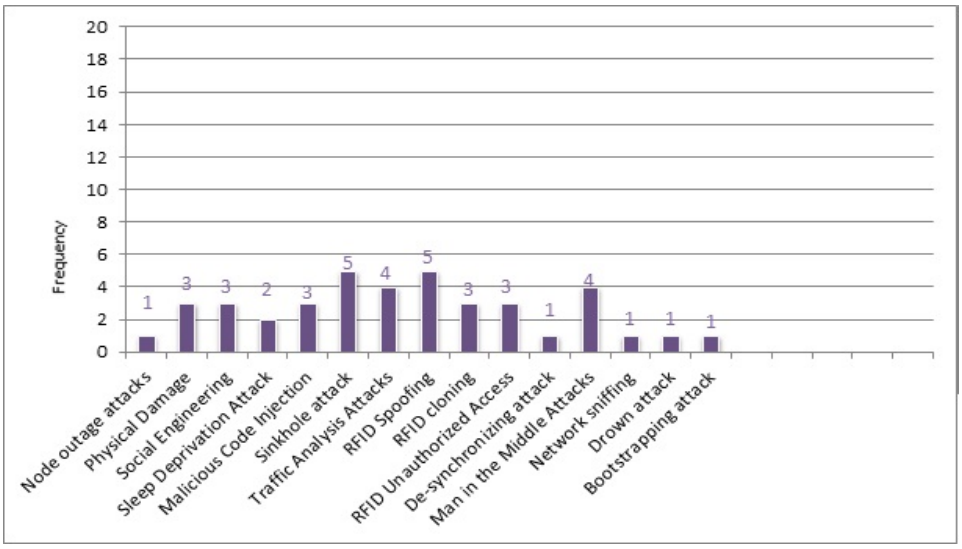

FIGURE 3.2: Group B

Figure 3.3 includes the highest frequency in all of the attack types. The highest frequency of attacks are DoS/DDoS attack, routing information attacks, sybil attack, virus, worm, trojan horse, spyware and adware attack and side channel attack.

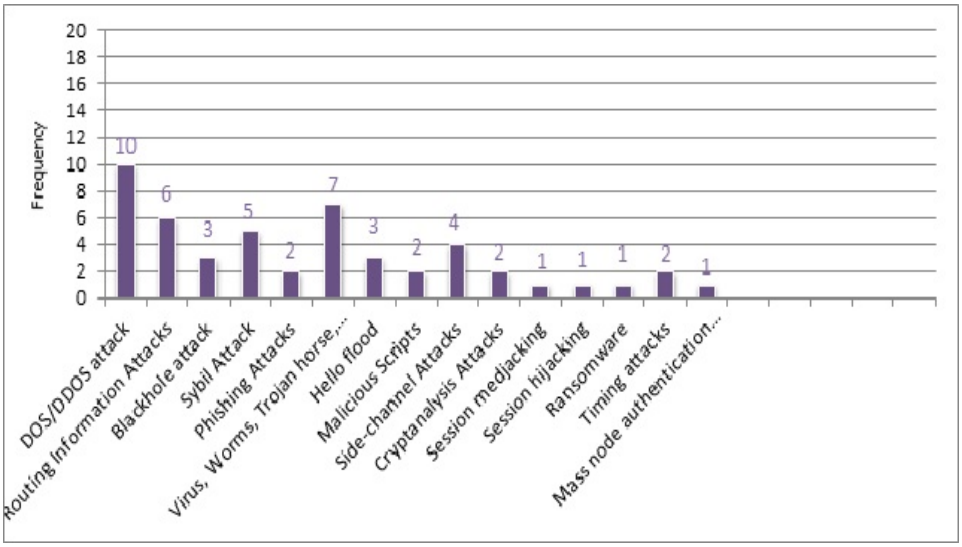

FIGURE 3.3: Group C

Figure 3.4 includes the lowest frequency attacks.

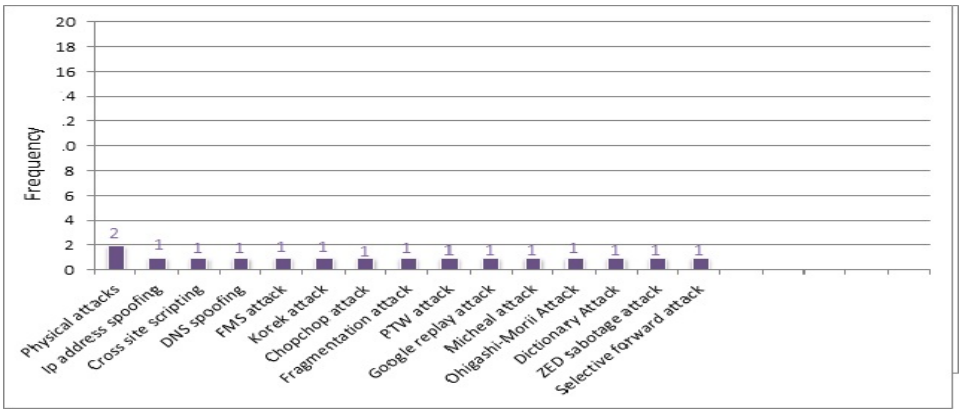

FIGURE 3.4: Group D

Figure 3.5 also contain lowest frequency attack on IoT based healthcare system.

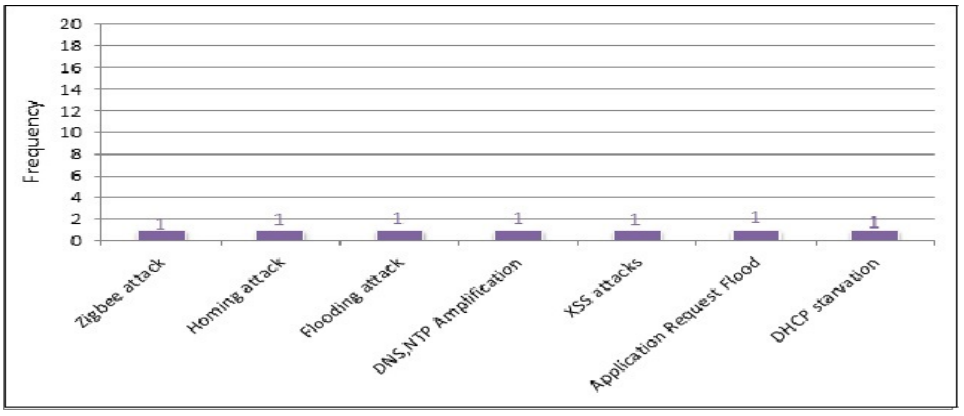

FIGURE 3.5: Group E

These charts that are shown in figure 3.1, 3.2, 3.3, 3.4 and 3.5 show attacks and their frequencies. These frequencies tells which attack is more critical as compared to others.

3.1.1.3 Venn Diagram for Knowledge Acquisition

From the surveyed techniques in literature review, we have gathered attacks which is modeled in tabular form. From those tables we find the frequency occurrence of IoT attacks in healthcare domain. These attacks are categorized in four subclasses which is Network protocol layer based attacks, health care data attack, network infrastructure base attack and miscellaneous attacks. These subclasses are further

divided into subclasses. The Venn diagram is only made for an abstract class of IoT attacks. These attacks show the overlapping relationship between them.

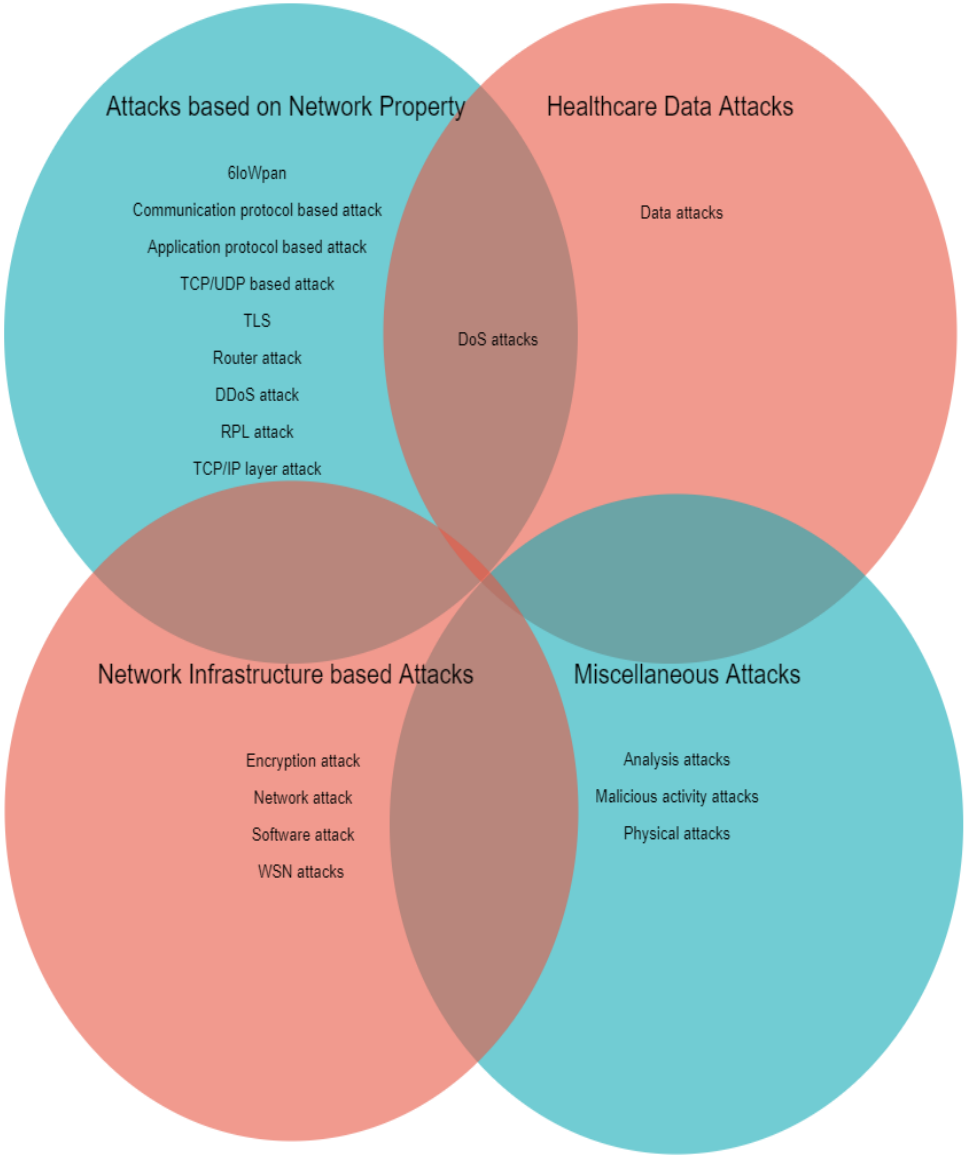

FIGURE 3.6: Venn diagram of IoT attacks

3.1.2 Conceptualization

On the basis of the acquired knowledge which we gathered in the previous section we conceptualize the base class into four sub-classes shown in figure 3.7 by using the top down method. These subclasses are classified according to basis of network protocol, data attacks, network structure and miscellaneous attacks which further

explain in 1, 2, 3 and 4 connector. These connectors connect subclasses which are shown separately in diagrams.

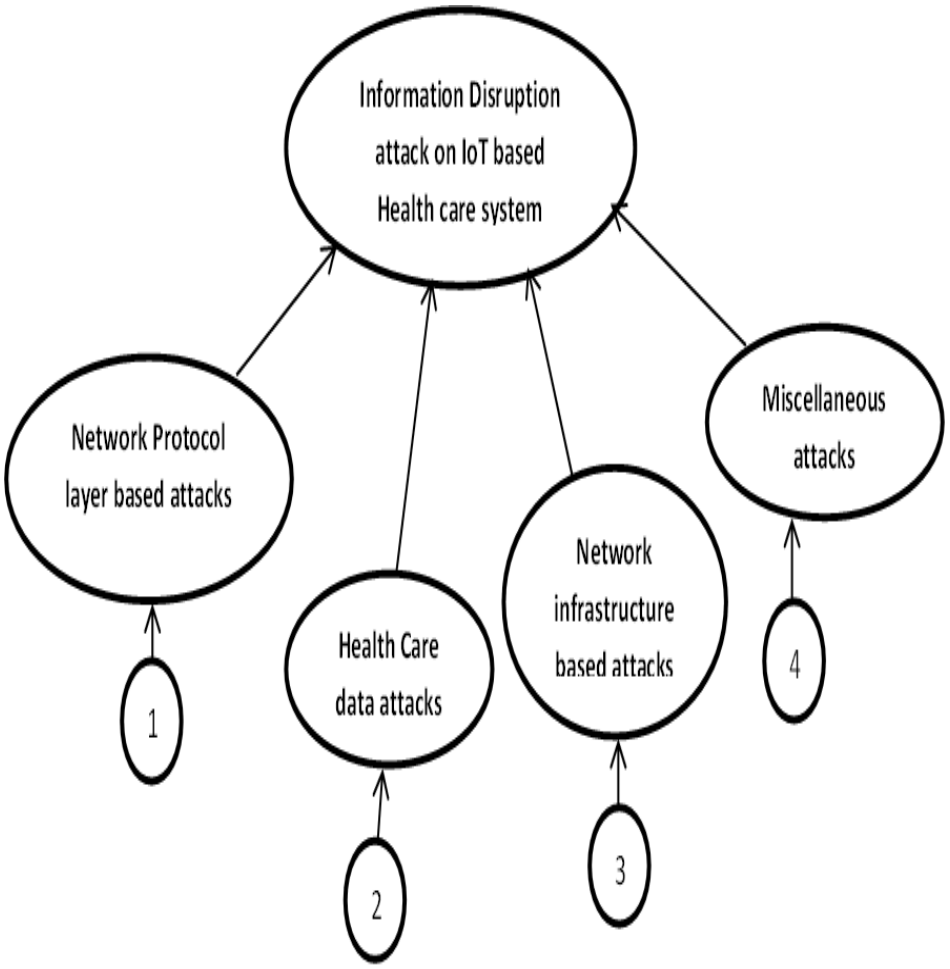

FIGURE 3.7: Conceptual model of Information Disruption Attack on IoT based healthcare system

Attack based on network protocol is shown in figure 3.8 which relates to network protocol attacks. It is further divided into TCP/IP layer attack, communication protocol based attack, RPL (Routing Protocol for Low Power and Lossy Networks) and 6loWpan. 6loWpan is the upgrade version of the Internet Protocol (IPv6) and Low-power Wireless Personal Area Networks (LoWPAN). 6LoWPAN, allow for the smallest devices with limited processing ability to transmit information wirelessly using an internet protocol. Some attacks like sybil attack and hello flood attacks are repeated in different sub classes like WSN attack, network attack, etc. Some subclasses are further divided into subclasses which are shown in 1.1, 1.2, 1.3, 1.4, 1.5, 1.6, 1.7, 1.8, 1.9 node diagrams.

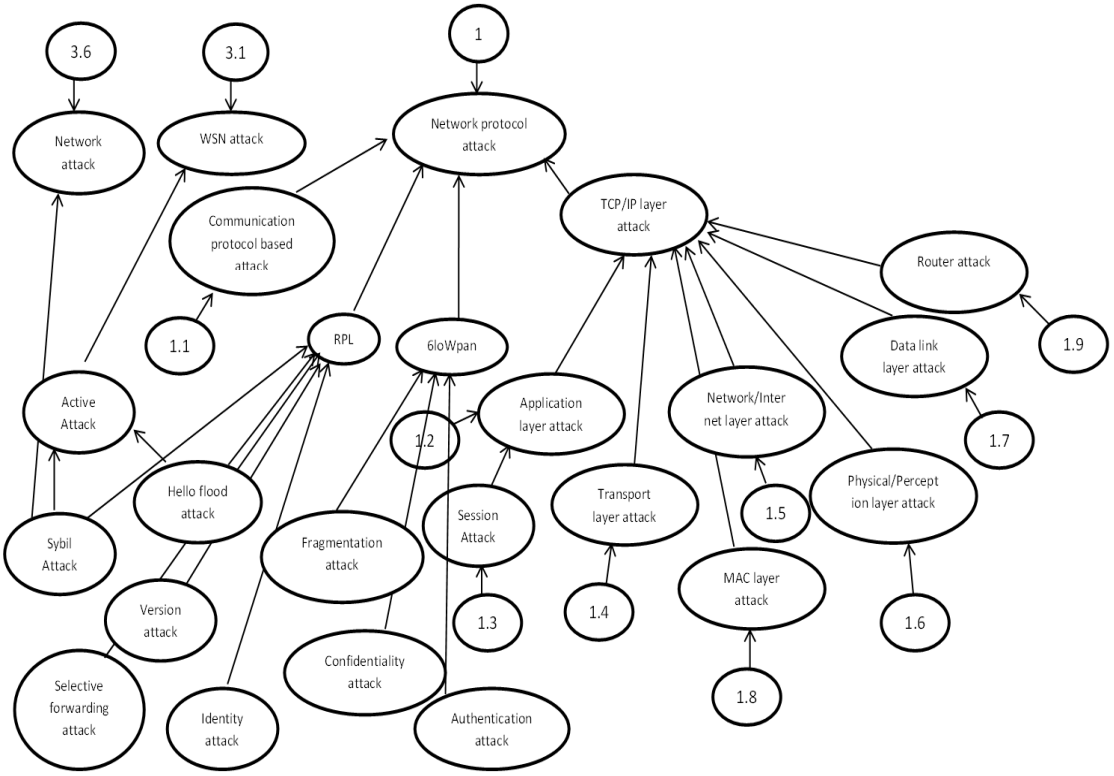

FIGURE 3.8: Conceptual model of attack based on network protocol

This classification which is shown in figure 3.9 is related to the actual data which resides locally or remotely on devices. It is further divided in a subclass which is shown in 2.1 node diagram.

FIGURE 3.9: Conceptual model of healthcare data attack

Network infrastructure base attacks in figure 3.10 are further divided into four subclasses i.e. WSN attacks, network attack, software attack and encryption attack. WSN (wireless sensor network) consist of low cost and low power, small devices which are compromised by an attacker by different attacks. WSN attacks are further categorized in active attacks and passive attacks. Network attack gain unauthorized access to IoT devices. The attacker does not need to be close to network to implement these attacks. In computerized system software attack are the main source for attacker to implement attacks by using its vulnerabilities. Encryption attacks are based on how the attacker can attack by breaking the encryption scheme i.e. used in IoT devices. It is further divided into subclasses which are 3.1, 3.2, 3.3, 3.4, 3.5, 3.6 nodes. These sub classes are shown below.

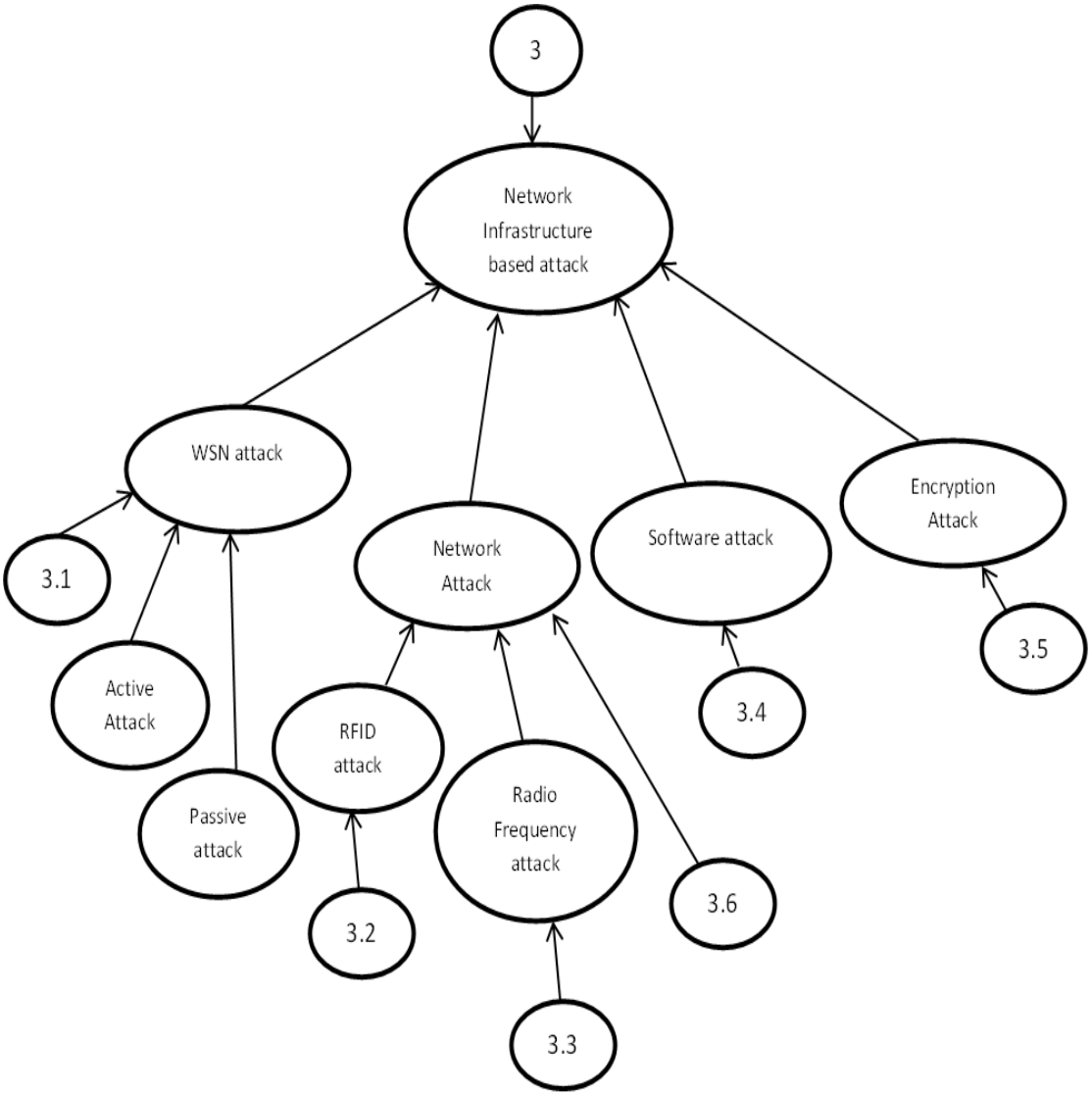

FIGURE 3.10: Conceptual model of network infrastructure base attack

This category shown in figure 3.11 is designed to keep some passive attacks and physical attacks on IoT devices. It is divided into three categories, i.e. analysis attacks, malicious activity attacks and physical attacks which are shown in 4.1, 4.2 and 4.3 node. Analysis and malicious activity attacks are only monitoring base attacks. They monitor the network activity and steal information. On the other hand, physical attacks focused on hardware based attacks. An attacker needs to be very close to hardware to implement these attacks.

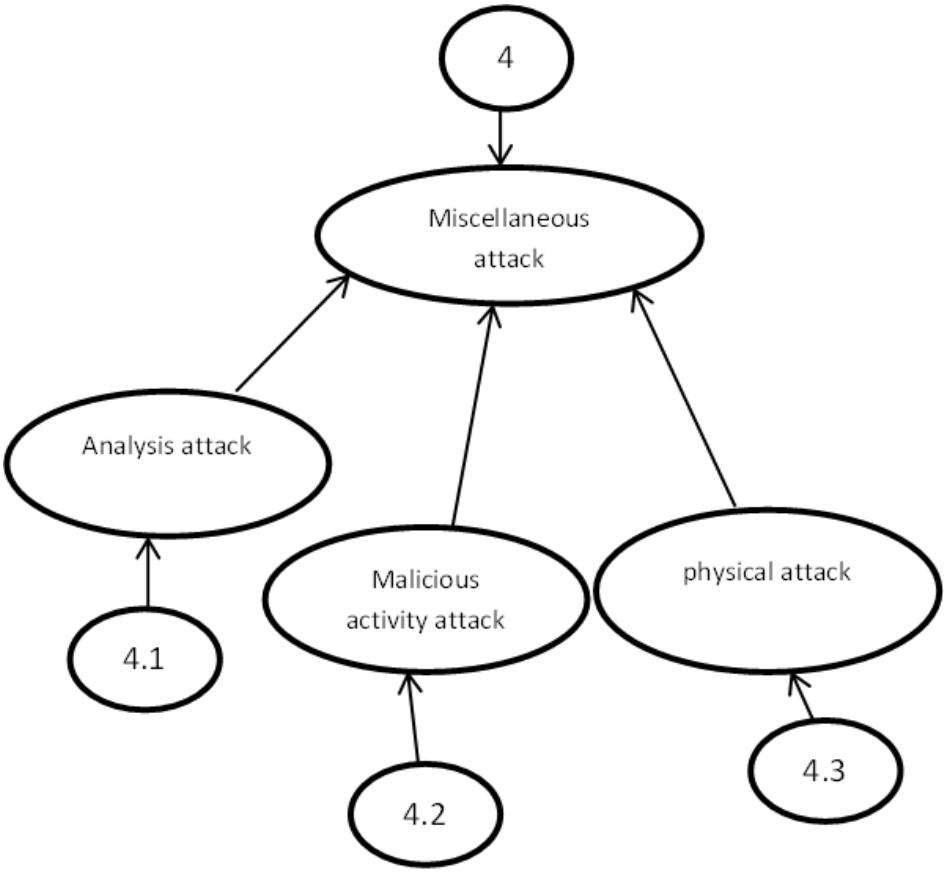

FIGURE 3.11: Conceptual model of miscellaneous attack

Communication protocol shown in figure 3.12 is used to exchange messages between IoT objects and provide a standard way for naming, messaging and controlling. Naming means by which an object of IoT device is recognized. Messaging means how IoT message is structured. Controlling mean manage the flow. It is divided into three subclasses i.e., TLS, application protocol and TCP/UDP protocol. TCP/UDP is transport layer attack. Application protocol based on application layer attacks which compromises the sensitive data. The main target of

such attack is to try to take out the use of Transport Layer Security (SSL/TLS) by manipulating unencrypted protocols.

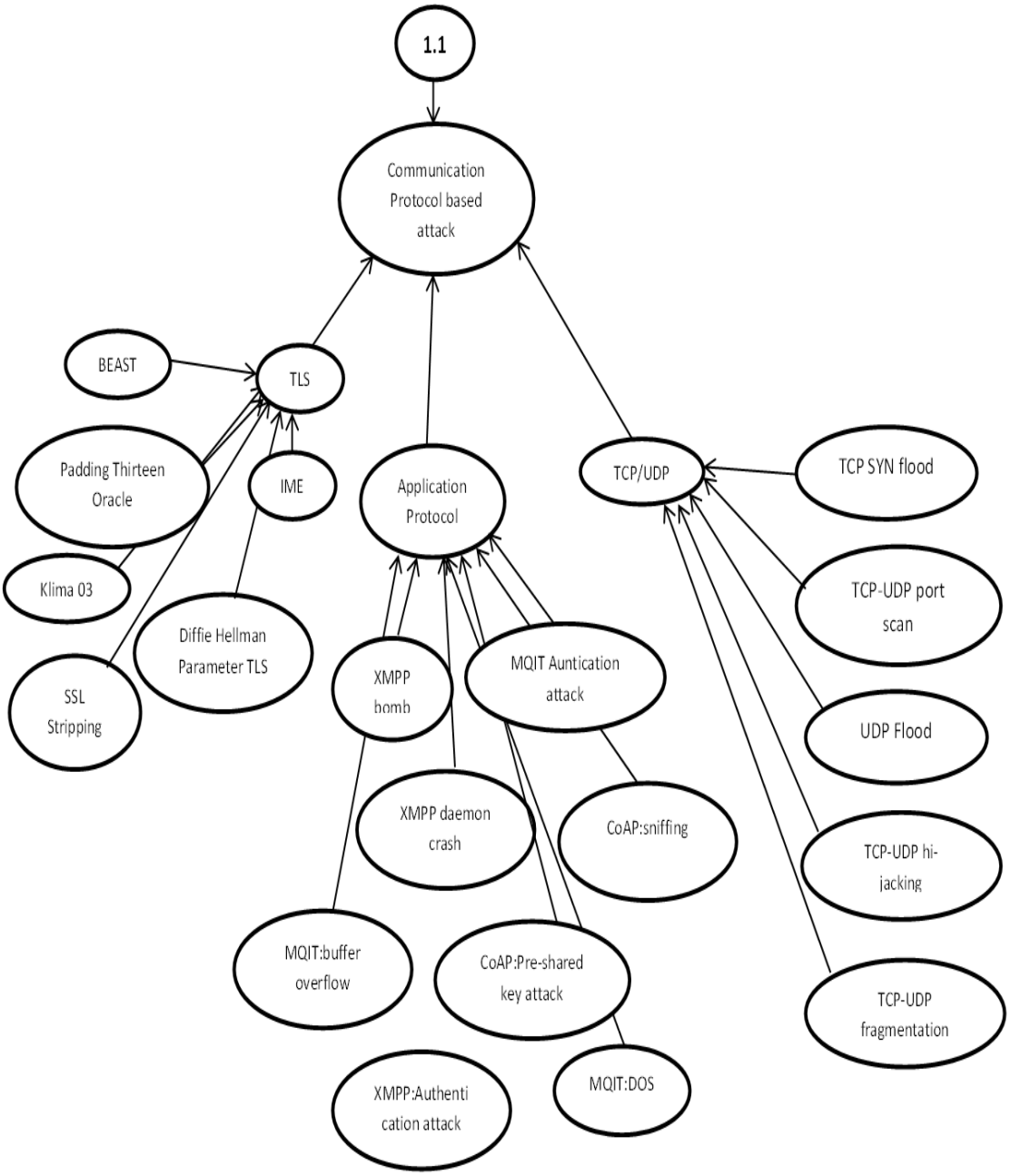

FIGURE 3.12: Conceptual model of communication protocol based attack

As application layer support all sorts of business services such as recognizing valid data, spam data and even malicious data, and filter them. The data in IoT is huge and dynamic so it can easily be compromised by the attacker. Application layer attacks which are shown in 3.13 contains those attacks which compromise its security. Some of its attacks are also repeated in WSN attacks.

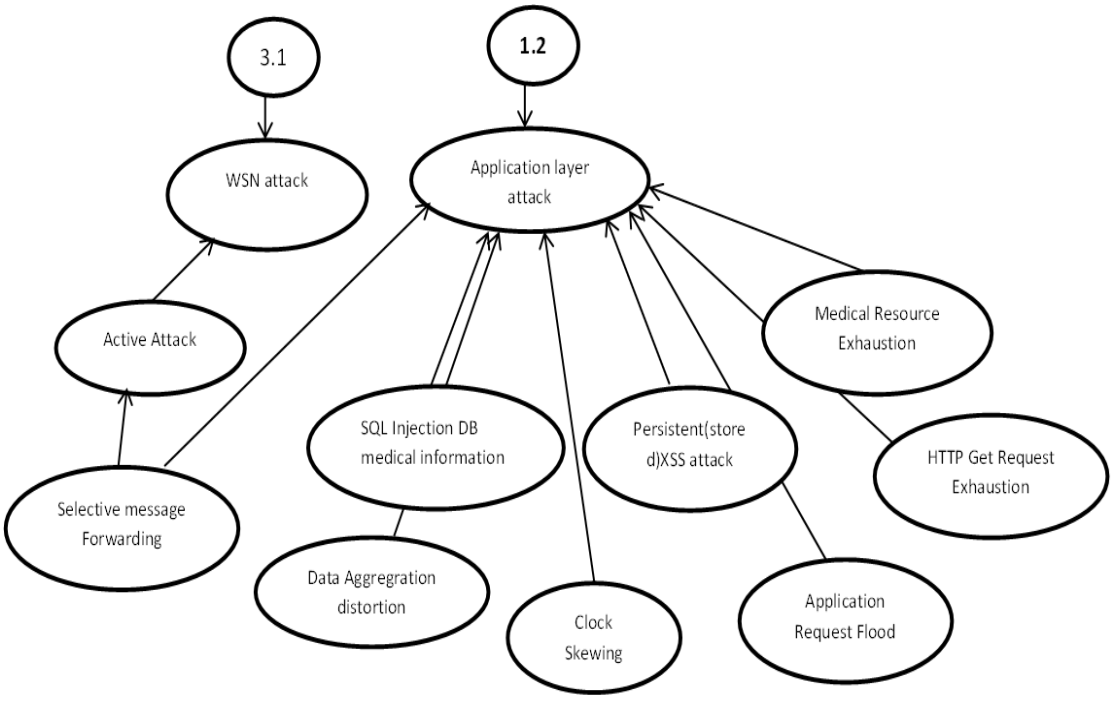

FIGURE 3.13: Conceptual model of application layer attack

Session attacks are shown in figure 3.14 poses a serious threat to all session key schemes in healthcare domain of IoT. Its attacks are repeated in application layer attacks, network attacks and encryption attacks.

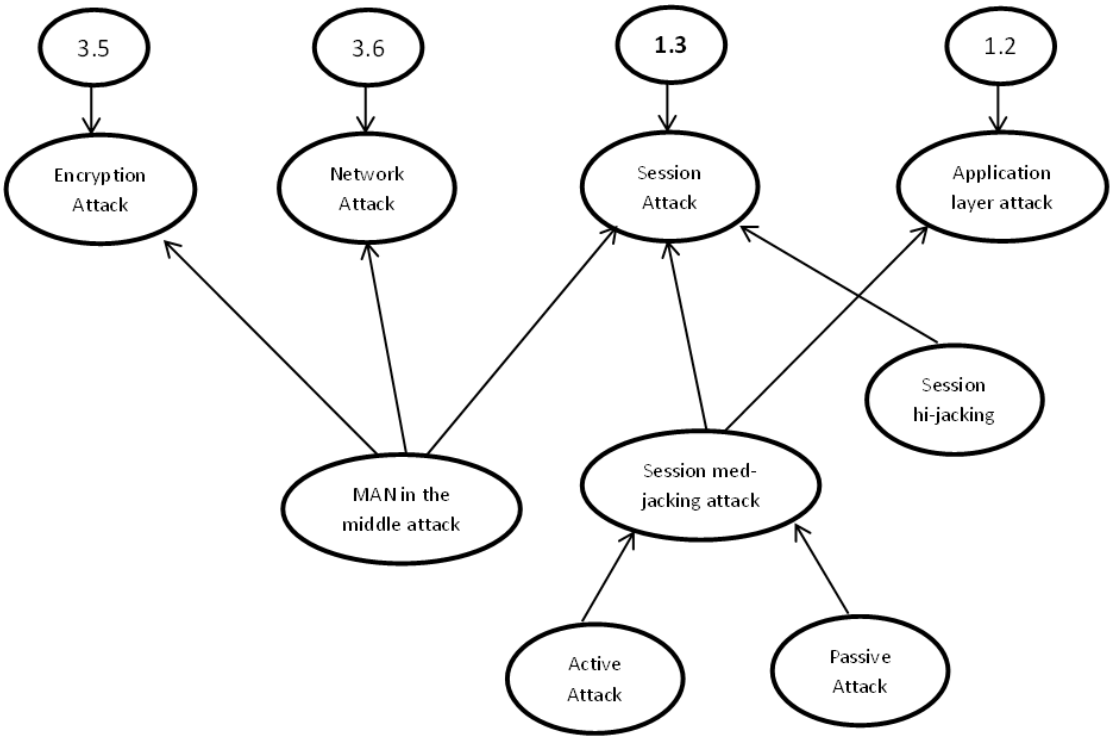

FIGURE 3.14: Conceptual model of session attack

Transport layer can access network, core network and LAN. By accessing network, core network and LAN different attacks can compromise its security which is shown in figure 3.15. It is the combination of heterogeneous network. Its attacks are also repeated in WSN attacks.

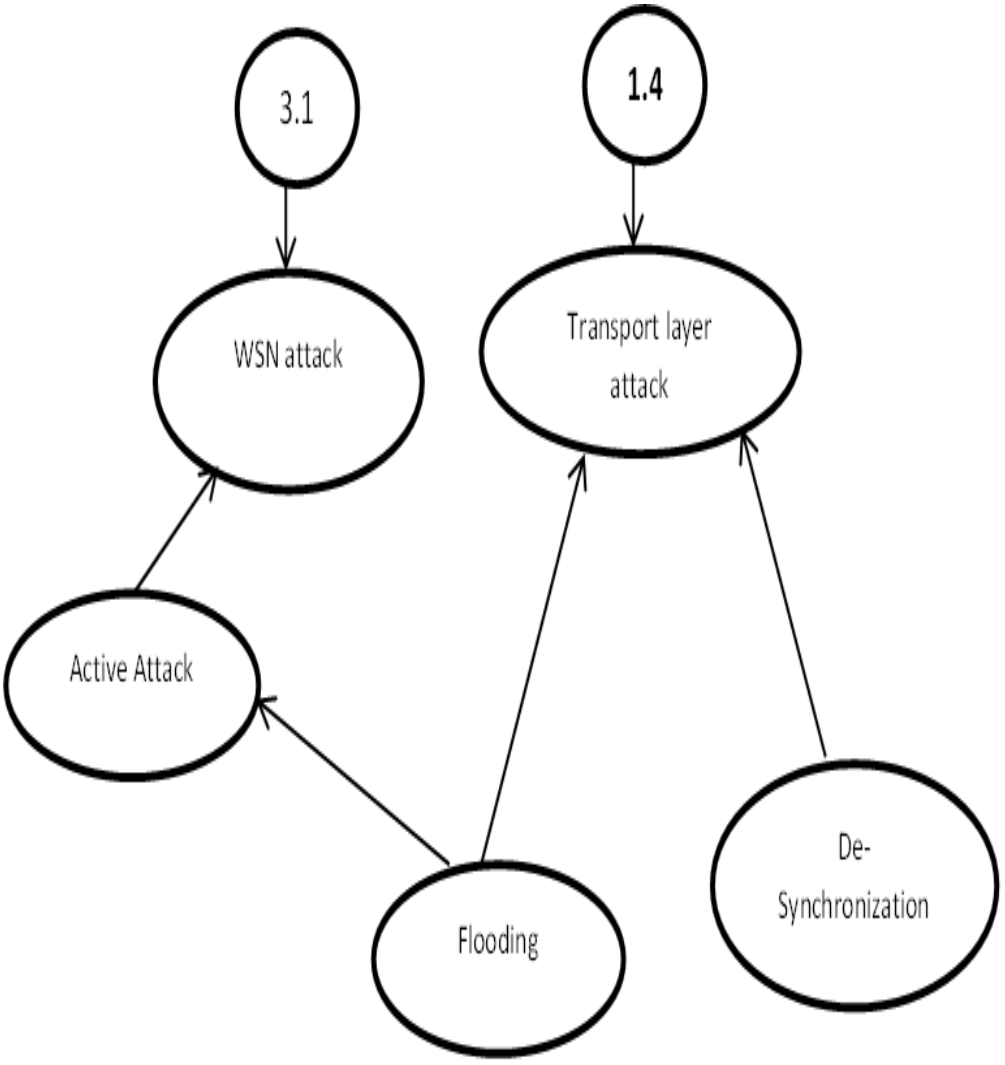

FIGURE 3.15: Conceptual model of transport layer attack

Network/Internet layer is the backbone of IoT base healthcare system. This layer provides services to open interface for the various services related to medical staff and patients. The attacks based on this layer which is shown in figure 3.16 are very crucial. An attacker can compromise the security of every device which is connected to this network. Number of attacks which exist in this model is repeated in many sub classes such as WSN attacks, router attack, network attacks and network protocol attacks.

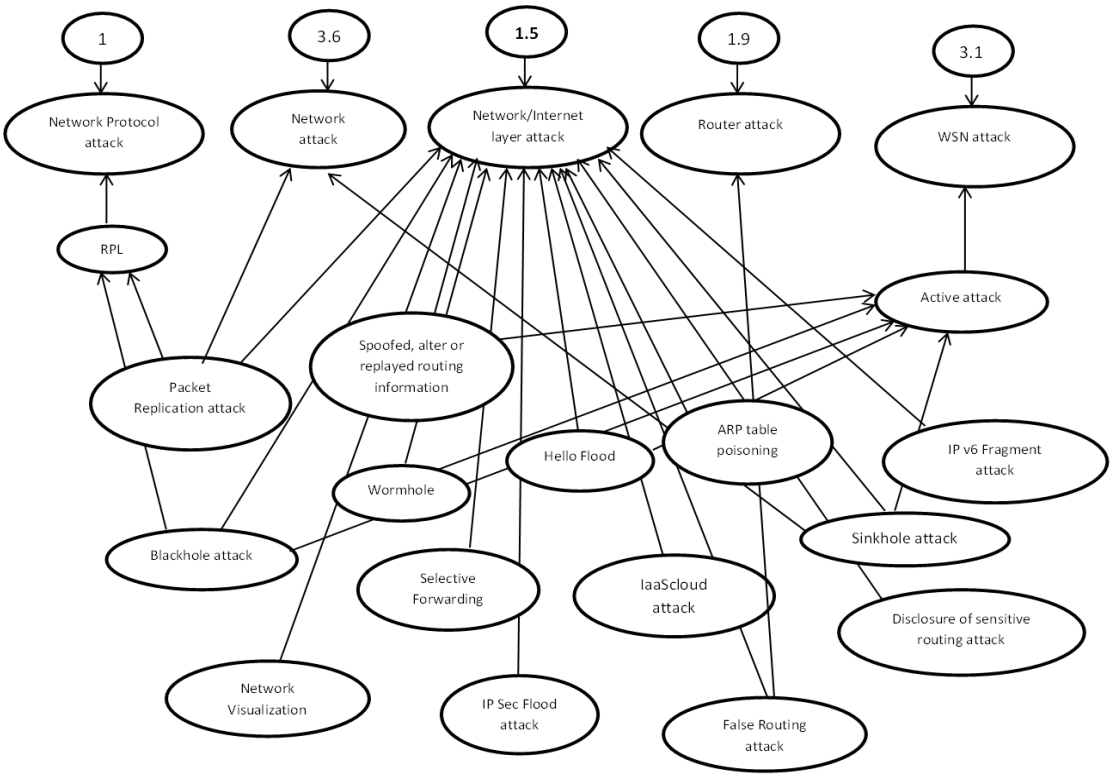

FIGURE 3.16: Conceptual model of network/internet layer attack

Figure 3.17 shows that Data link layer which can transmit data between network entities and detecting and likely correcting errors that may occur in the physical layer. The attacker can intercept data frames on a network, modify or stop them. Its attacks are repeated in WSN attacks as well.

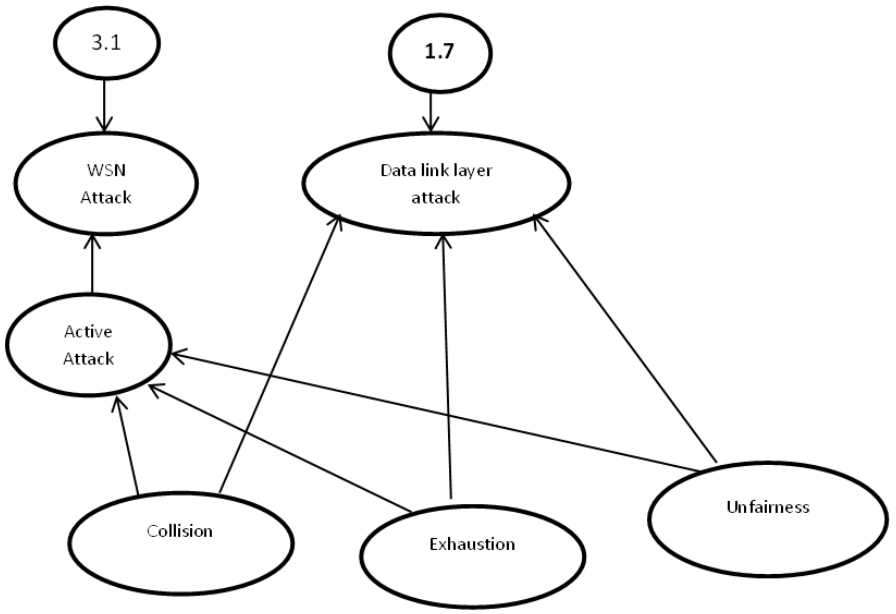

FIGURE 3.17: Conceptual model of data link layer attack

Figure 3.18 shows MAC layer attacks while transmitting the data between IoT objects, node should gain right for a transmission for a specific period of time. Node identification is embedded on packets which are being transmitted. The attacker can easily manipulate the packet.

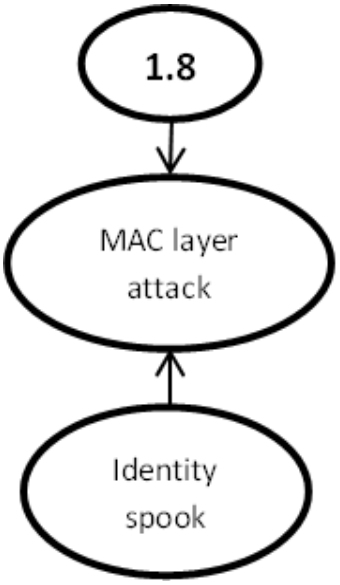

FIGURE 3.18: Conceptual model of MAC layer attack

Those attacks which are shown in figure 3.19 which put impact on network layer are routing attacks. The attacker can target the routing information where data exchange between IoT object occur.

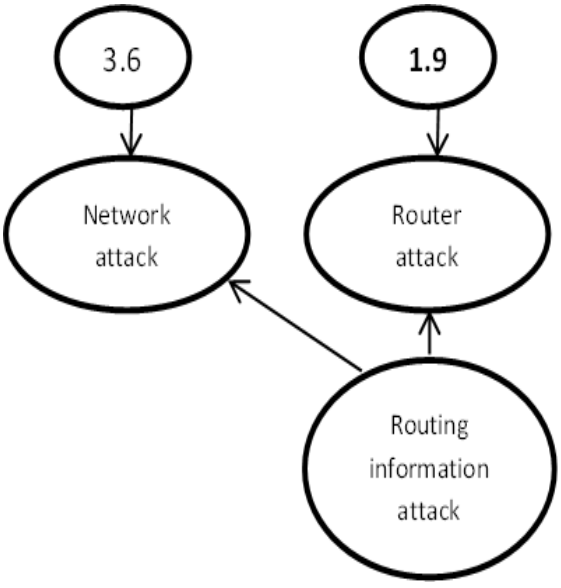

FIGURE 3.19: Conceptual model of router attack

In this model different attacks which are shown in figure 3.20 can affect the data that is in transit or at rest.

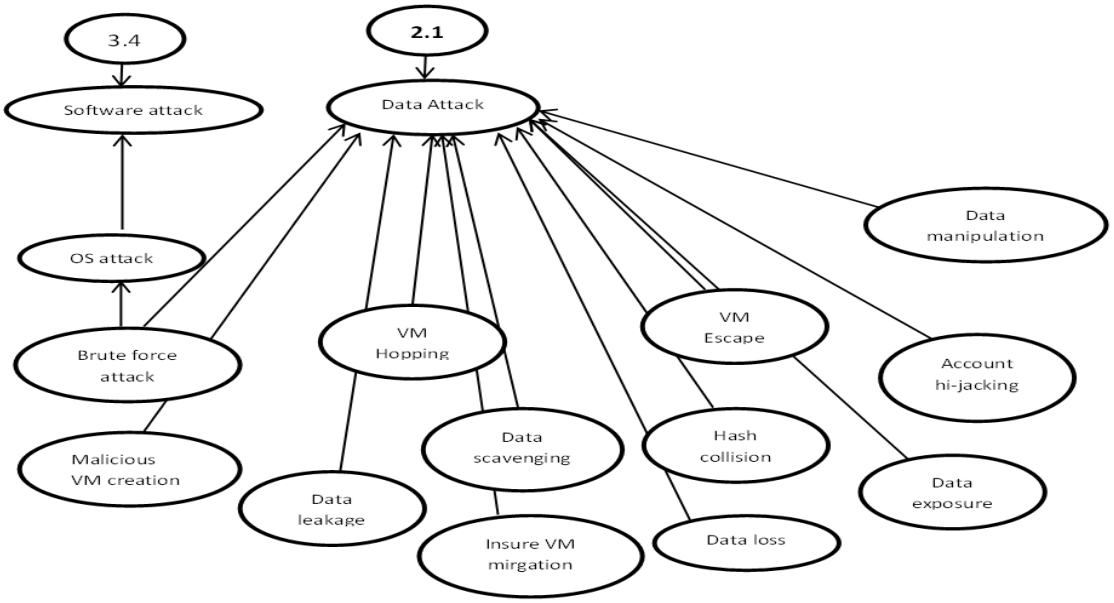

FIGURE 3.20: Conceptual model of data attack

Wireless sensor network is low cost and low power small devices. It is categorized into two subclasses which are shown in figure 3.21. It has two subclasses which are active class and passive class. In active class attack, the attacker can interfere with the radio frequency of nodes and manipulate it while in passive attacks, the attacker can only monitor the network traffic and steal information.

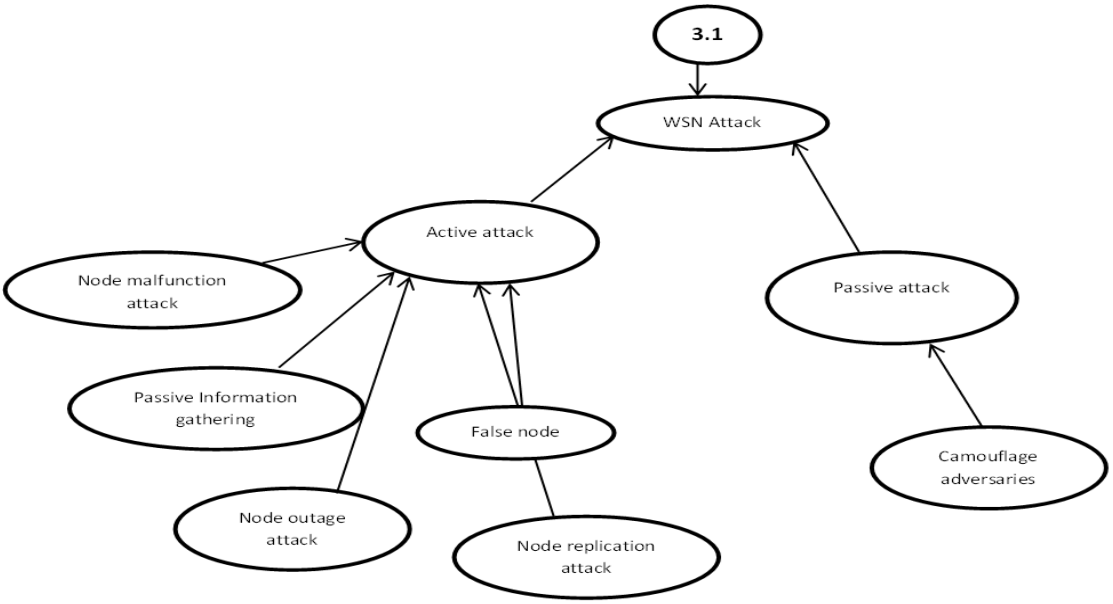

FIGURE 3.21: Conceptual model of WSN attack

IoT object exchange information using RFID (radio frequency identification) technology. There are a lot of attacks which can alter radio frequencies and compromise object's security which are shown in figure 3.22. Some attacks of RFID are also repeated in network attack and physical/perception layer attack.

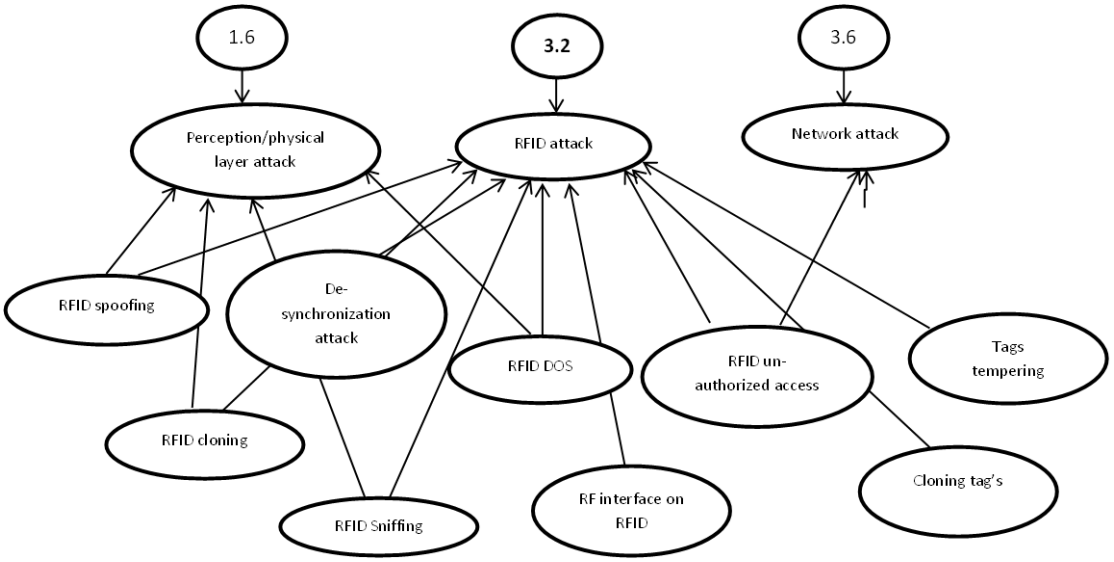

FIGURE 3.22: Conceptual model of RFID attack

Figure 3.23 shows that the attacker can interfere the radio frequency of IoT object to compromise its security.

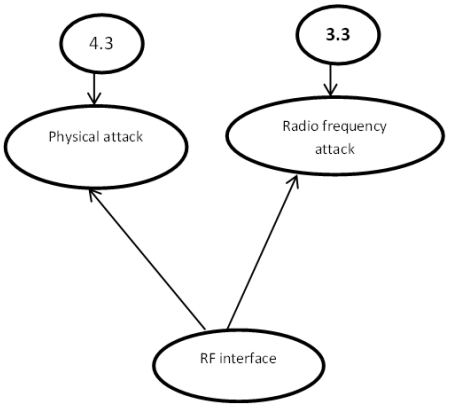

FIGURE 3.23: Conceptual model of radio frequency attack

In IoT objects data security and software security are two different aspects. Software attacks which are shown in figure 3.24 are further divided into three categories i.e. operating system attacks, firmware attacks and application based attacks. In

operating system attacker can attack on IoT object by backdoor attack, unknown attack etc. Majority of IoT devices lack this opportunity to be updated. So attacker can exploit the vulnerability and attack on IoT devices. IoT application attacks are related to IoT web based attacks. These applications are connected to other applications which create a lot of vulnerabilities that an attacker can exploit. A lot of attacks are repeated in WSN attacks, network attacks, application layer attack, router attack, data attack, network layer attack.

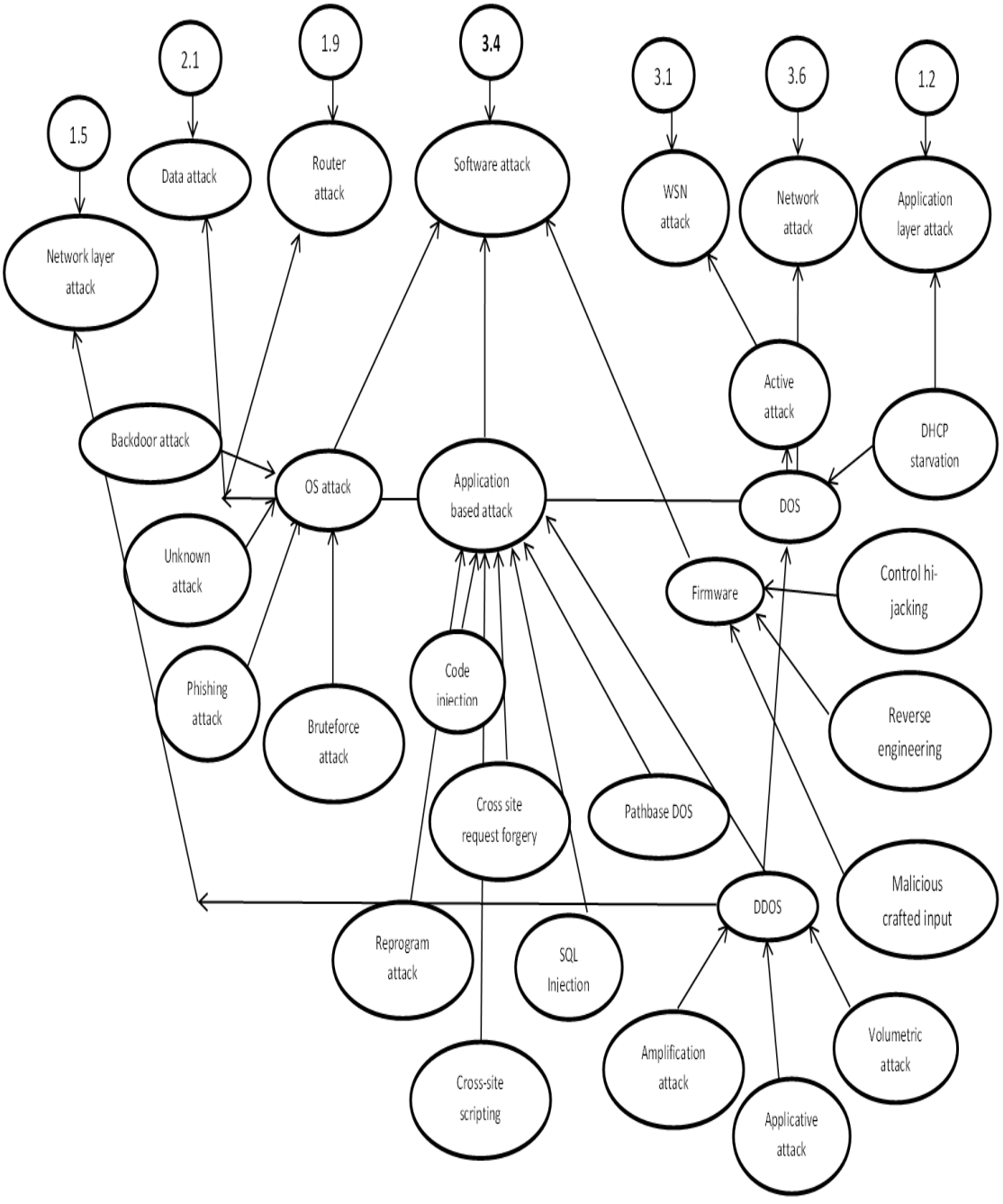

FIGURE 3.24: Conceptual model of software attack

Those attacks which are shown in figure 3.25 destroy encryption schemes and obtain encrypted data related to IoT devices.

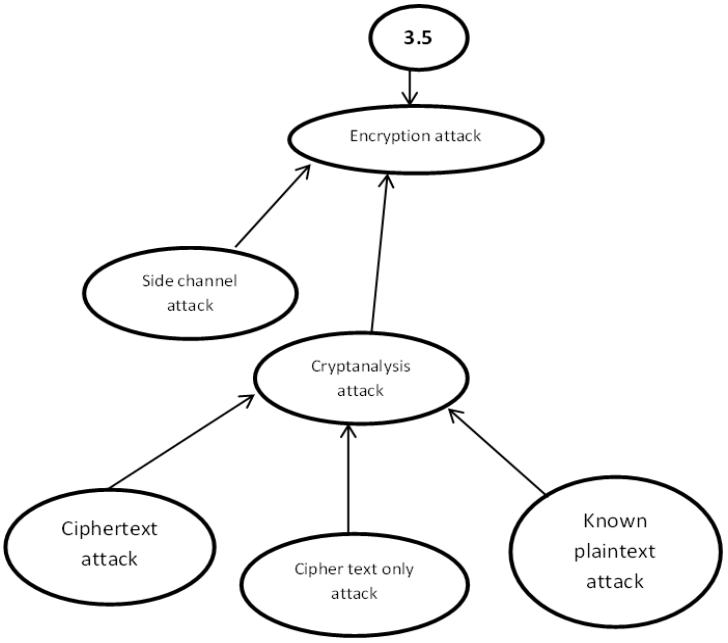

FIGURE 3.25: Conceptual model of encryption attack

Analysis attacks which are shown in figure 3.26 are passive attacks which can only monitor the network data transmission and observe the sensitive information related to IoT devices. These attacks are repeated in WSN attacks, software attacks and network attacks.

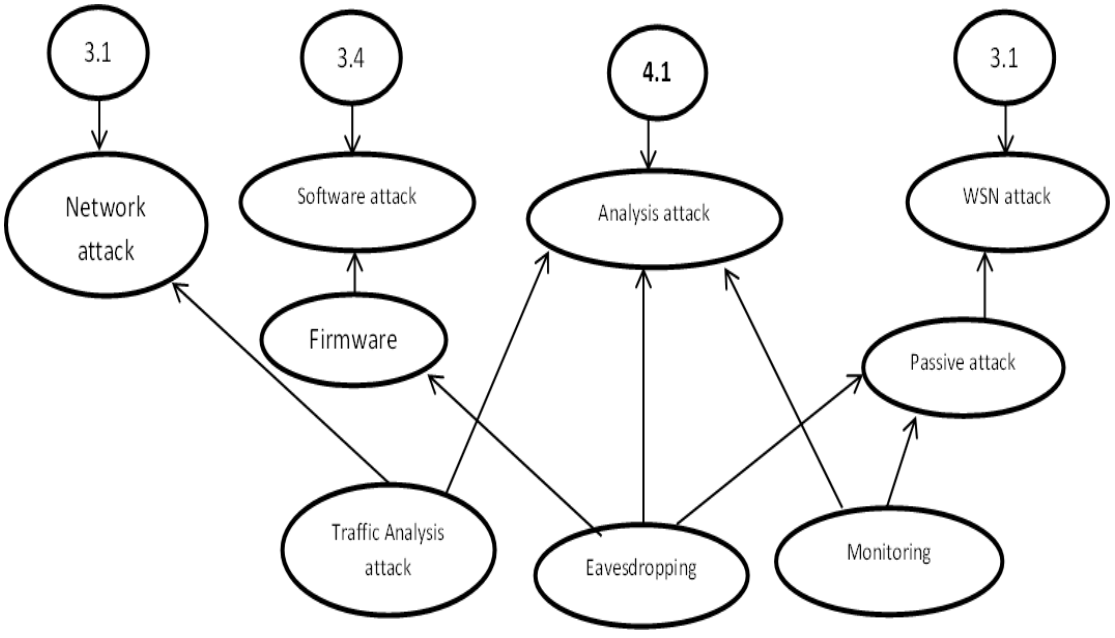

FIGURE 3.26: Conceptual model of analysis attack

The category which is shown in figure 3.27 contains all those attacks which can maliciously alter the flow of information or manipulate data related to IoT devices. Number of attacks which exists in this module is repeated into physical attacks, network layer attacks, application layer attacks, software attacks and WSN attacks.

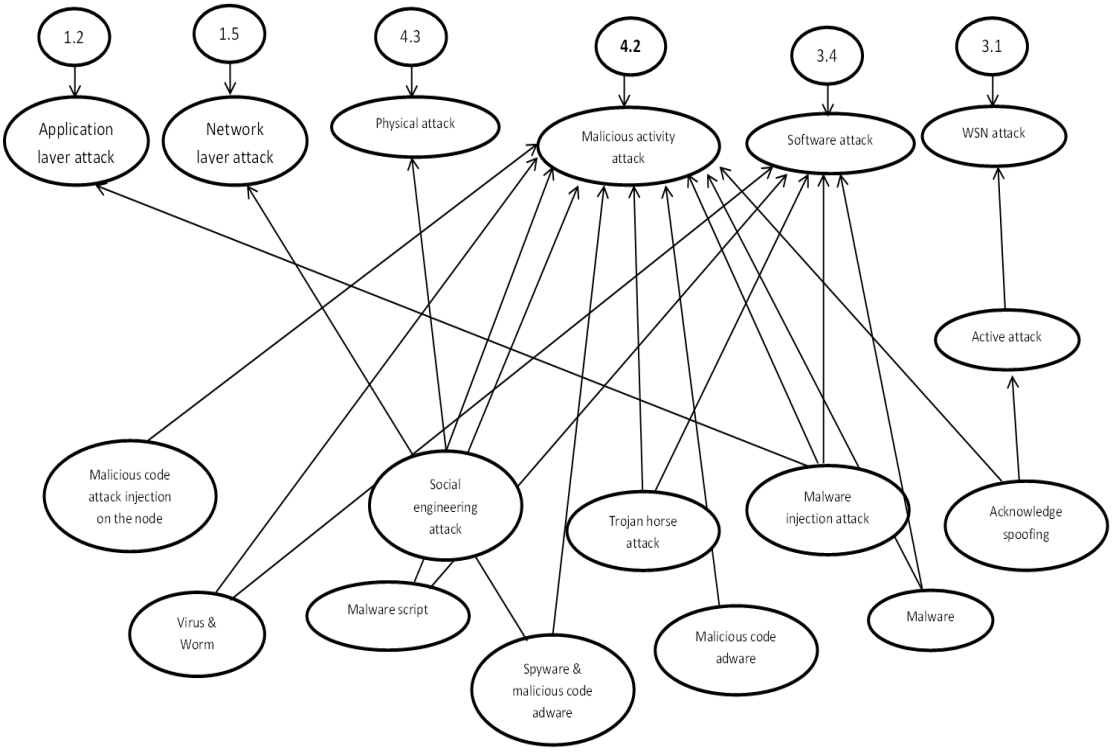

FIGURE 3.27: Conceptual model of malicious activity attack

This type of attacks which is shown in figure 3.28 is focused on destroying the hardware components related to IoT devices.

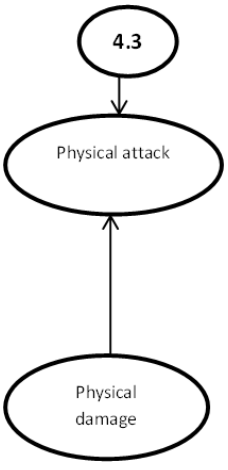

FIGURE 3.28: Conceptual model of physical attack

3.1.3 Ontology Implementation

In this section we discuss the implementation of a comprehensive ontology of information disruption attacks for IoT based healthcare domain which we conceptualized in the previous section. The proposed model consists of all these gathered attacks related to IoT based healthcare system. These attacks are then implemented by using protégé.

Protégé [39] is an open-source tool for the development and management of ontologies by developers. It is more than a tool for terminology editing. It also provides developers with a medium for using terminology in end-user applications. It operates on a broad variety of operating systems, including Windows, Linux, Mac OS X. The new version of Protégé 5.5.0, released on 15 March 2019, is installed and used to build an ontology for the healthcare system based on IoT.

Protégé software is used to implement 67 attacks. These attacks are classified into four main categories which are attack based on network protocols, healthcare data attack, network infrastructure based attack and miscellaneous attacks.

3.1.3.1 Definition of Classes and Sub-Classes

In this section we have used the knowledge from the survey of published techniques from knowledge acquisition and conceptualization. First, we discussed the abstract level classes from IoT based healthcare system. After that we have presented the class hierarchies in a Protégé environment [40] by using Graphviz plugin. Information disruption attacks on IoT have four major child classes which are further divided into nine sub-classes.

Figure 3.29 contains four sub-classes. These classes are classified according to some properties. Attack based on network properties contains the classes which are related to TCP/IP layers attack. Network infrastructure based attacks are related to those attacks which target network through various methods like encryption,

network attack etc. Miscellaneous attacks contains only passive attacks. Health care data attacks are related to actual data which is transmitted within the device.

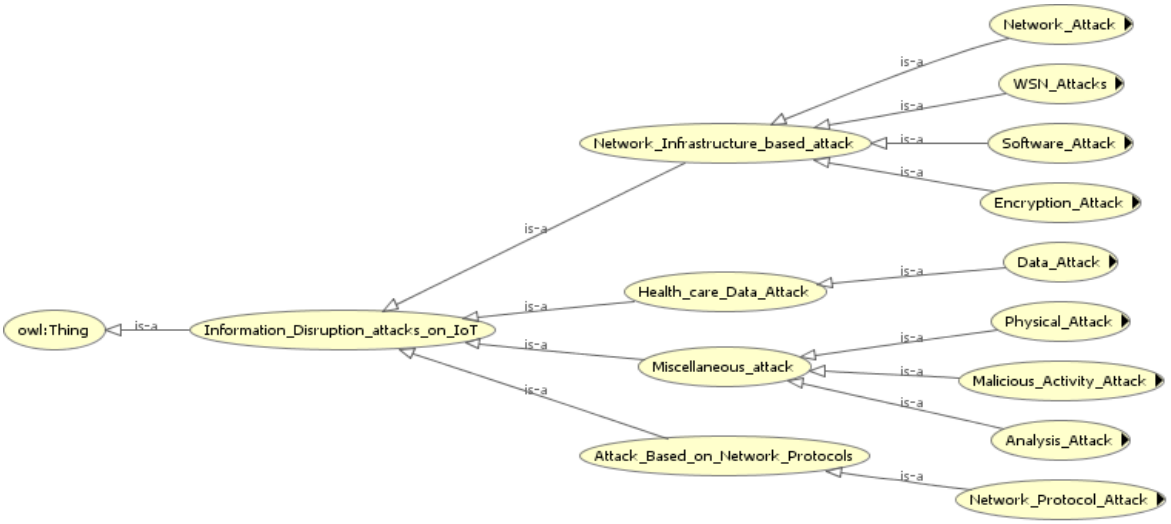

FIGURE 3.29: Abstract classes related to IoT base healthcare system

Attacks based on network protocol shown in figure 3.30 contain five more sub-classes which are related to TCP/IP layer attack, router attack, communication protocol attack, 6loWpan and RPL.

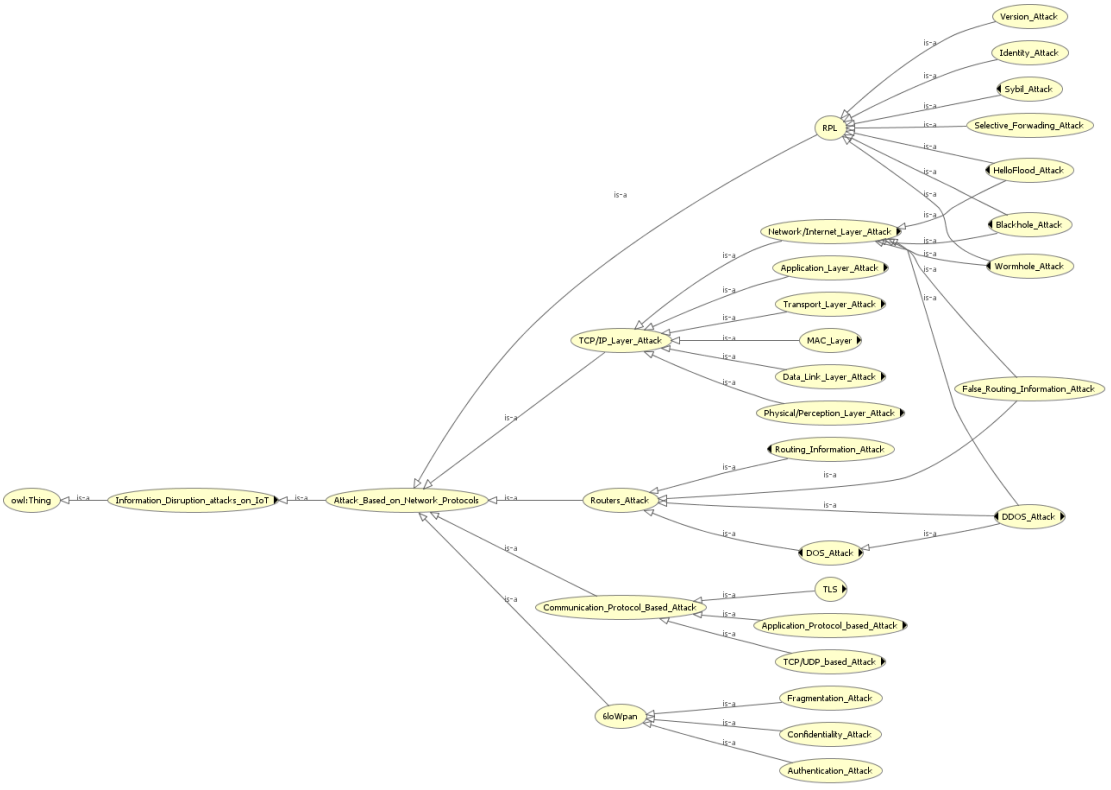

FIGURE 3.30: Sub-Class: Attack based on network protocol

All those attacks that can conveniently modify data in IoT based healthcare devices include in healthcare data attacks shown in figure 3.31.

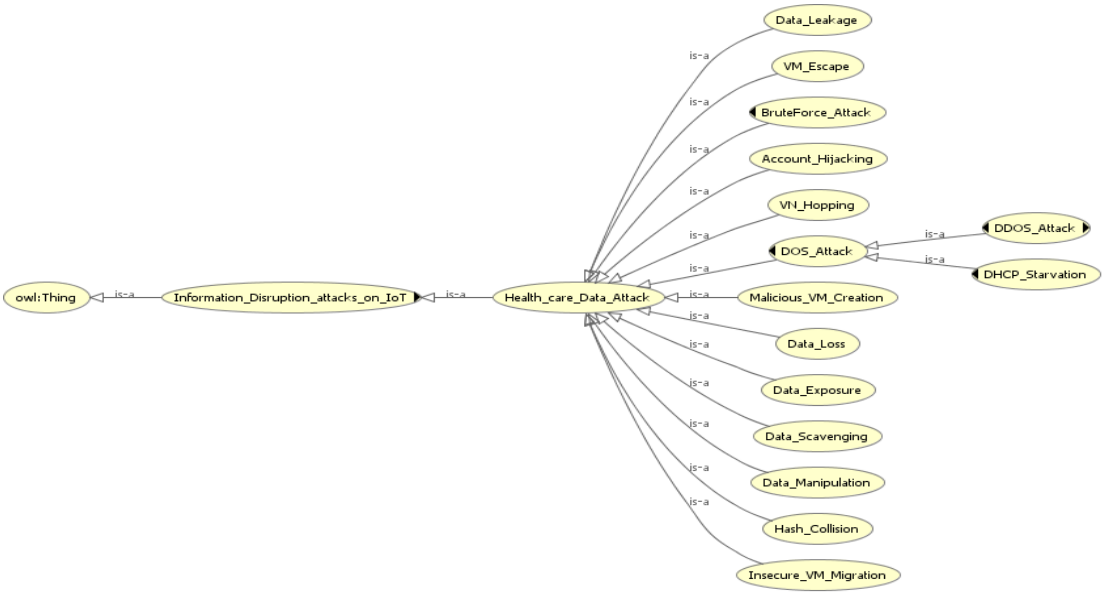

FIGURE 3.31: Sub-Class: Health care data attack

Miscellaneous attacks which is shown in 3.32 are further divided into three sub classs i.e. physical attack, malicious activity attack and analysis attack.

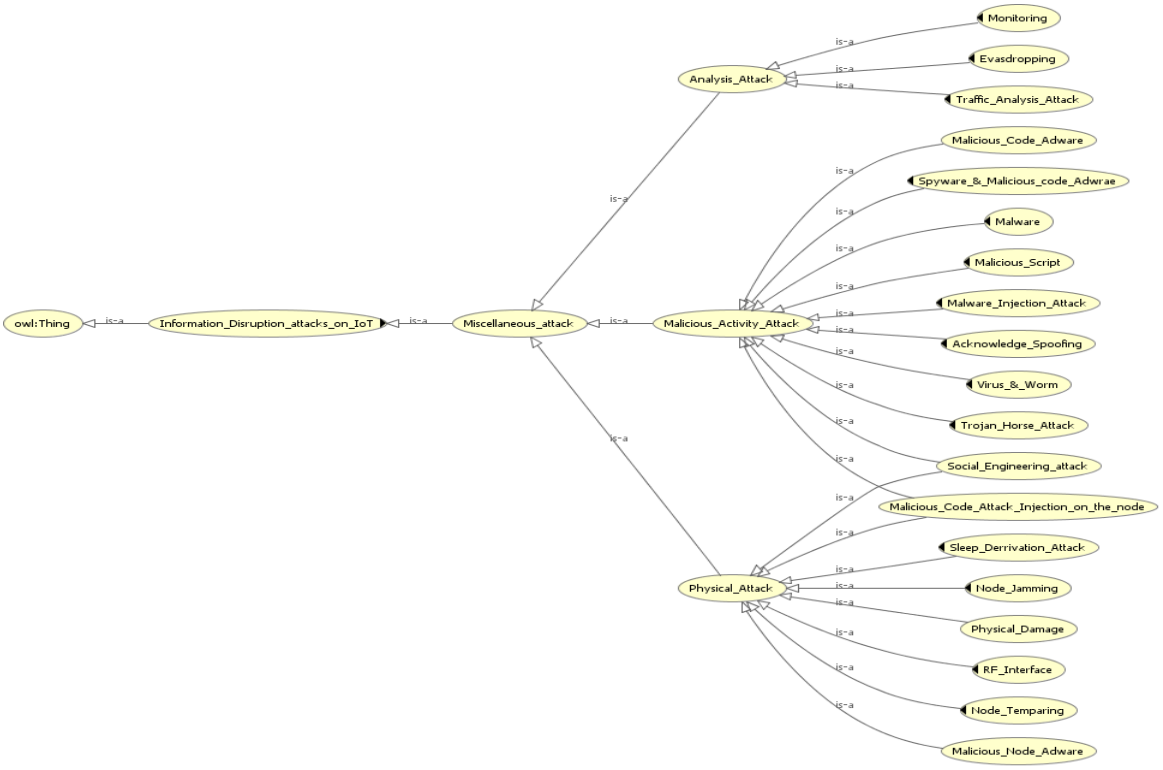

FIGURE 3.32: Sub-Class: Miscellaneous attack

Network infrastructure attacks which is shown in 3.33 are further divided into four sub classes which are software attack, WSN attack, network attack and encryption attack. These attacks damage the network infrastructure.

FIGURE 3.33: Sub-Class: Network infrastructure base attacks

In this section we have implemented the proposed ontology in protégé. Each subclass has a subsumption relationship with its parent class. We apply object property to abstract subclasses of this ontology which are network protocol layer based attacks, health care data attack, network infrastructure base attack and miscellaneous attacks.

3.2 Conclusions

In this chapter we have successfully acquired knowledge related to attacks in IoT base healthcare system. We then make its conceptual model. By using Protégé we have provided detailed ontology of IoT based healthcare system. In the next chapter, we will evaluate our ontology by using standard parameters.

Chapter 4

Ontology Evaluation

There are different methods of ontology evaluation available. In order to use ontologies in various applications effectively, we need to check if these ontologies are good ontologies or not? For this we need to understand the ontology evaluation. In this chapter, we will understand the various parameters of ontology evaluation. The results of these evaluations are discussed in coming sections. We have divided this chapter into the two sections. Section 4.1 shows the ontology evaluation parameters which are further divided into completeness, consistency and accuracy. Section 4.2 concludes this chapter.

4.1 Ontology Evaluation Parameters

Ontologies are considered as reference model [41], [42], [43], [44]. There are seven ontology evaluation parameters which are accuracy, adaptability, clarity, completeness, computational efficiency, conciseness and consistency [34], [45], [46], [47], [48]. The size of ontology may create new problems that affect various phases of ontology, such as real-world ontology and complex ontology. Ontology related to medical field is very complex, such as medicine which involves thousands of concepts. In our ontology, we focused basic three parameters which are completeness, consistency and accuracy. These parameters are considered important to evaluate

every ontology [47].

Completeness: It measures that, if the domain of interest is properly covered in this ontology.

Consistency: It describes that the ontology does not include or allow any contradictions.

Accuracy: This is a criterion that determines whether or not the definition, description of classes and properties in the ontology is correct?

4.1.1 Completeness

In this section evaluation of ontology for completeness is based on user study. At this stage, a questionnaire has designed for domain experts to test this ontology. This questionnaire is available in the Appendix A of the Appendix section. The questionnaire was given to three domain experts along with document of proposed ontology.

Results of user study based evaluation are shown in figures 4.1. This plot represent the statistics of answers from the questionnaire. Following are statements of questions from questionnaire:

1. According to the scope of this research does this ontology fulfill the criteria?
2. Is the proposed ontology more comprehensive than the existing classification?
3. In our proposed ontology, does each subclass falls accurately under parent class?
4. Is the number of classes repeated in different subclasses is clearly modeled and have a relationship?

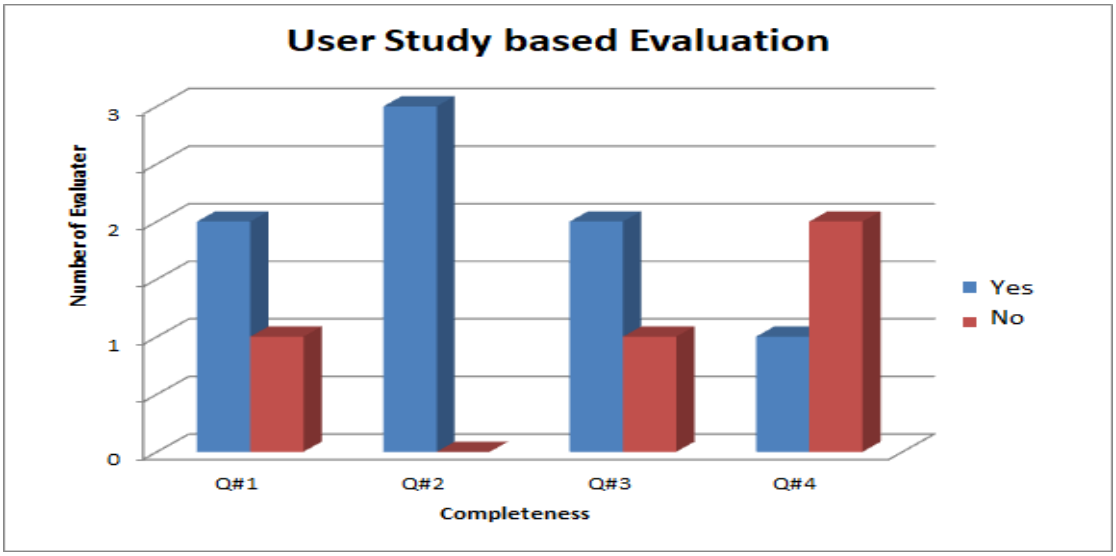

FIGURE 4.1: Plot for User study base evaluation for completeness

Average number of classes in published hierarchies is 18. Our proposed ontology consists of 169 classes which ensure that our proposed ontology is more comprehensive. The number of classes repeated in different subclasses is clearly modeled in the conceptual model in chapter 3. We perform a comparison shown in table 4.1 on published technique with our proposed ontology. This quantitative evaluation of our ontology concludes that our ontology is comprehensive and covers almost all attacks. We will publish our ontology and get feedback from domain scholars.

Published Techniques	**Number of classes exist**	**Proposed ontology classes**
IoT and its security attacks [2]	29	169
Cyber attacks classification in IoT based healthcare [3]	31	169
Classifications of IoT attacks [4]	29	169
Taxonomy of security attacks on IoT [24]	31	169
Layered based attacks with their attack strategies in IoT System [24]	23	169
A categorization of IoT vulnerabilities [28]	3	169
Thematic taxonomy of ML/DL for IoT security [29]	7	169
Potential threats in the IoT system [29]	6	169
OSI layers attacks [13]	13	169
Security attacks on wireless sensor network [9]	20	169

Taxonomy of physical attacks against IoT objects [18]	14	169
Taxonomy of network attacks against IoT objects [18]	13	169
Taxonomy of communication protocols attacks [18]	27	169
Taxonomy of data at rest attacks [18]	14	169
Taxonomy of IoT software [18]	23	169

TABLE 4.1: Comparison between published techniques and proposed ontology

Table 4.1 concludes that published techniques contain classes related to IoT base healthcare. Maximum number of classes exist in published techniques are 31 [3], [24] which are far less than our proposed ontology. On the basis of this conclusion, this ontology is complete.

4.1.2 Consistency

An ontology evaluation tool named Hermit reasoner is used to evaluate our proposed ontology. It is used to determine whether or not the ontology is consistent. It also identifies the subsumption relationship. Figure 4.2 use to represent the Hermit reasoner to evaluate our ontology in Protégé 5.5.0. JFact is also an OWL reasoner. Figure 4.3 use to represent the JFact reasoner to evaluate our ontology. We have not found any error so this ontology is consistent.

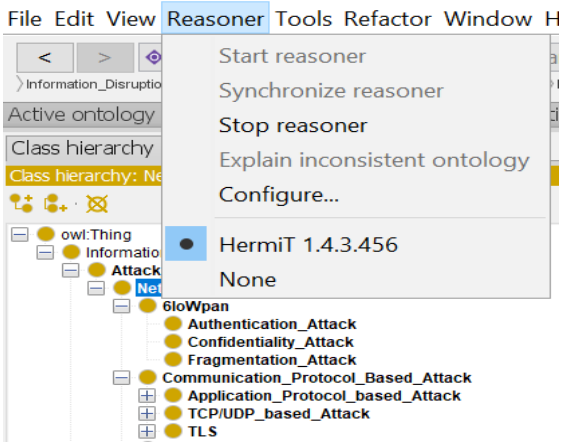

FIGURE 4.2: Hermit Reasoner running without any error

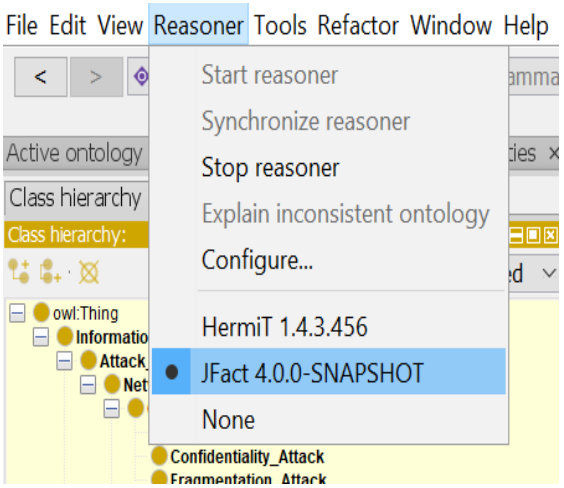

FIGURE 4.3: JFact Reasoner running without any error

4.1.3 Accuracy

In this section accuracy is measured according to the questioner from user study based evaluation. In Figure 4.4 statistics about answers from domain experts are summarized. These domain experts verified the accuracy of our proposed ontology

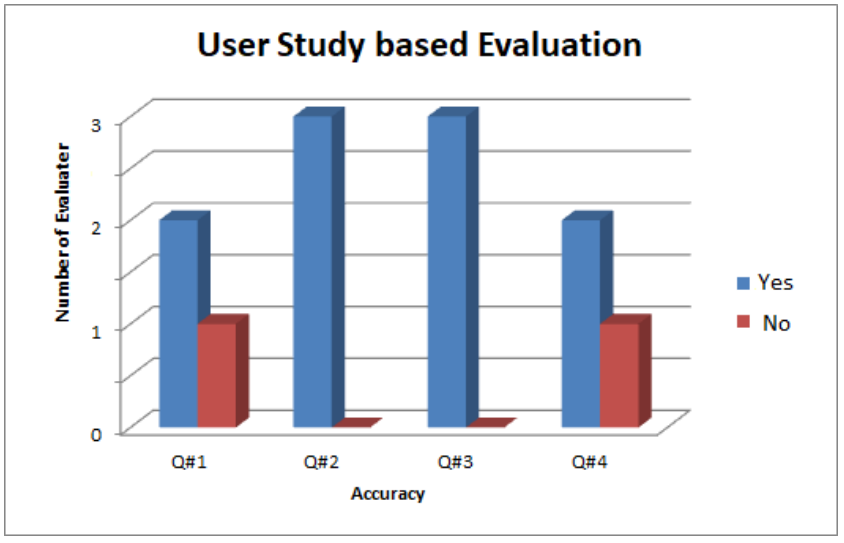

FIGURE 4.4: Plot for User study base evaluation for completeness

by evaluating each abstract class. Each abstract class includes attacks which are conceptually modeled in chapter 3. Each subclass has their own criteria such as attack based on network protocol, network infrastructure base attacks, health care data attack and miscellaneous attacks. The distributions of attacks are based

on that criterion. Our domain expert concludes that our proposed ontology is accurately mapped on protégé.

4.2 Conclusions

In this chapter We have used two ontology evaluation tools (Hermit and JFact reasoners) and user study based evaluation method to evaluate this ontology. By successfully evaluating this ontology in term of completeness, correctness and accuracy. We are certain to publish our ontology on the internet so other researcher can give us feedback regarding the completeness, correctness and accuracy of our ontology.

Chapter 5

Conclusions and Future Work

In this chapter, we are finally concluding the work that we have carried out and discussed in depth in the previous four chapters. This chapter also elaborates the directions in which we would recommend to extend this work in future. The major conclusion from the thesis are listed below:

1. We looked at the different classifications of IoT attacks mentioned in literature and proposed ontology related to IoT attacks.

2. In our research thesis, an ontology named Information Disruption Attacks related to IoT based healthcare system has proposed.

3. There were no comprehensive classification found related to IoT attack based healthcare system. We acquire knowledge related to different attacks of this domain and conceptually modeled it.

4. We implement these conceptual models using protégé 5.5.0 and evaluate this ontology. This ontology was evaluated by using ontology evaluation techniques. These evaluation techniques are user based and tool based.

5. This ontology was found consistent, accurate and complete thus considered as good ontology.

6. We will publish proposed ontology and hoping to get some recommendations from readers. This ontology, according to their views, may be revised.

7. The scientific group can also be assisted by this ontology to expand this proposed ontology. This ontology can help to recognize crucial attacks and to establish countermeasures against these attacks as well.

Bibliography

[1] A. Dean and M. O. Agyeman, "A study of the advances in iot security," in *Proceedings of the 2nd International Symposium on Computer Science and Intelligent Control*, 2018, pp. 1–5.

[2] J. Deogirikar and A. Vidhate, "Security attacks in iot: A survey," in *2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC)*. IEEE, 2017, pp. 32–37.

[3] A. Djenna and D. E. Saïdouni, "Cyber attacks classification in iot-based-healthcare infrastructure," in *2018 2nd Cyber Security in Networking Conference (CSNet)*. IEEE, 2018, pp. 1–4.

[4] I. Andrea, C. Chrysostomou, and G. Hadjichristofi, "Internet of things: Security vulnerabilities and challenges," in *2015 IEEE symposium on computers and communication (ISCC)*. IEEE, 2015, pp. 180–187.

[5] S. R. Islam, D. Kwak, M. H. Kabir, M. Hossain, and K.-S. Kwak, "The internet of things for health care: a comprehensive survey," *IEEE access*, vol. 3, pp. 678–708, 2015.

[6] H. Li, Y. Chen, and Z. He, "The survey of rfid attacks and defenses," in *2012 8th International Conference on Wireless Communications, Networking and Mobile Computing*. ieee, 2012, pp. 1–4.

[7] A. Mitrokotsa, M. R. Rieback, and A. S. Tanenbaum, "Classification of rfid attacks," *Gen*, vol. 15693, no. 14443, p. 14, 2010.

[8] J. S. Kumar and D. R. Patel, "A survey on internet of things: Security and privacy issues," *International Journal of Computer Applications*, vol. 90, no. 11, 2014.

[9] A. Wahid and P. Kumar, "A survey on attacks, challenges and security mechanisms in wireless sensor network," *International Journal for Innovative Research in Science and Technology*, vol. 1, no. 8, pp. 189–196, 2015.

[10] A. Mpitziopoulos, D. Gavalas, C. Konstantopoulos, and G. Pantziou, "A survey on jamming attacks and countermeasures in wsns," *IEEE Communications Surveys & Tutorials*, vol. 11, no. 4, pp. 42–56, 2009.

[11] A. Kardi and R. Zagrouba, "Attacks classification and security mechanisms in wireless sensor networks."

[12] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: Attacks and countermeasures," *Ad hoc networks*, vol. 1, no. 2-3, pp. 293–315, 2003.

[13] D. Kaur and P. Singh, "Various osi layer attacks and countermeasure to enhance the performance of wsns during wormhole attack," *International Journal on Network Security*, vol. 5, no. 1, p. 62, 2014.

[14] J. A. Manrique, J. S. Rueda-Rueda, and J. M. Portocarrero, "Contrasting internet of things and wireless sensor network from a conceptual overview," in *2016 IEEE international conference on Internet of Things (iThings) and IEEE green computing and communications (GreenCom) and IEEE cyber, physical and social computing (CPSCom) and IEEE smart data (SmartData)*. IEEE, 2016, pp. 252–257.

[15] M.-L. Messai, "Classification of attacks in wireless sensor networks," *arXiv preprint arXiv:1406.4516*, 2014.

[16] W. Wang, S. De, R. Toenjes, E. Reetz, and K. Moessner, "A comprehensive ontology for knowledge representation in the internet of things," in *2012 IEEE*

11th International Conference on Trust, Security and Privacy in Computing and Communications. IEEE, 2012, pp. 1793–1798.

[17] A. S. A. Sukor, A. Zakaria, N. A. Rahim, L. M. Kamarudin, R. Setchi, and H. Nishizaki, "A hybrid approach of knowledge-driven and data-driven reasoning for activity recognition in smart homes," *Journal of Intelligent & Fuzzy Systems*, vol. 36, no. 5, pp. 4177–4188, 2019.

[18] H. A. Abdul-Ghani, D. Konstantas, and M. Mahyoub, "A comprehensive iot attacks survey based on a building-blocked reference model," *International Journal of Advanced Computer Science and Applications*, vol. 9, no. 3, pp. 355–373, 2018.

[19] S. J. Bhasha and P. Sunita, "An iot-based body area network in medical care system: Related challenges and issues," *International Journal of Innovative Technology and Exploring Engineering (IJITEE)*, vol. 9, no. 1, pp. 541–546, 2019.

[20] F. Meneghello, M. Calore, D. Zucchetto, M. Polese, and A. 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.

[21] M. F. Elrawy, A. I. Awad, and H. F. Hamed, "Intrusion detection systems for iot-based smart environments: a survey," *Journal of Cloud Computing*, vol. 7, no. 1, pp. 1–20, 2018.

[22] K. Zhao and L. Ge, "A survey on the internet of things security," in *2013 Ninth international conference on computational intelligence and security*. IEEE, 2013, pp. 663–667.

[23] D. E. Kouicem, A. Bouabdallah, and H. Lakhlef, "Internet of things security: A top-down survey," *Computer Networks*, vol. 141, pp. 199–221, 2018.

[24] M. Nawir, A. Amir, N. Yaakob, and O. B. Lynn, "Internet of things (iot): Taxonomy of security attacks," in *2016 3rd International Conference on Electronic Design (ICED)*. IEEE, 2016, pp. 321–326.

[25] Q. Jing, A. V. Vasilakos, J. Wan, J. Lu, and D. Qiu, "Security of the internet of things: perspectives and challenges," *Wireless Networks*, vol. 20, no. 8, pp. 2481–2501, 2014.

[26] I. Stellios, P. Kotzanikolaou, M. Psarakis, C. Alcaraz, and J. Lopez, "A survey of iot-enabled cyberattacks: Assessing attack paths to critical infrastructures and services," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 4, pp. 3453–3495, 2018.

[27] H. Tao, M. Z. A. Bhuiyan, A. N. Abdalla, M. M. Hassan, J. M. Zain, and T. Hayajneh, "Secured data collection with hardware-based ciphers for iot-based healthcare," *IEEE Internet of Things Journal*, vol. 6, no. 1, pp. 410–420, 2018.

[28] 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 Communications Surveys & Tutorials*, vol. 21, no. 3, pp. 2702–2733, 2019.

[29] 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," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 3, pp. 1646–1685, 2020.

[30] M. Farooq, M. Waseem, S. Mazhar, A. Khairi, and T. Kamal, "A review on internet of things (iot)," *International Journal of Computer Applications*, vol. 975, no. 8887, pp. 1–7, 2015.

[31] I. B. Ida, A. Jemai, and A. Loukil, "A survey on security of iot in the context of ehealth and clouds," in *2016 11th International Design & Test Symposium (IDT)*. IEEE, 2016, pp. 25–30.

[32] K. S. Gill, S. Saxena, and A. Sharma, "Taxonomy of security attacks on cloud environment: A case study on telemedicine," in *2019 Amity International Conference on Artificial Intelligence (AICAI)*. IEEE, 2019, pp. 454–460.

[33] K. Sonar and H. Upadhyay, "A survey: Ddos attack on internet of things," *International Journal of Engineering Research and Development*, vol. 10, no. 11, pp. 58–63, 2014.

[34] A. Aviad, K. Wecel, and W. Abramowicz, "The semantic approach to cyber security towards ontology based body of knowledge," in *European Conference on Cyber Warfare and Security*. Academic Conferences International Limited, 2015, p. 328.

[35] R. Gurunath, M. Agarwal, A. Nandi, and D. Samanta, "An overview: security issue in iot network," in *2018 2nd International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC) I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC), 2018 2nd International Conference on*. IEEE, 2018, pp. 104–107.

[36] S. Li, L. Da Xu, and S. Zhao, "The internet of things: a survey," *Information Systems Frontiers*, vol. 17, no. 2, pp. 243–259, 2015.

[37] M. A. Musen, "The protégé project: A look back and a look forward," *AI Matters*, vol. 1, no. 4, p. 412, Jun. 2015. [Online]. Available: https://doi.org/10.1145/2757001.2757003

[38] D. Jones, T. Bench-Capon, and P. Visser, "Methodologies for ontology development," 1998.

[39] Protege offical website. [Online]. Available: https://protege.stanford.edu/

[40] J. H. Gennari, M. A. Musen, R. W. Fergerson, W. E. Grosso, M. Crubézy, H. Eriksson, N. F. Noy, and S. W. Tu, "The evolution of protégé: an environment for knowledge-based systems development," *International Journal of Human-computer studies*, vol. 58, no. 1, pp. 89–123, 2003.

[41] J. Pak and L. Zhou, "A framework for ontology evaluation," in *Workshop on E-Business*. Springer, 2009, pp. 10–18.

[42] N. Guarino, D. Oberle, and S. Staab, "What is an ontology?" in *Handbook on ontologies*. Springer, 2009, pp. 1–17.

[43] P. Simons, "Parts: A study in ontology," 1999.

[44] B. Smith, "Ontology," 2003.

[45] J. Raad and C. Cruz, "A survey on ontology evaluation methods," in *Proceedings of the International Conference on Knowledge Engineering and Ontology Development, part of the 7th International Joint Conference on Knowledge Discovery, Knowledge Engineering and Knowledge Management*, 2015.

[46] J. Brank, M. Grobelnik, and D. Mladenic, "A survey of ontology evaluation techniques," in *Proceedings of the conference on data mining and data warehouses (SiKDD 2005)*, vol. 17. Citeseer Ljubljana, Slovenia, 2005.

[47] A. Gómez-Pérez, "Ontology evaluation," in *Handbook on ontologies*. Springer, 2004, pp. 251–273.

[48] H. Hlomani and D. Stacey, "Approaches, methods, metrics, measures, and subjectivity in ontology evaluation: A survey," *Semantic Web Journal*, vol. 1, no. 5, pp. 1–11, 2014.

Appendix A Questioner for user based evaluation of completeness

The following table represents a questionnaire which was given to different domain experts. This questionnaire contains four questions related to the completeness of ontology. These questions can be answered Yes/No. After getting feedback from experts on these questionnaires, statistical measures regarding results for evaluation of completeness were computed.

A sample questionnaire for user study based for completeness.

Question	**Type of Question**	**Answer**
According to the scope of this research does this ontology fulfill the criteria?	Yes/No	
Is the proposed ontology more comprehensive than the existing classification?	Yes/No	
In our proposed ontology, does each subclass falls accurately under parent class?	Yes/No	
Is the number of classes repeated in different subclasses is clearly modeled and have a relationship?	Yes/No	