POLITECNICO
DI TORINO

UNIVERISITY OF POLYTECNICO DI TORINO

MASTER'S THESIS

Risk based Adaptive Authentication for IoT in Smart Home eHealth

---

Author: Mattias Tsegaye Gebrie

Master of Science in Computer Engineering

Submission date: Nov 2017.

Supervisors: Habtamu Abie, PhD (Norwegian Computing Center)
Prof. Prinetto Paolo Ernesto
Eng. Giuseppe Airò Farulla

Abstract

Health care is one of the primary beneficiaries of the technological revolution created by Internet of Things (IoT). In the implementation of health care with IoT, wireless body area network (WBAN) is a suitable communication tool. That being the case security has been one of the major concerns to efficiently utilize the services of WBAN. The diverse nature of the technologies involved in WBAN, the broadcast nature of wireless networks, and the existence of resource constrained devices are the main challenges to implement heavy security protocols for WBAN.

This thesis aims to develop a risk-based adaptive authentication mechanism which continuously monitors the channel characteristics variation, analyzes a potential risk using naive Bayes machine learning algorithm and performs adaptation of the authentication solution. Our solution validates both the authenticity of the user and the device. In addition we evaluate the resource need of the selected authentication solution and provide an offloading functionality in case of scarce resource to perform the selected protocol. The approach is novel because it defines the whole adaptation process and methods required in each phase of the adaptation. The paper also briefly describes the evaluation use case - Smart Home eHealth.

Acknowledgment

No matter how fascinating the subject matter, there was a real challenge to produce this thesis. The challenge lies in holding into the single-mindedness, drive and focus required to research, produce new ideas and write the thesis for the period of time required to complete it.

I could not have reached to this point without my supervisor Habtamu Abie, PhD for he provided me all the possible supports and allowed me the complete freedom to define and explore my ideas in this thesis. I would like to extend my acknowledgement also to Prof. Prinetto Paolo Ernesto and Eng. Giuseppe Airò Farulla for their tireless and prompt support.

My sincere thanks to those who contributed by proofreading all my drafts and drew my attention to strange sentences I constructed during the highly pressurized days. Special thanks must also go to my wife Bezawit and my children Emada and Abem for their understanding and provision of unrestricted support and encouragement.

And finally, thanks to the almighty God for the abundant wisdom and guidance He provided at all times.

Contents

List of Figures

List of Tables

List of Acronyms

AP	Access Point
API	Application Program Interface
BCU	Body Control Unit
BN	Bayesian Network
COAP	Constrained Application Protocol
DOS	Denial of Service Attack
DT	Decision Tree
DTLS	Data Transport Layer Security
ECC	Elliptic Curve Cryptography
ECG	Electrocardiography
EEG	Electroencephalography
EMG	Electromyography
EPC	Electronic Product Code
IEEE	Institute of Electrical and Electronics Engineers
IoT	Internet of Things
IoV	Internet of vehicles
IoE	Internet of Energy
IoS	Internet of Sensors
LR	Linear Regression
M2M	Machine to Machine
MAC	Medium Access Control
MQQT	Message Queue Telemetry Transport
NB	Naïve Bayes

NN	Neural Network
OAuth	Open Authorization
PD	Personal Device
PKC	Public Key Cryptography
RF	Radio Frequency
RFC	Request for Comments
RFID	Radio-frequency identification
RSSI	Received Signal Strength Indicator
SPO2	oxygen saturation
SSL	Secure Socket Layer
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UDP	User Datagram Protocol
UWB	Ultra wideband
WBAN	Wireless Body Area Network
WirelessHART	Wireless Highway Addressable Remote Transducer Protocol
WPAN	Wireless Personal Area Network
WSN	Wireless Sensor Network
ZigBee	

CHAPTER ONE

1. Introduction

The future Smart Homes are expected to deliver many kinds of services, with particular regards to Health care. Integration of health care system in to a Smart Home will enable the provision of high quality, low cost and easily accessible care to the ever increasing population of the world particulalry the elderly suffering from age related diseases [1]. One way to implement health care system in Smart Home is the use of wearable sensor nodes, actuators nodes and wireless communication technologies, which is referred to as wireless body area network (WBAN). A WBAN is a collection of low-power and lightweight wireless sensor nodes, with limited computation, communication and storage capacity [2]. Keeping WBAN and its supporting infrastructure safe and sound is a challenging task in dynamic environment such as a Smart Home.

WBAN contains diverse set of devices with different communication, processing, battery life and memory capacity. The fact that the devices involved in the network are unattended and communicate wirelessly create a large threat surface for attacks, an attack that makes one of the nodes to malfunction or the network vulnerable to data stealing. Data is collected, processed and transmitted by the network are confidential and sensitive in nature. Moreover, an attack on one of the nodes in the network, to break it of force it to misbehave, may lead a patient to a dangerous condition and sometimes to death. Thus, stringent and scalable security mechanisms are required to prevent malicious interaction with WBAN [3].

One way of maintaining the integrity and security of such a network is authentication. It is a means to identify and verify a device/user who it claims to be. Existing conventional high-level authentication mechanisms can only monitor a particular infrastructure unit and safeguard a particular service. They focus on building a bigger and bigger fortress around infrastructures and services in order to make breaching unlikely. These kinds of authentication solutions are platform specific and cannot protect a system against ever-changing attacks and vulnerabilities, while taking into account constrained resource and dynamic network.

A compromised node in WBAN can intercept the communication among legitimate nodes, as a result compromising privacy of the whole network data. Thus, a secure authentication mechanism of node and data is crucial for the privacy and security of the system. To ensure authentication in WBAN networks, we need a mechanism which automatically proves all the communicating nodes are trusted ones.

These challenges demand a risk aware and an adaptive authentication solution that is able to change and modify its authentication protocols autonomously on the fly. The adaptation must consider the environment in which the system is operating. The surrounding physical and operational environmental changes can help in determining when an event indicates a security incident or not. In addition, the authentication solution must also consider the fact that the devices in the network are maybe resource constrained to perform heavy authentication task.

In an effort to overcome some of the above-mentioned challenges, many researches have been conducted over the past few years on authentication solution. Researches in[4-9] focused on IoT in Smart Home authentication and in [10-20] focused on WSN and WBAN. While most of the researches focused on how to efficiently utilize the limited resource on the constrained network[4, 15, 16, 21-23] , some tried to consider authentication in dynamic environment [19, 21]. Few researches begun to consider adaptation of the authentication protocol based on the context of the system [12, 24]. None, to the best of our knowledge, has tried to implement adaptation of the authentication based on the risk involved in the process.

In response to the preceding challenges, i propose a risk based adaptive authentication method, which involves continuously monitoring the radio signal characteristics of WBAN links. Since WBAN uses human body tissue as the medium of signal propagation which is subject specific[25] and unique in Smart Home environment[26], not least because of the complex antenna and body electromagnetic interaction effects which can occur. This is further compounded by the impact of body activity and the propagation characteristics of the Smart Home environment which all have an effect upon communications channels.

Thus these subject specific radio signal characteristics of the communication link is used to analyze a risk and then authentication re-authentication protocol is selected based on the security risk involved.

The method further compares the selected authentication protocols' resource need with the available resource of the authenticating device, which will help us to decide to offload or not to the authentication process.

1.1 Problem statement

The applicability of WBANs in Smart Home for providing remote health care is becoming more practical and usable. The main constraints of WBAN are that of energy, memory, computational overheads, the existence of heterogeneous device, and the unattended nature of wireless network. Security issues arise because of these constraints as to how to provide complete security. Since the sensors in the WBAN network collect personal medical data, security and privacy are important components. One of the means that helps us to maintain system security is Authentication. There are a lot of researches done so far in this regard mainly focusing on the optimization of resource usage of the authentication protocols and methods. However, little is done to address the dynamic network environment the WBAN is operating and the risk related to it.

In this Thesis, we present a risk based adaptive authentication framework. Our framework exploits radio signals characteristics of the sensor device to uniquely identify the sensors involved in the network.

1.2 Thesis Contribution

The main contribution of this work is the development of a risk-based adaptive authentication framework that integrates radio signal characteristics of the sensors involved in the network and physiological characteristics of the user using the sensor device. The framework ensures that the device and the individual using it are authentic by analyzing the radio signal behavior exhibited, which is unique according to the place where the sensor is mounted on the body, the body weight, the body height and skin texture of the individual. The proposed authentication scheme is a dynamic risk based

authentication system in which security risk is evaluated for active sessions of the service. Another contribution of the thesis is the development of a Bayesian network model for analyzing the radio signal characteristics of sensor devices. These contributions have been published in [27]

1.3 Thesis outline

The rest of the thesis is organized as follows:

Chapter 2 summarizes and discusses state of the art technologies on IOT, Smart Home, and WBAN.

Chapter 3 presents background knowledge on authentication, risk based adaptive authentication, and constrained network protocols.

Chapter 4 discusses machine Learning and using Bayesian network for authentication solution.

Chapter 5 describes the proposed risk based adaptive authentication system by focusing on the three main modules.

Chapter 6 summarizes our work and discusses future work.

CHAPTER TWO

2. State of the Art

In this chapter, we discuss background concepts on IoT, Smart Home, WBAN, adaptive risk based authentication, and constrained device protocols and present a brief state of the art in naïve Bayesian network. We also review related works on authentication solutions for constrained networks.

2.1 Internet of Things (IoT)

The phrase ‘’ínternet of things’’ was coined and used for the first time by Kevin Ashton [28]. In an effort to improve barcode identification of products, kevin ashton, proposes, every electronic equipment and physical objects to have a unique electronic product code (EPC) stored in an electromangnetic identification tag (RFID) embedded in them. This will enable the product communicate with the outside world [28]. Ever since its introduction the ‘’Internet of things’’ is becoming an increasingly growing topic of discussion.

2.1.1 Definitions

There is no single common diffinition for the IoT. There are several approaches and views among academicians, researchers, practitioners, innovators, developers and corporate people in defining what it is. Let us take a look at some of the definitions.

“The Internet of Things (IoT) is the network of physical objects that contain embedded technology to communicate and sense or interact with their internal states or the external environment. [Gartner]”[1]

“The Internet of Things (IoT) is the intelligent connectivity of smart devices, expected to drive massive gains in efficiency, business growth and quality of life. In other words,

[1] *http://www.gartner.com/it-glossary/internet-of-things/*

https://www.cisco.com/web/offer/emear/38586/images/Presentations/P11.pdf

when objects can sense each other and communicate, it changes how and where and who makes decisions about our physical world." [Ciso][2]

""Internet of Things, or IoT, refers to the growing range of Internet-connected devices that capture or generate an enormous amount of information every day. For consumers, these devices include mobile phones, sports wearables, home heating and air conditioning systems, and more. In an industrial setting, these devices and sensors can be found in manufacturing equipment, the supply chain, and in-vehicle components." [IBM][3]

"A dynamic global network infrastructure with self-configuring capabilities based on standard and interoperable communication protocols where physical and virtual "things" have identities, physical attributes, and virtual personalities and use intelligent interfaces, and are seamlessly integrated into the information network."[IERC] definition."[4]

We can summarize the definitions of internet things in the following equation below.

[Physical Objects]
+
[Controllers, Sensors and Actuators]
+
[Internet]
=
[Internet of Things]

Figure 1 Internet of Things Equation

2

3 *https://www.ibm.com/internet-of-things/learn/library/what-is-iot/*

4 *http://www.internet-of-things-research.eu/about_iot.htm*

2.1.2 Internet of Things Application Areas

Since its emergence, the IoT has been providing a valuable assistance to various dimensions of human life. Integrating IoT into vehicles, traffic systems, roads and bridges making transport easier and safer. IoT in farming and food security can help us to monitor and control production from farm to fork. In manufacturing industry IoT can help to automate difficult and routine tasks. The integration of IoT to wearable will bring functionality into clothes and other wearable objects. IoT can help in the health industry by providing low cost, quality and accessible health service. In smart house and buildings IoT spanning services from automate routine daily tasks to providing safety and security of the dweller.

You can read more [29] for wider view. Our focus of the IoT application area in this thesis however will be on health in Smart Home.

2.2 Smart Home Overview

Technological advancement in area of IoT and ubiquitous computing brought us an opportunity to live in an environment which is intelligent enough to monitor and react to events and activities around us. Such as controlling the heat level of our home, monitoring items in our refrigerator, protecting the security of our assets and more importantly controlling and monitoring our health and wellness. An environment with such capability is referred to as a “Smart Home” [30].

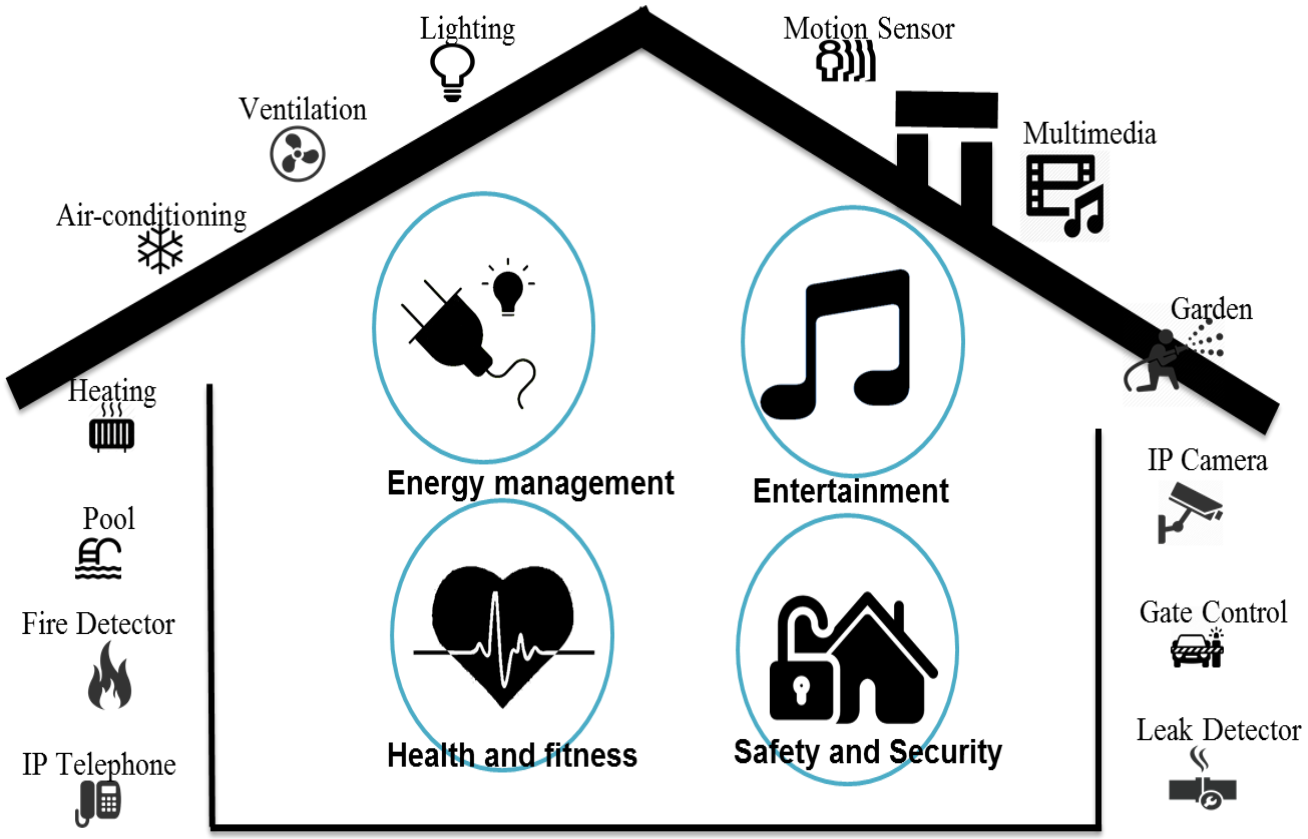

Figure 2. Internet of Things Application Areas in Smart Home

A ”Smart Home” can be defined as a residence equipped with computing and information technology which anticipates and responds to the needs of the occupants, working to promote their comfort, convenience, security and entertainment through the management of technology within the home and connections to the world beyond” [31]. Smart home provides varies types of services. De Silva et al. [30] categorize those services in four main classes as Entertainment, Energy management, safety and Security, and Health.

2.2.1 Health and Fitness in smart home

The provision of high quality, low cost and easily accessible care to the ever increasing population of the world particulalry the elderly suffering from age related diseases is the main challenge in the worldwide health care system [1]. In addition, people nowadays

become health conscious and the demand for quality health service is increasing more than ever as noted in [32].

2.2.2 Devices in Smart Home

A successful implementation of authentication protocols heavily depends on the available resource of the device implementing the protocol. Thus, we have to consider the resources constrained devices in the network when selecting our authentication protocol. Smart home includes a diverse set of devices from different manufacturers, with different communication and resource capabilities [33]. For the purpose of this thesis however, we can take the two categories of devices as (defined as per RFC 7228) constrained devices and less constrained devices. Constrained devices are further classified in to three classes based on their processing capability, memory size, communication channel, and battery life. Table 1 depicts the classification of devices.

Table 1 classification of devices based on their resources [RFC 7228] *[34]*

Name	data size	code size
Class 0, C0	<< 10 KiB	<< 10 KiB
Class 1, C1	~ 10 KiB	~ 100 KiB
Class 2, C2	~ 50 KiB	~ 250 KiB
None constrained	>50 KiB	>250 KiB

2.3. WBAN

A Body Area Network is formally defined by IEEE 802.15 as, "a communication standard optimized for low power devices and operation on, in or around the human body (but not limited to humans) to serve a variety of applications including medical, consumer electronics / personal entertainment and other"[35]. A wireless body area network is a network of wearable sensor and actuator nodes that have the capability to sample, processes and communicate one or more vital signs (heart rate, blood pressure, oxygen saturation, activity) or environmental parameters such as location temperature and humidity, light etc.

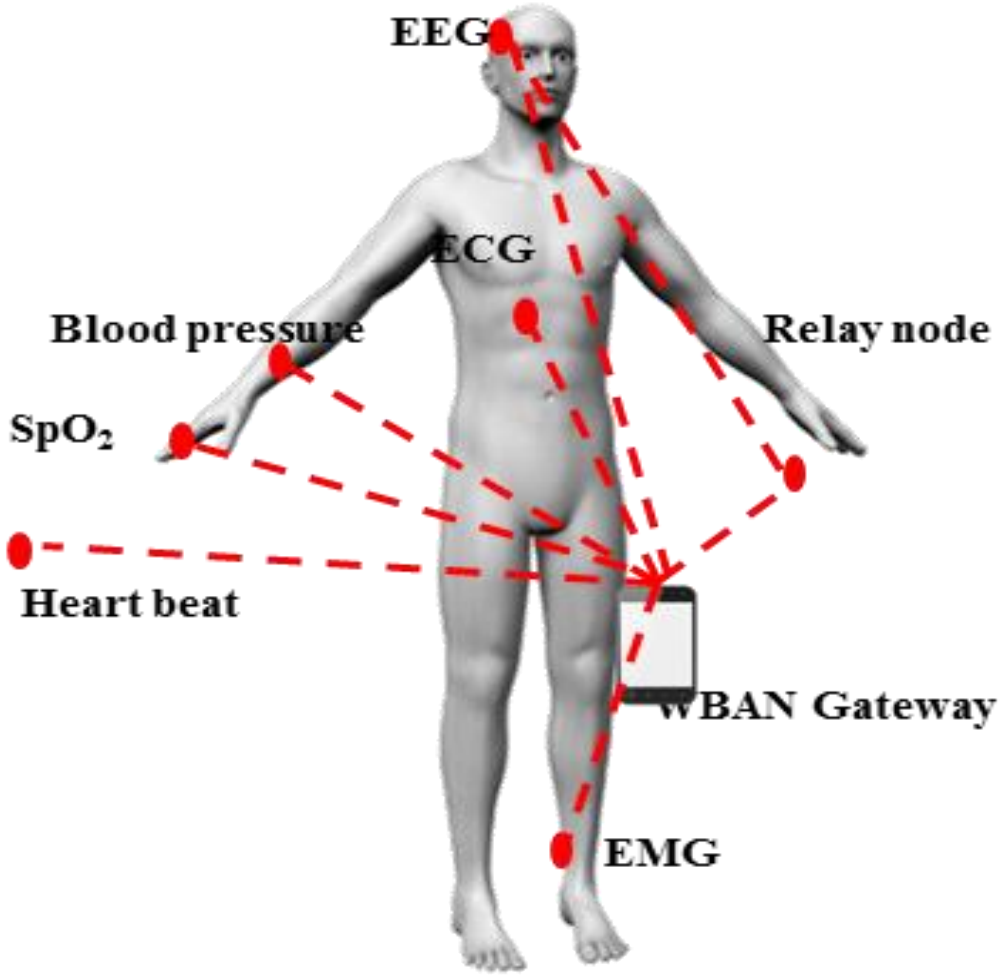

Figure 3 WBAN System

The WBAN mainly consists of wireless sensor and actuator nodes that are placed in, on, or around a body. A node is an independent device with communication capability. Nodes can be classified based on their functionality as personal device, sensors and actuators. Based on the way they are implemented within the body, they can also be classified as implant node, body surface node, and external node. Based on their role in the network nodes can be classified as coordinator, end node and relay node.

WBAN can be applicable in numerous fields in order to improve the user's quality of life. The application area of WBAN can generally be categorized weather they are used in medical field or in non-medical field. Non-medical application includes for motion and gesture detection, military application, fitness monitoring, driving assistance, cognitive and emotional recognition, interactive gaming, social interactions and medical assistance in disaster events, like terrorist attacks, earthquakes and bushfires. Medical application includes remote medical diagnosis, early detection, prevention and monitoring of diseases, elderly assistance at home, and rehabilitation after surgeries.

Healthcare will be the really dominating application area for WBANs. WBAN for health care applications show great promise in improving the quality of life of people and satisfying many requirements of elderly people by enabling them to live safely, securely, healthily and independently.

2.3.1 Communication Architecture

The general Communication architecture of the WBAN network has three tiers Intra-WBAN, inter-WBAN and beyond-WBAN[36].

The Intra-WBAN

Intra-WBAN refers to a communication among sensors/actuators in the body and a communication between these sensors/actuators and a single centralized entity called personal server (PS), also called body gateway. The sensors can be on, near or within the body, and they are of two types. The first types responds to physical stimuli to

monitor, collect, process and report this information wirelessly to the body gateway. The second types called actuators perform medicine administration based on the information received from other sensors in the same network, or through interaction with the user. The body gateway is the one that gathers all the information acquired by sensors and actuators. Once this information is collected by the body gateway, it has to be communicated through one or more access points (AP) to other networks that are easily reachable.

The Inter-WBAN

This communication tier is between the PS and one or more access points (APs). The APs can be considered as part of the infrastructure, or even be placed strategically in a dynamic environment to handle emergency situations. “Tier-2 communication aims to interconnect WBANs with various networks, which can easily be accessed in daily life as well as cellular networks and the Internet”[37]. The more technologies supported by a WBAN, the easier for them to be integrated within applications

Beyond WBAN

The design of this communication Beyond WBAN architecture is for use in metropolitan areas. A gateway such as a PDA can be used to bridge the connection between Tier-2 and this tier; in essence from the Internet to the Medical Server (MS) in a specific application.

2.3.2 Communication Technologies

There are many wireless communication technologies in WBAN such as IEEE 802.11, IEEE 802.15.1 (Bluetooth), and IEEE 802.15.4 (ZigBee). IEEE 802.15.6 (ultra-wideband, UWB) is an optimized communication standard specifically designed for low-power in-body/on-body nodes to serve a variety of medical and non-medical applications. Other technologies such as Wi-Fi, Bluetooth and mobile networks can also

be solutions for implementing WBAN applications, since each technology offers specific characteristics, allowing it to meet the constraints of some applications.

Table 2 Comparisons of the key enabling standards for wearable wireless networks[38]

Parameters	IEEE 802.11 a/b/g/n (Wi-Fi)	IEEE802.15.1 (Blue-tooth)	IEEE802.15.1 (BECAME)	IEEE 802.15.4 (Zigbee)	3GPPLTE / 4G	IEEE802.15.4j (HOLD)	IEEE802.15.6 (WBAN)
Modes of Operation	Adhoc, Infra structure	Adhoc	Adhoc	Adhoc	Infra-structure	Adhoc	Adhoc
Physical(PHY) Layers	NB	NB	NB	NB	NB	NB	NB UWB,HBC
Radio Frequencies (MHz)2400	2400, 5000	2400	2400	868/915/2400	700, 750,800, 850,900,1900,1700/2100	2360-2390/2390-2400	402-405,420-450,863-870,902-928,950-956,2360-2400,2400-2483.5
Power Consumption	High (~800mW)	Medium(~100mW)	Low (~10mW)	Low(~60mW)	NA	Low(~50mW)	Ultra low Power (~1mW at1mdistance)
Maximal Signal Rate	Up to 150 Mb/s	Up to 3Mb/s	Up to 1Mb/s	Up to 250 Kb/s	Up to 300Mb/s	Up to 250 Kb/s	
Communication Range	Up to 250 m (802.11n)	100 m(class 1device)	>100 m	Up to 75 m	Up to 100Km	Up to 75 m	Up to 10 m
Networking Topology	Infrastructure-based	Adhoc very small networks	Adhoc very small networks	Infrastructure-based	Adhoc, Peer-to-Peer, Star, Mesh	Adhoc, Peer-to-Peer, Star	Intra-WBAN: 1or 2-hopstar. Inter-WBAN: non-standardized
Target Size	2007 devices for structured Wi-Fi BSS	Up to 8devices per Piconet	Up to 8devices per Piconet	Up to 65536 devices per network	NA	Up to65536devices per network	Up to 256devices per body, and up to 10 WBANs in 6m3
Target Applications	Data Networks	Voice Links	Healthcare, Fitness, beacon, security, etc.	Sensor Networks, home automation, etc.	Data Networks and Voice Links	Short range Medical Body Area Networks	Body Centric applications
Target BAN Architectures	Off-body	On-body	On-body	Body-to-Body, Off-Body	Body-to-Body, Off-Body	On-Body	On-Body

2.3.4 Privacy and Security in WBAN

Among the challenges mentioned in the previous chapters for successful implementation of WBAN Privacy and security is one of the major Concerns, specially in Medical application of WBAN, since the system deals with life critical data they must be secure. Nevertheless, addressing privacy and security in these systems faces some difficulties.

The term data security means the data is protected from unauthorized user when collected, processed transferred and stored. Whereas data privacy means the data can only be accessed by the people who have authorization to view and use it. In the following subsections, we discuss the major and fundamental security and privacy requirements, security attacks and existing security mechanisms in WBANs.

WBAN Security requirement

We can categorize the security and privacy requirements into three categories according to[39] and[40]: (a)Data storage security requirements, (b)Data access security requirement and (c)Network communication security requirement.

Data storage security requirements

- **Data Confidentiality**: Data confidentiality is required to protect confidential data from disclosure. A patient's identity is authenticated by providing evidence that it holds the specified identity. These include digital certificates and signatures, tokens and passwords between WSN devices in addition to being registered in WBAN. This function is one of the most important roles of security before transferring any data.

- **Dependability**: The system must be reliable and dependable. A failure in retrieving the correct data represents a critical concern in WBANs as it may become a life-threatening matter for the patient

- **Data Integrity**: The patient's information could be altered by an adversary when transmitted over an insecure WBAN and a modified patient data could lead a patient to life critical condition. Therefore proper data integrity mechanism must be implemented

Data access security requirement

- **Data Access control**: In WBAN systems, patient's medical data could be accessed by different users such as, doctors, nurses, pharmacies, insurance companies, lab staff, social workers, and other supportive staff and agencies therefore, it should be prevented from an authorized access by implementing proper access control mechanism.

- **Accountability**: When a user abuses his/her privilege to carry out unauthorized actions on patient data, he/she should be identified and held accountable

- **Revocability:** The privileges of WBAN users or nodes should be deprived in time if they are identified as compromised or behave maliciously

- **Non-repudiation:** The origin of a piece of patient-related data cannot be denied by the source that generated it.

Network communication security requirement

- **Data Authentication:** Data authenticity means making sure that the information is sent by the trusted sender. The recipient of the data must verify and trust the identity of the original source sender. This property is crucial for WBANs because specific actions are launched only if the legitimate nodes requested the action.

- **Data Freshness:** The adversary may sometimes capture data in transit and replay them later using the old key in order to confuse the coordinator. Data freshness implies that the data is fresh and that no one can replay old messages.

There are two types of data freshness: weak freshness, which guarantees partial data frames ordering but does not guarantee delay, and strong freshness, which guarantees data frames ordering as well as delay.

- **Localization:** Most WBAN applications require accurate estimation of the patient's location. Lack of smart tracking mechanisms allow an attacker to send incorrect reports about the patient's location either by reporting false signal strengths or by using replaying signals.

- **Availability:** Availability implies efficient availability of patient's information to the physician. The adversary may target the availability of WBAN by capturing or disabling a particular node, which may sometimes result in loss of life. One of the best ways is to switch the operation of a node that has been attacked to another node in the network.

Possible Security Threats and Attacks

A WBAN is vulnerable to a considerable number of attacks. Such as Denial of Service (DoS) attacks, privacy violation, and physical attacks. Due to the resource constrained nature of the sensor nodes in WBAN network, protection against these types of attacks is a challenging task. A powerful sensor can easily jam a sensor node and can prevent it from collecting user's data on regular basis.

Attacks on WBAN can be classified into three main categories: (a) attacks on secrecy and authentication, where an adversary performs eavesdropping, packet replay attacks, or spoofing of packets, (b) attacks on service integrity, where the network is forced to accept false information, and (c) attacks on network availability (DoS attacks), where the attacker tries to reduce the network's capacity. In the following section, we briefly present most important DoS attacks at physical, data link, network, and transport layers

Table 3 Types of Security Attacks

Layers	DoS Attacks	Defenses
Physical	Jamming	Spread-spectrum, priority messages, lower duty cycle, region mapping, mode change
	Tampering	Tamper-proof, hiding
Link	Collision	Error correcting code
	Unfairness	Small frames
	Exhaustion	Rate limitation
Network	Neglect and greed	Redundancy, probing
	Homing	Encryption
	Misdirection	Egress filtering, authorization monitoring
	Black holes	Authorization, monitoring, redundancy
Transport	Flooding	Client Puzzles

Physical Layer Attacks

Some of the main responsibilities of physical layer include frequency selection and generation, signal detection, modulation, and encryption. Since the medium is radio-based, jamming the network is always possible. The most common attacks are jamming and tampering.

- **Jamming:** refers to interference with the radio frequencies of the nodes. The jamming source can be powerful enough to disrupt the entire network. In this kind of attack, an attacker transmits radio signal randomly with a frequency as the sensor nodes are sending signals for communication. The radio signal interferes with the other signal sent by a sensor node and receives within the range of the attacker cannot receive any message. Thus, the nodes in the range of any attacker signal s become totally isolated as long as the jamming signal continues and no messages can be given or received among the affected nodes

- **Tampering:** refers to the physical attacks on the sensor nodes. However, nodes in WBAN are deployed in close proximity to the human body, and this reduces the chances of physical tampering. Because of unattended and distributed nature; the nodes in a WBAN are highly susceptible to physical attacks. The physical attacks may cause reversible damage to nodes. The adversary can exploit cryptographic keys from the captured node, change the information, modify the program codes or even replace it with a malicious. It has been proven that sensor nodes such as MICA2 motes can be compromised in less than one minute time

Data Link Layer Attacks

This layer is responsible for multiplexing, frame detection, channel access, and reliability. Attacks on this layer include creating collision, unfairness in allocation, and resource exhaustion. Collision occurs when two or more nodes attempt to transmit at the same time. An adversary may strategically create extra collisions by sending

repeated messages on the channel. Unfairness degrades the network performance by interrupting the MAC priority schemes. Exhaustion of battery resources may occur when a self-sacrificing node always keeps the channel busy.

- **Collision**: An adversary can cause collisions in some special packets such as ACK control messages. One of the results of such collisions is the costly exponential back off in certain media access control protocols.

- **Unfairness**: degrades the network performance by interrupting the Medium Access Control (MAC) priority schemes. Exhaustion of battery resources may occur when a self- sacrificing node always keeps the channel busy.

- **Resource Exhaustion:** Daniel of Service (DoS) attacks happen because of resource exhaustion. For instance, a native link layer implementation may try to transmit the corrupted packets continuously. Unless these hopeless retransmissions are found or prevented, the energy reserved of retransmitting node and those surrounding it will be quickly depleted.

Network Layer Attacks

The nodes in WBAN are not required to route the packets to other nodes. Routing is possible when multiple WBANs communicate with each other through their coordinators. Possible attacks include spoofing, selective forwarding, Sybil, and hello flood. In spoofing, the attacker targets the routing information and alters it to disrupt the network. In selective forwarding, the attacker forwards selective messages and drops the others. In sybil, the attacker represents more than one identity in the network. The hello flood attacks are used to fool the network, i.e., the sender is within the radio range of the receiver [41].

- **Spoofed Routing Information:** Targeting the routing information in a network can be considered the most direct attack against an outing protocol. An attacker may perform everything in the network such as spoofing, altering, or replay routing information. These disruptions include creation of routing loops,

generating fake error messages, extending or shortening source routes, attracting or repelling network traffic from selected nodes, causing network partitioning, and increasing end-to-end delay.

- **Selective Forwarding:** Selective forwarding is a kind of attack where a compromised or malicious node just drops packets it likes and selectively forwards packets to make the suspicion minimum to the neighbor nodes. The damage becomes powerful when these malicious nodes are located closer to the base station [42]. There are two kinds of countermeasures that have been presented against selective forwarding attack. The first involves detection of compromised nodes and routing the data seeking an alternative path and the second involves sending data using multi-path routing [43].

- **Sinkhole Attack:** In this attack, a malicious node behaves as a black hole to attract all the traffic in the sensor network. In a flooding -based protocol, at first the attacker listens to requests for routes then replies to the target nodes that contains the high quality or shortest path to the base station. Once the malicious device has the ability to insert itself among the communicating nodes (for example, a sink and sensor node), it is able to do anything with the packets exchanging between them. As a matter of fact, this attack can affect even the nodes that are significantly farther from the base station

- **Wormhole Attack:** A wormhole attack is a sort of attack in which the attacker keeps the packets (or bits) at one location in the network and tunnels those to another location. Wormhole attacks are serious and dangerous threats to WSNs, because they do not need to compromise a sensor in the network. Rather, they can be applied even at the initial phase when the sensors start to detect the neighboring information (Figure 3). For example, when node B (which can be the base station or any other sensor in the sys- tem) broadcasts the routing request packet, the attacker receives this packet and sends it again in its neighborhood. All neighboring nodes receiving this replayed packet will consider themselves to be in the range of Node B, and will consider this node as their parent. GPSR[44]

and GEAR [45] are two such geographic -based routing protocols. In one recent article [46], researchers present a secure routing protocol named SERWA that fights against wormhole attacks. This protocol can discover wormhole attacks without using any specific hardware and can provide a real secure route against them. The simulation of this protocol has shown [47] that when there are more than two wormholes in the network, more than 50% of the data packets will be attracted to the fake neighbor connections and will be discarded.

- **Hello Flood Attack**: In a Hello Flood attack, the attacker sends a hello message with a very powerful radio transmission to the network to convince all nodes to choose the attacker for routing their messages[48]. A good countermeasure against Hello Flood attack is authentication. An effective method is to use Authenticated broadcast protocols such as µTESLA. This protocol is based on symmetric key cryptography with minimum packet overheads. Hamid et al**.** describes a countermeasure against Hello Flood attack that involves adopting a probabilistic secret sharing protocol and uses bidirectional verification.

- **Sybil Attack**: In a Sybil attack [49, 50], a single node pretends to have multiple identities in the network. Any peer-to-peer network (especially wireless ad-hoc) is prone to Sybil attack. This kind of attack has an important effect in geographic routing protocols Newsome et al.. In the location-based routing protocols, nodes need to exchange location information with their neighbors to route the geographically addressed packets efficiently. A paper by Douceur et al. suggests that without a logically centralized authority, Sybil attacks are always probable except under severe and unrealistic assumptions of resource parity and coordination between entities. One of the key requirements for countering Sybil attacks is identity verification. Newsome et al. have presented a technique using quantitative analysis where random key pre distribution schemes can defend against Sybil attack. For this purpose, they associate a sensor node’s identity with its assigned key using one-way hash function. Based on their mechanism, the network has ability to check part or all of the keys that an identity claims to have and thus counters against Sybil attack. Moreover, authentication and

encryption techniques can prevent an outsider from starting a Sybil attack on the sensor network. Public key cryptography can prevent such an insider attack, but because of the high cost it cannot be used in the resource constrained sensor networks. One solution is to have every node share a unique symmetric key with a trusted base station. Two nodes can then use a Needham-Schroeder-like protocol to verify each other's identity and set up a

Transport Layer Attacks

The attacks on the transport layer are flooding and de-synchronization. In flooding, the attacker repeatedly places requests for connection until the required resources are exhausted or reach a maximum limit. In de-synchronization, the attacker forges messages between nodes causing them to request the transmission of missing frames.

- **Flooding Attack:** As shown in [51], adversaries at the transport layer can exploit the protocols that maintain state at either end of the connection. As an example, the adversary may broadcast many connection establishment requests to the victim node to use all the power of its resources, causing a flooding attack. Limiting the number of connections that a node can make is one solution against this kind of attack. However, this can prevent legitimate nodes from connecting to the victim node. Another solution is based on the client puzzles idea presented in [52]. According to this idea, if a node wants to connect with other nodes, it at first must solve a Challenge An attacker is unlikely to have the necessary resources, making it impossible to connect fast enough to use a power of a serving node. Although solving puzzles includes processing overhead, it is more suitable than excessive communication.

- **De-synchronization Attack:** In a de-synchronization attack, an attacker copies massages many times to one or both endpoints of an active connection using a fake sequence number or control flag [53]. Thus, attackers desynchronize the endpoints so that sensor nodes transmit the massages again and waste their energy. One solution against this sort of attack is to authenticate all the packets

given and received among sensor nodes along with all the control fields in a transport header. The adversary cannot spoof the packets and header and, thus, this attack can be blocked

CHAPTER THREE

3. Authentication

Among various security measures authentication is one of the primary and most commonly ways of ascertaining and ensuring security in a network of communicating devices [54], especially in the areas where security compromise can lead to serious level of damage such as in health application. A lot of researches have been proposed on authentication methods for IoTs in a smart home in general and wireless sensor and actuator network in particular.

3.1 Authentication factors

The authentication problem is simple to describe but hard to solve. Two parties are communicating, and one or both wish to establish their identity to the other. Authentication is thus the process of verifying the physical identity of a person, i.e., user authentication and the digital identity of a process/computer. Authentication is the gatekeeper for other security tasks such as confidentiality–restricting data access to authorized persons, integrity–ensuring data modification by authorized persons, non-repudiation–conclusively tracing an action to an individual and availability–ensuring availability of data to authorized persons. Thus user authentication is a central component of any security infrastructure and users can get authenticated in many different authentication factors.

An authentication factor is a category of credential that is used to verify a user who he claims to be There are Four categories of authentication factors [55]. These are generally broken down as: something a user knows, something a user has, something a user is, something a user does, and combinations of any of these as illustrated in Table 3.

Table 4 Authentication Types

Authentication	Types
Something you know	Password, PIN, Personal number, Phone number, date of birth, etc.
Something you have	Tokens, Smartcards, Bank Card, Passport, Driving license, etc.
Something you are	Biometrics: Physiological biometrics such as fingerprint, facial recognition, iris-scan, hand geometry, retina scan, etc., and Behavioral biometrics such as voice recognition, keystroke-scan, signature-scan, gaits, etc.
Something you do	User behaviors patterns, bank transactions, travelling, calls, social media logs, etc.
Combinations	Any combinations of the above (aka multifactor authentication, e.g. PIN-enabled bank card)

As the last factor indicates for each of these authentication types a lot of solutions have been developed with varying factors, single factor (e.g. user name and password) to multi-factor (using two or more distinct and different types of authentication mechanisms). The focus of this study is to adapt authentication mechanisms dynamically according to contextual changes in order to increase the flexibility of authentication and level of security.

3.2 Authentication methods

For the purpose of this study the author prefers to categorize authentication methods based on the protocol they are implementing into two groups, authentication solutions that use symmetric cryptography in one group and authentication solutions that use asymmetric cryptography in the other group.

Symmetric cryptography

Symmetric cryptography is a class of cryptography that performs encryption and decryption operation based on a single key that is shared by both end-points. A number of symmetric cryptographic techniques for WBAN and WSN authentication have been developed in the literature. Symmetric cryptography based authentication is simple and faster method of authentication. The problem of symmetric key based authentication schemes, however, is that a shared key is needed, having in turn the overhead of generating and managing the key, which can be particularly difficult for constrained network. Kumar et al. [5] proposed symmetric cryptography based authentication for Sensor network. In [56], Mana et al. use ECG generated binary sequence as a biometric key to establish secure session between sensor nodes. A zero knowledge proof based on symmetric cryptographic protocol for mutual authentication, that lets nodes exchange a challenge response mechanism before disclosing secret key, is proposed by Khernane et al. [57].

Asymmetric cryptography

Asymmetric cryptography or Public Key Cryptography (PKC) is another way of providing authentication. However, in contrast to symmetric cryptography, in the PKC two different keys are involved for encryption and decryption. In addition we need a certification authority to issue and maintain pool of certificates for the clients, which result in certificate management problem. Thus Public-key cryptography involves significant computation, transmission, and memory overheads in the context of constrained devices. As alternative authors in [58, 59] proposed authentication schemes based on

elliptic curve cryptosystem (ECC), which have better performance. However their alternative solution still needs a certification authority to maintain pool of certificates for users' public key.

Authors in [60, 61] proposed identity based cryptography which solves the issue of storage, transmission and verification of public key certificates. It uses a client identifier as a public key and a trusted key generation center to generate the corresponding private key.

Sattam et al. [62] proposed certificateless public key cryptography. The Key generating center will only process a partial private key for users according to the master key and user's identity, and then the users combine it with a secret value selected by them to get their complete private key.

3.3 Constrained device standards and protocols

3.3.1 IEEE 802.15.4 standard

Wireless communication standards such as IEEE 802.11 and IEEE 802.15 provide higher data throughput and range, but they consume more energy resulting in a crucial disadvantage for constrained sensor network. IEEE 802.15.4 [51] is a standard defined by IEEE 802.15.4 Working Group for data communication devices operating in Low Rate Wireless Personal Area Networks (LR-WPANs). It provides low cost, short-range, low power and low data-rate communication for sensor networks. It targets wireless sensor applications which require short range communication to maximize battery life. The standard specifies the lowest two layers of the protocol stack; the physical and medium access control layers. The upper layers and interoperability sub-layers of the protocol stack are separately defined by other architectures such as 6LoWPAN [63], ZigBee [64], ISA100.11a [65], and WirelessHART [65], as well as other proprietary technologies such as ANT, Z-Wave and more.

3.3.2 Constrained network application level protocol

- **CoAP (Constrained Application Protocol):** Application layers usually employ HTTP to provide web service, but HTTP request uses complex headers, has low

data rate and high energy consumption. Therefore, the Internet Engineering Task Force (IETF) has developed a lightweight protocol for constrained device, CoAP. CoAP is a specialized web protocol designed primarily for constrained nodes and constrained networks, which use UDP transport and DTLS[66].

- **MQTT (**machine-to-machine (M2M) Internet of Things): MQTT is a publish/subscribe messaging protocol designed for lightweight M2M communications that was introduced by Andy Stanford Clark of IBM and Arlen Nipper of Arcom in 1999 and was standardized in 2013 by OASIS (Organization for the Advancement of Structured Information Standards). MQTT has a client server architecture model, where every sensor is a client and connects over TCP to a server, known as broker.

3.3.3 Constrained network security protocols

There are many aspects to being able to secure connections between communication devices. The primary step is to properly encrypt the data stream so that it doesn't leak confidential data to someone who has been able to intercept the messages and to avoid a malicious user to impersonate either the sender device or receiver device. Two very popular encryption protocols for constrained device communications are TLS and DTLS.

- **SSS/TLS:** SSL (Secure Sockets Layer) is a cryptographic protocol for providing security for the communicating devices. SSL has three versions namely SSL 1.0, SSL 2.0, and SSL 3.0, which are all considered insecure due to flaws in their design. TLS is the successor of the SSL protocol; it was created to address the weaknesses in the SSL protocol. TLS is a recommended Transport layer security for providing encrypted communication channel for resource constrained device that implements MQTT protocol.

- **DTLS:** Datagram Transport Layer Security (DTLS) is a modification of TLS for the unreliable UDP. This protocol is originally designed to construct transport layer security over data gram protocol for web application[67]; however due to its

futures of packet retransmission, assigning explicit sequence number with in the handshake and replay detection it become a de facto standard for IoT [15].

3.4. Delegation of authentication

3.4.1 OAuth 2.0

OAuth is an open standard for delegated authorization protocol framework[68] allowing the third-party applications a limited access to protected resource, while maintaining strict authentication and access control. OAuth provides an access token to a client, so that it can access a protected resource, based on the permission of the resource owner. OAuth is not an authentication protocol by itself, it provides a framework for authentication decisions mechanisms. Emerson et al. [69] proposed an OAuth based authentication mechanism for IoT networks.

3.4.2 Delegated authentication for resource constrained Devices

In order to ensure a secure transmission of sensitive information in constrained devices CoAP mandates the use of DTLS protocol as the channel security underneath. However, DTLS was initially designed for resource rich devices that are connected through reliable and high bandwidth link. Thus deploying DTLS over constrained resource network will incur considerable overhead[66]. To alleviate these limitations, authors in [15, 16] proposed a delegation architecture that offloads DTLS connection establishment to dedicated server.

Table 5 Security at the transport layer for constrained and non-constrained network

Layer	For non-constrained network	For constrained network
Application layer protocol	**HTTP, IMAP, FTP, LDAP**	**CoAP | MQTT**
Transport layer security	**SSL/TSL**	**DTLS | TLS**
Transport layer protocol	**TCP**	**UDP | TCP**

3.5. Adaptive authentication

Adaptive security is a security model that changes its behavior autonomously by monitoring and regulating the situations or changes under observation to safeguarding systems against threats over a network. There exists a body of work on adaptive security for IoT in eHealth. In [70] a risk-based adaptive security framework for IoTs in eHealth has been presented, which estimates and predicts risk damages and future benefits using game theory and context-awareness techniques. Savola et al. [71] analyzed security objectives of eHealth IoT applications and their adaptive security decision-making needs, and proposed a high-level adaptive security management mechanism based on security metrics to cope with the challenges. Following this, on one hand Savola and Abie [72] argue that adaptive security solutions need security metrics to be able to adapt the relevant security parameters according to contextual and threat changes, which are typical for patient-centric IoT solutions. The authors developed a context-aware Markov game theoretic model for measurably evaluating and validating the run-time adaptivity of IoT security solutions. On the other hand, Torjusen et al. [73] argue that the integration of run-time enablers into an adaptive

security framework could lead to a sustainable security framework for IoT in eHealth. A brief survey and comparison of adaptive security with their special features and benefits categorized according to their types of adaptation can be found in [32].

The main focus of this paper is specifically on adaptive authentication. Adaptive authentication refers to an authentication solution that continuously monitors and analyzes the changing environment and adapts its solution dynamical based on system requirement to thwart a system against unknown threats [55, 74]. In static authentication, a system user provides identity and gives proof of this identity when first accessing a service and will be valid throughout the full session whereas an adaptive authentication takes a different view from this conventional authentication mechanism. Instead of locking the door and hoping for the best, it focuses on observing for threats and attacks and reacting to them dynamically head-on. Sections 3.8 present review of adaptive security techniques and solutions proposed by various researchers.

3.6 Adaptive authentication mechanisms

Authentication methods and mechanisms may consider different forms of adaptation according to the dynamically changing environment, such as the behavior of the user, threats and the resource of the device, and can adapt its authentication goal, parameter or structure.

In [75] Yeh et al. proposed an adaptive authentication method for IoT based network. In their architecture, they analyze physiological and behavioral characteristics of user i.e. weight and ways of walking from intelligent wearable object to support continual user identification and verification.

In [12] Kim et al. proposed an authentication method which selects it authentication policy based on the available energy.

In [76] Kim and Chae proposed an authentication system which changes its authentication strength based on reputation of the sensor nodes. The authors proposed a mechanism to monitor and record the activity of the sensor nodes in the network. From the monitored data, the reputation of the sensor node is calculated. Based on the

reputation of the sensor node and urgency of the transmitting information, the system sets a priority to a node with best reputation. And latter performs post authentication.

In [24] Caparra et al. proposed two step authentication process. In the first step the source node is authenticated by the concentrator node and the estimated channel is broadcasted to selected anchor node. Selected anchor nodes are involved in the authentication process to estimate the channel of the source node to concentrator node and a comparison of the solution is energy aware and considers the energy level of the anchor before letting them involve in the authentication process. Spooren et al. [77] also proposed authentication adaptation that continuously monitors the battery charge level of the device and keep track of how battery charges are distributed throughout the day to check the authenticity of the device.

3.7 Risk based authentication

Risk-based authentication uses contextual and historical information extracted from user's previous activity to calculate the risk score associated with the user's current activity. The risk score is calculated on real time basis according to a set of rules that can be used to make authentication decisions. The overall goal of risk-based authentication is to gather available information from the user environment, compare it with a known user profile, and determine if that user needs to step through an additional identification process. In [78] Hintze et al. consider geographical location as authentication factor to evaluate the risk and to make authentication decision for mobile devices. Their method uses location-based risk in combination with multi-modal biometrics to adjust the level of authentication necessary to a risk situation. Adam and Hurkala [79] proposed a context risk aware authentication. They used user IP address, time of access, device cookie, device profiling and number of failed authentication attempts to study the risk related to the user identity. Traore et al. [80] proposed a Bayesian network model for analyzing and evaluating the keystroke and free mouse movement of user's to calculate the risk in web sessions. Researches in [81, 82] considered the evaluation of fingerprint movement for learning the behavior of the smartphone user. However, to the best of our knowledge, none of the work published so far has taken into account the evaluation of risk in a resource constrained network such

as the WBAN. In this study, we use the resource constrained devices in WBAN and the dynamic network environment of Smart Home in designing risk-based adaptive authentication solution. The channel characteristics variations among the communicating devices are used to uniquely identify devices validity. The validation of the devices is based on the naïve Bayes network.

3.8 Authentication Mechanisms Review and Comparison

This Section presents a brief overview authentication mechanism and the evaluation of some of user/devices authentication methods proposed in the literature. We evaluate each method based on its resources use (energy, memory, computation and communication) efficiently, and/or adapt its method to the available resource and risk as illustrated in Table 2.

In [15], the reduction of memory overhead, computational overhead and network transmission overhead has been claimed. In [15] a delegation architecture that offloads the expensive Data Transport Layer Security (DTLS) handshake when employing public-key cryptography for peer authentication and key agreement purpose, proposed. In [83], biometric-based user authentication mechanism for wireless sensor networks proposed, which uses one-way hash function and symmetric secret session key shared between the user and a sensor node so that the secret session can be used latter. Caparra et al. [24] proposed authentication process with anchor node involvement in the authentication process to estimate the channel of the source node to concentrator node. The solution is energy aware. It considers the energy level of the anchor before letting them involve in the authentication process.

Spooren et al. [77] proposed authentication adaptation that continuously monitors the battery charge level of the device and keep track of how battery charges are distributed throughout the day to check the authenticity of the device. Han et al. [21] proposed node authentication and key exchange protocol for Smart Home Environment that supports the dynamic nature of the Sensor node by introducing a concept known as Neighbor sink link that helps store the neighbor identity detail in order to reduce computation and communication overhead. Nan et al. [17] used the RSSI signal variation between communicating nodes and user physiological pattern to solve

authentication problem which as they claimed, resulted in a prolonged battery life of the WBAN sensors. Hamdi and Abie [84] proposed a novel game-based adaptive security model for IoT in eHealth, which uses energy consumption, channel bandwidth, memory capacity, and nearby node intrusion to determine whether or not to authenticate the sender node. The model uses the trade-off between security effectiveness and energy-efficiency to evaluate adaptive authentication strategies. A comprehensive survey of authentication protocols for IoT under 4 environments, machine-to-machine communications (M2M), Internet of Vehicles (IoV), Internet of Energy (IoE), and Internet of Sensors (IoS) can be found in [85]. Table 2 compares closely relevant authentication solutions

Table 6 Comparison of Authentication Solutions

Ref	Energy		Memory		Computation		Communication	Risk aware
	Battery efficiency	Battery level adaptation	Memory efficiency	Memory size adaptation	Overhead optimization	Overhead adaptation	Overhead optimization	Adaptation
[15, 83]			X		X		X	
[84]		X		X			X	
[24, 77]		X						
[21]					X		X	
[18, 20, 86]	X							
[11, 14]			X		X			
[87]	X		X					
[80, 81]								X

3.9 Authentication parameters

There is a wide array of device specific information that is available to be considered when evaluating the risk in authentication. The following are some of the factors.

Radio finger print: Radio fingerprinting is a technique which uses the hardware properties of the wireless devices and their signal characteristics for the purpose of unique identification. The radio fingerprints are determined by analyzing the radio signal properties of a received signal such as frequency, amplitude and phase error. These properties will manifest specific characteristics of a device, which are caused by hardware impairments of the device [88-90].

Device Profile: Device profile is a set of attributes such as name, description, and MAC address that are associated with a particular device and describe hardware and software configuration of a device.

User Biometric: User biometric is a physiological or behavioral value of a user that may assist authentication process, such as ECG, retina, fingerprint, voice, face etc.

Radio Signal characteristics

Among the wide array of information that is available to be considered when evaluating the validity of devices and users in authentication. For the purpose of this study, channel characteristics variation between the sensor nodes and the gateway of the WBAN are the preferred means to validate devices identity. That is because channel characteristics in WBAN exhibit unique properties according to the movement of the user, the posture of the user, the skin texture of the user, the surrounding environment, the position of the antennas and the location of the node on the body . Yin et al. [53] have demonstrated that the accuracy of the measurement and thus the identification probability can be maintained above 98%, which is sufficient for this purpose since it is not possible to achieve 100% security.

In the Smart Home scenario of WBAN communications, signal propagation can experience fading due to different reasons, such as energy absorption, reflection, diffraction, shadowing by body, multipath due to the environment around the body and body posture.

The channel characteristics variation between communicating devices can be obtained by studying the property of the signal travelling from the transmitter node to the receiver node. We have identified RSSI (Received signal strength indicator), Channel gain, Temporal link signature, and Doppler measurement as means to model the channel characteristics variation exhibited due to the unique environmental setup of the Smart Home and the unique physiological pattern of mobility of the user wearing the sensor nodes.

- **Received signal strength indicator (RSSI):** is an indication of the power level being received by a client device in a wireless environment. RSSI is often expressed in decibels (db), or as percentage values between 1 up to 100, and can be either a negative, or a positive value. In [17, 91-93] RSSI variation is analyzed to assist authentication solution.
- **Channel gain:** When a radio signal is transmitted from a transmitter to a receiver, the different carrier waves experience different gains in the wireless channel due to the multipath characteristics. A vector of these channel gains can serve as a link signature which can be used to verify the authenticity of a transmitter [94].
- **Temporal link signature:** A radio signal from a transmitter to a receiver takes many paths and each path has a different length. A wave propagating as such takes a different amount of time to arrive at the receiver resulting to a unique temporal link signature. Patrawi [95] proposed the use of channel impulse response generated temporal link signature for each device in the wireless channel to uniquely identify the link between a transmitter and a receiver. The author argues that temporal link signature is useful for efficient location estimation in WSN, physical security for managing objects, and prevention of impersonation in wireless networks.
- **Doppler measurements:** Doppler is the frequency shift caused by the velocity of a transmitter. It involves in measuring the carrier frequency deviation of the moving emitter, in order to calculate its velocity. Doppler measurements, detect motion while the device is moving [96].

CHAPTER FOUR

4. Machine learning

Machine learning algorithms use computational methods to learn information directly from data. The algorithms detect natural patterns in data and use the uncovered patterns to generate insight and help to make better decisions and predictions. Machine learning uses two types of techniques: supervised learning, which trains a model on known input and output data so that it can predict future outputs, and unsupervised learning, which finds hidden patterns or intrinsic structures in input data.

4.1 Unsupervised learning

In unsupervised machine learning only input data is present, no classification or categorization is available. The goal of unsupervised learning is to model the underlying structure or distribution in the data in order to learn more about the data. The most common unsupervised machine learning methods are clustering, dependency modeling and association rule mining.

- **Clustering**: is concerned with grouping together objects that are similar to each other and dissimilar to the objects belonging to other clusters. Clustering is a technique for extracting information from unlabeled data.
- **Association rule mining**: analyzes past information in order to conclude that two items are linked by an associative relationship. Association rules in data mining are useful for analyzing and predicting customer behavior. They play an important part in shopping basket data analysis, product clustering catalog design and store layout.
- **Dependency modeling**: identify dependencies among data items. The aim is developing a model that shows how a number of variables are related to one another (precisely, in a specific application field, seemingly separate variables can have an influence on one another and dependency modeling is about finding out what this influence is).

4.2 Supervised learning

The aim of supervised machine learning is to build a model that makes predictions based on evidence in the presence of uncertainty. A supervised learning algorithm takes a known set of input data and known responses to the data (output) and trains a model to generate reasonable predictions for the response. Classification and Regression are the most frequent types of tasks that are applied in data mining

- **Classification:** classification consists in mapping or classifying data into one of several predefined classes, starting from a situation where none of these assignments are known from the start. Given distinct classes, classification poses itself the problem of assigning a new piece of information to one of them, discretely and without considering any kind of ordering [97].
- **Regression:** regression is a technique used for numerical prediction. Regression is a statistical measure that attempts to determine the strength of the relationship between one dependent variable (i.e. the label attribute) and a series of other changing variables known as independent variables (regular attributes). Just like Classification is used for predicting categorical labels, Regression is used for predicting a continuous value. For example, we may wish to predict the salary of university graduates with 5 years of work experience, or the potential sales of a new product given its price. Regression is often used to determine how many specific factors such as the price of a commodity, interest rates, particular industries or sectors influence the price movement of an asset.

4.3 Classification Prediction

In machine learning classification is the problem of identifying to which of a set of categories a new observation belongs, on the basis of a training set of data containing observations whose category membership is known. The goals of classification are to group objects into a number of categories referred to as classes. Objects refer to compact data units specific to a particular problem, which is in general, known as patterns. Classification prediction encompasses two levels: classifier construction and the usage of the classifier constructed. The former is concerned with the building of a classification model by describing a set of predetermined classes from a training set as

a result of learning from that dataset. Each sample in the training set is assumed to belong to a predefined class, as determined by the class attribute label. The model is represented as classification rules, decision trees, or mathematical formula. The later involves the use of a classifier built to predict or classify unknown objects based on the patterns observed in the training set. The entire process begins with collection of evidence acquired from various data sources or warehouses. In the ideal situation, the data should be of low dimensionality, independent and discriminative so that its values are very similar to characteristics in the same class but very different in features from different classes. Raw data hardly satisfies these conditions and therefore a set of procedures called material selection, feature generation, and feature extraction is required to provide a relevant input for classification system.

4.4 Building a Classification Prediction System

The building of a classification process model can be broken down into four major components technique choice, data pre-processing, training, and testing or evaluation. This ends the classification part of the process.

4.4.1 Technique selection

As the “no free lunch” theorem suggests, there is no technique that has been proven to offer the best solution to all classification or prediction problems [98]. The decision regarding the selection of the classification model is critical as well as difficult, especially if there is little prior knowledge about the nature of the problem. Another problem stems from the fact that the classification process is to a large extent unpredictable and quite often nondeterministic, which means that the appropriateness of the choice made cannot be immediately justified. This can be achieved after going through the entire classification process and a feedback on the performance is established. A new iteration begins again when the feedback indicates poor or unsatisfactory performance until an acceptable level of confidence is established in the performance feedback.

4.4.2 Data Pre-processing and Transformation

Even though there is a defined stage–material selection, feature extraction and generation- where the data may have already been pre-processed to enhance its class predictive power, the choice of the classification technique to be used may call for further adjustment. Different forms of normalization are usually required [99]. Data

transformation could be in different forms. For example, by use of mathematical functions, world knowledge such as, days of the week and civic holidays in order to change certain values. It could also mean performing normalization to convert numeric attributes to nominal attributes to enable the underlying classifier to handle or vice versa.

It must be noted here, that normalization may lead to destruction of the original data structure, where outliers are present. It is therefore important to remove outliers before normalization [100]. The classifier modeler may decide to add different levels of noise on the data to test for robustness of the learning algorithms. Various methods may also be employed to deal with data that are imbalanced to ensure a balanced representation of instances from the datasets at this stage.

4.4.3 Learning

Learning is the term used to describe the actual process of training the classification model. One can distinguish three learning strategies: Supervised, Unsupervised and Reinforcement learning. In supervised learning, the learning algorithm is given a labeled training set to build the model on. It is called “supervised” as it could be thought of as the teacher providing the patterns and their true classes on the basis of which the model learn show to return the best solution to the given problem. In situations where the training data does not contain a known class, in other words, no pastoral guide is provided by a teacher to the learning model. This is referred to as unsupervised. Intermediate reinforcement learning is where the clear label of classifications of dataset is not known, and a feedback is given on whether the classifier output is correct or incorrect without specifying the correct answer. The trained models learn from the labeled instances in the training dataset. It is worth mentioning here that the number of labeled data is limited and usually very small and expensive to obtain. Another important fact is that these data have to be used for performance evaluation. This implies that a part of the available data has to be left out for testing purposes, which further narrows down the amount of data to be used for a proper training of the classifier. It is therefore imperative to take the cost implications of the training into account. That is, to know the cost involved in misclassification and at what percentage of tolerance.

4.4.4 Testing

The testing stage is arguably the most critical phase of the classification model development process. This stems from the fact that it offers the model developer the most informative measure of classifier performance which then could justify its use, leading to possible optimization, redesign or elimination of other models showing bad performance. This in effect will form the basis of model selection. Model testing has some caveats, which must be noted. Complex models tend to over fit the training data so that although their performance on the training set is usually much better than simple linear models, they could show very weak performance for new dataset[98] . Data over fitting is a common issue when it comes to training of learning algorithm models. This can only be avoided when complexity control mechanisms are incorporated in the design of such classifiers. The model is expected to have similarity in performance on training, testing, and data from the problem domain provided they are all well-balanced in complexity. Concrete estimation of the performance of classifiers poses a great problem when there is limited amount of training data. Methods have therefore been devised to solve this problem. Random multiple splitting into training and testing sets is the simplest method to harness the performance reliability. In a situation where smaller testing sets is available, multiple splitting may not work well since some areas of the input space may be scarcely covered, leading to substantial bias in performance estimate. In such cases multiple cross-validations have proven to offer better results [101]. During cross-validation, the testing set is rotated over exclusive subsets, exhaustively covering the whole dataset. Another method of cross validation with a rotation of only a single pattern used for testing is known as “leave one-out”[102] and is preferred whenever its application computational requirement effort is not an issue. A further method is boot-strapping[103] which is used to generate a test set by sampling with replacement from a training set during training.

4.5 Prediction Techniques

Predicting is making claims about something that will happen, often based on information from past and from current state. Everyone solves the problem of prediction every day with various degrees of success. For example, weather, harvest, energy consumption, movements of foreign exchange currency pairs or of shares of stocks, earthquakes, and a lot of other stuff needs to be predicted. In technical domain, predictable parameters of a system can be often expressed and evaluated using equations - prediction is then simply evaluation or solution of such equations. However, practically we face problems where such a description would be too complicated or not possible at all. In addition, the solution by this method could be very complicated computationally, and sometimes we would get the solution after the event to be predicted happened.

Naïve Bayes

The Bayesian Classification represents a supervised probabilistic learning method as well as a statistical method for classification. It calculates explicit probabilities for hypothesis and it is robust to noise in input data. The probabilities of an event A may well depend on the previous or simultaneous occurrence of an event B and A is said to be conditioned on B. The basic idea of Bayes rule is that the outcome of an event A can be predicted based on some evidences (x) that can be observed. A Naïve Bayes Classifier is a simple probabilistic statistical classifier based on applying Bayes probability theorem. Bayes theorem can be described as follows:

$$Posterior\ probability(c/x) = \frac{Class\ prior\ probability(c) * likelihood(x/c)}{evidence(x)}$$

The posterior probability, in the context of a classification problem can be interpreted as “What is the probability that a particular object belongs to class C given its observed feature values?”

Bayesian probability provides a way of calculating posterior probability P(y) from P(C), P(X) and P(x/y)

Naïve Bayes is based on the Bayesian theorem. This classification technique analyses the relationship between each attribute and the class for each instance to derive a conditional probability for the relationships between the attribute values and the class. Naive Bayes classifier assumes that the effect of the value of a predictor(X) on a given class(C) is independent of the values of other predictors. The principle behind Naïve Bayes for classification is a fairly simple process. During training, the probability of each class is computed by counting how many times it occurs in the training dataset. This is called the “prior probability” P(C=c). In addition to the prior probability, the algorithm also computes the probability for the instance x given c with the assumption that the attributes are independent. This probability becomes the product of the probabilities of each single attribute. The probabilities can then be estimated from the frequencies of the instances in the training set [104].

Neural Network (NN)

NN is made up of a structure or a network of numerous interconnected units (artificial neurons). Each of these units consists of input/output characteristics that implement a local computation or function. The function could be a computation of weighted sum of inputs which produces an output if it exceeds a given threshold. The output (whatever the result), could serve as an input to other neurons in the network. This process iterates until a final output is produced. The overall functionality of the network is, however, achieved by the network topology, the individual neurons, and the learning or training strategy and training data. NN is considered to mimic the way the human brain works in the sense that it acquires knowledge from its environment through a learning process. Also, the interneuron connection strengths (synaptic weights) are used to store the knowledge acquired[105].

There are numerous types of neural networks with the main categories being “Feed-forward” and “Recurrent” neural networks. The Feedback Neural networks are the first and arguably simplest types of artificial neural networks devised. In this network, the information moves in only one direction, forward from the input neuron, through the hidden neuron (if any) and to the output neuron. The Recurrent, on the other hand, is a neural network, where the connections between the units form a directed cycle. The simplest kind of feed forward network is considered to have single layer perceptron,

which consists of a single layer output node. The other type of feed forward neural network is the Multilayer perceptron network. With this, each neuron in one layer has direct connections with the neurons in the network. Multilayer perceptron with back propagation (MBP) is the most popular learning algorithm.

In general terms, NN has been noted to have some advantage and disadvantages in their adaptation. The advantages are that: first they are capable of handling a wide range of problems, second, they have an ability to produce good results even in complicated domains, and third they are able to handle both categorical and continuous data types, and have been made available in most off-the-shell packages. The disadvantages include that it requires inputs in the range from 0 to 1, which it is difficult to explain the output of NN models and finally that is also possible for NN to converge prematurely during prediction which could lead to inferior results. This usually occurs when the input features happened to be many. A large number of features make it more difficult for the network to find patterns, resulting in a long training phase that never converges to a good solution.

Linear Regression (LR)

LR attempts to model the relationship between a scalar variable (dependent variable) and one or more explanatory (independent variable) variables by fitting a linear equation to observed data.

Decision Tree (DT)

DT is well-known to be one other effective classification technique in several domains. It is a way of representing series of rules that lead to a class or value. DT models are commonly used in data mining to examine data and induce the tree and its rules that will be used to make predictions. The prediction could be to predict categorical values (classification trees) when instances are to be placed in categories or classes. The technique could also be utilized in the prediction of continues variables (regression tress), where absolute values are required. DT is developed through an iterative process of splitting data into discreet groups, where the objective is to maximize the distance between groups at each split. How the split is done depends on the algorithm used to implement it. In principle, it is possible to construct as many DTs as possible from a given dataset of attributes. While some of these trees are more accurate than

others, finding the optimal tree is computationally impossible when the search space is large. Efficient algorithms have, however, been developed to induce a reasonable accuracy within a reasonable amount of time. An example of such algorithms is the Hunt's algorithm that forms the bases of many existing decision tree induction algorithms, which include C4.5. These algorithms usually employ greedy strategy in searching the attributes space and use for partitioning the data. This point is illustrated by how Hunt algorithm works from a high level point of view. A decision tree is grown in a recursive fashion by partitioning the training dataset into successive subsets. Assuming Ts is the set of training records instances that are associated with node s and y = y1,y2……yc that represent the class labels. Hunts algorithm recursively defines the following:

- If all the instances in Ts belong to the same class Y1 then s is the leaf node labeled as Ys.
- If Ts contains instances that belong to more than one class, an attribute test condition is selected to partition the instance into a smaller subset and the instances in Ts are distributed to the children based on the outcome. This is applied to each child node.

DT is known to have an advantage over numerous techniques due to the output it produces. The output of a decision tree is transparent, which makes it easy for users or non-technical persons to understand. However, decision tree techniques are known to have scalability and efficiency problems, such as substantial decrease in performance and poor use of available system resources. Decision Tree has been successfully applied to many areas in data mining to solve classification problems. These applications indicate how useful DT can be in solving classification problems in data mining.

4.6. Machine learning using Rapid miner

RapidMiner is an open source software product developed by Rapid-I, Community Edition of its software, making it free for readers to obtain and use. is easy to install and will run on variety of computing platforms. RapidMiner Studio combines technology and applicability to serve a user-friendly integration of the latest as well as established data

mining techniques. Defining analysis processes with RapidMiner Studio is done by drag and drop of operators, setting parameters and combining operators. RapidMiner Studio contains more than 1500 operations altogether for all tasks of professional data analysis, from data partitioning, to market-based analysis, to attribute generation, it includes all the tools you need to make your data work for you. But also methods of text mining, web mining, the automatic sentiment analysis from Internet discussion forums (sentiment analysis, opinion mining)as well as the time series analysis and prediction are available. RapidMiner studio enables us to use strong visualizations like 3-D graphs, scatter matrices and self-organizing maps. It allows you to turn your data into fully customizable, exportable charts with support for zooming, panning, and rescaling for maximum visual impact. Radoop enhances RapidMiner's data analysis capabilities by providing key extensions for editing and running ETL, data analytics and machine learning processes in a Hadoop environment.

4.6.1 Rapid Miner Basic Operators

RapidMiner provide a vast variety of operators for data import, data export, data transformation, modeling, and performance evaluation.

- **Data transformation**:-For this purpose rapid miner Contains different operators, For Sorting, Aggregation, Filtering, Type conversion, discretization, Set Operators, Attribute set reductions and more.
- **Modeling**:-Rapid Miner supports different kinds of algorithms to model the classifier. It provides different algorithms for the following classical problems, for classification and regression; clustering and segmentation, Association and Item set Mining, Correlation and dependency.
- **Evaluation**:- For evaluation there are validation and performance measurement operator. Three different validation operators are available here split-validation, x-validation, and Bootstrapping validation.

4.6.2 Rapid Miner Extentions (API)

Even when leveraging on the functions provided by RapidMiner, there are still problems that are unsolvable or only solvable with complex processes. To solve these, there exist typically two alternatives: either using the built-in scripting operator for writing a "quick

and dirty” hack or building an ad-hoc extension to RapidMiner by providing new operators and new data objects with all the functionality of RapidMiner. The latter option is more heavy weight, so it really depends on the task at hand and the need for reusability. In this project we will use rapid miner API to extract the prediction of the rapidminer and further process it according to the proposed architecture.

CHAPTER FIVE

5. Architecture of Risk based Adaptive Authentication

Our network scenario focuses on a health application of body area network in smart home environment where there are both resources constrained and non-resource constrained sensor nodes, a home gateway, and a body area gateway.

In this chapter, we propose the overall design of risk based adaptive authentication architecture. We first introduce the overview and then explain the detail.

5.1 Design Overview

The whole process starts at the bootstrapping of devices into the network. Once devices are bootstrapped, the devices channel characteristics will be used as a parameter to build user behavioral patterns. A naive Bayesian network model machine learning algorithm will be used in order to build these patterns, which is unique for a given specific device over a set of daily routine activity of a user. The selected routine activities are sleeping, walking, sitting and eating.

Temporal link location, Doppler measurements, Received Signal Strength Indicator (RSSI) and channel gain are used to model the channel characteristics between a given node in the network and the gateway. Consequently, these channel characteristics will help us to model the behavioral patterns of the user. These collected parameters are then applied to the naïve Bayesian network algorithm to build the behavioral pattern of the user for a given device. The generated user behavioral pattern is then stored and the node joins the network.

After the bootstrapping and the first-time authentication, the system keeps monitoring and classifying the user behavioral patterns based on the knowledge obtained in the bootstrapping stage. This process yields a classification of the user behavioral pattern as one of the four classes. More importantly the process also yields the probabilistic score or similarity ratio which will be taken as a risk score and it is further classified as Normal, Suspicious, Abnormal and Critical. Then based on the classification of the risk

score a decision is made to raise up the authentication level strength, to lower the authentication strength, or to reject authentication.

Finally, if the authentication decision, which is a protocol selection for authentication, is too heavy to be handled by the node, the authentication process will be offloaded to non-constrained node. The proposed risk based adaptive authentication consists of three main components, the monitoring stage, the analyze stage and the adapt stage as in figure 4.

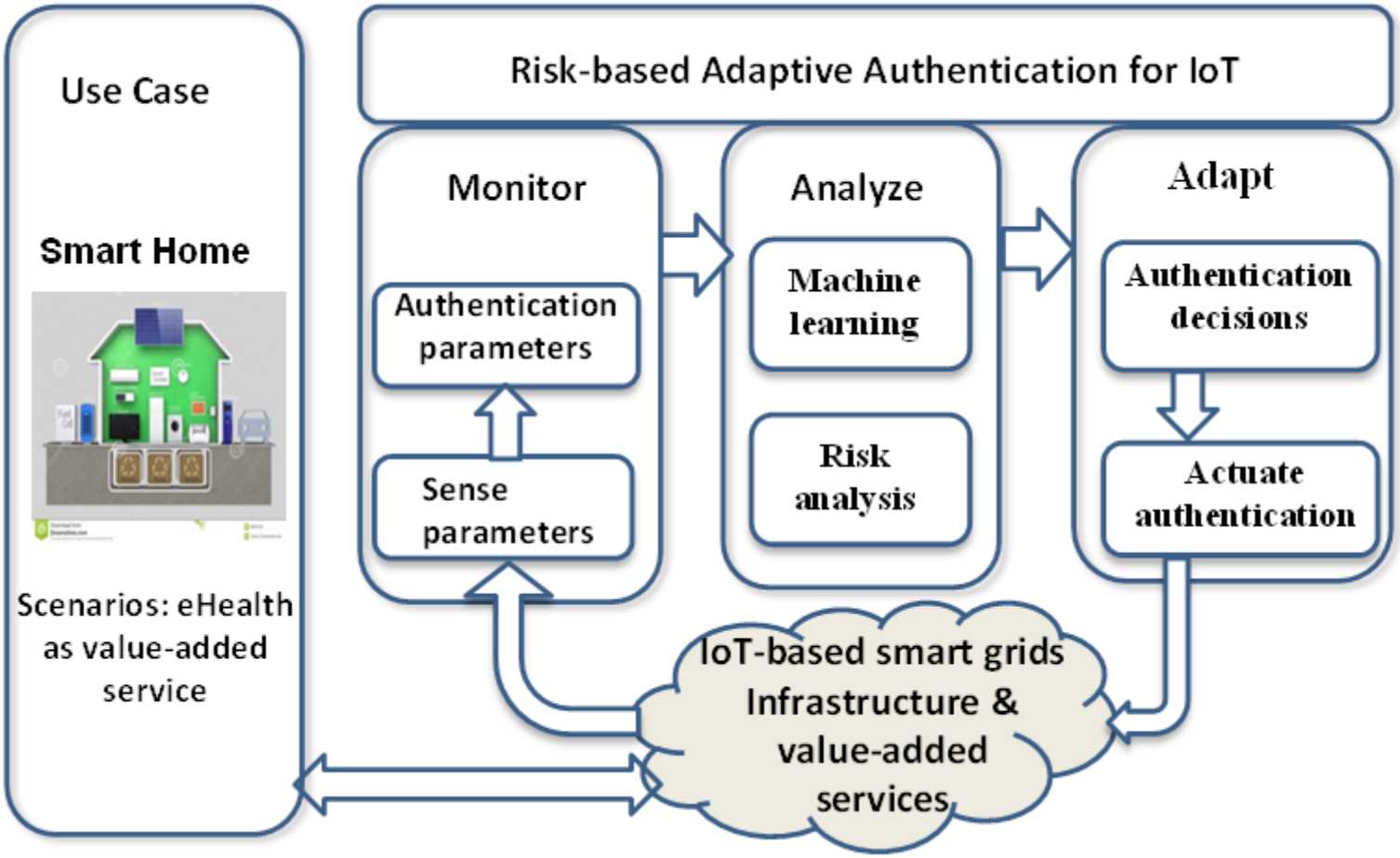

Figure 4 Proposed risk-based adaptive authentication model for IoT

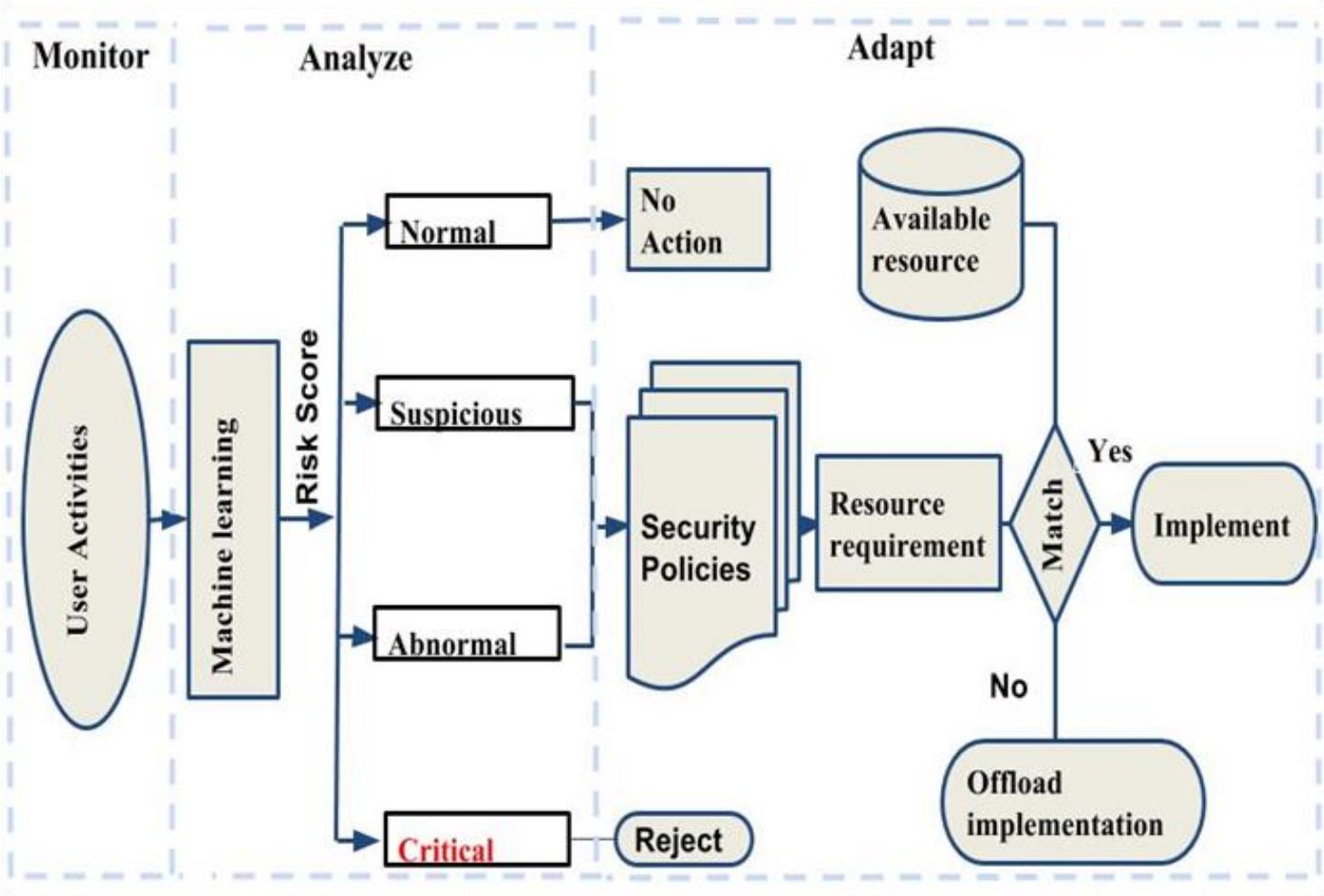

Figure 5 Detailed Architecture Diagram with offloading

5.2 Modules of the Architecture

5.2.1 Bootstrapping of the Network

In this phase, we register patterns on channel characteristics of devices and behavior of users to train the Bayesian network. During training, the probability of an element belonging to a class is computed by counting how many times it occurs in the training dataset. This is called the prior probability. The bootstrap process is described as follows.

1. RSSI, Channel gain, Temporal link signature, and Doppler measurements between each sensor node and the gateway are used to register the position of the node and behavioral patterns of the user. For each attribute, since all the features are continuous we define a range of values and compute the probability of each range.
2. A naïve Bayes classification algorithm is applied on the registered pattern to build a knowledge base for each sensor node. Sleeping, Walking, Sitting, and Eating are the selected daily routines that are used as a target class to classify the features selected in step 1. A signal value out of the range of a known value is classified as Unknown. During training, the probability of an element belonging to a class is computed by counting how many times it occurs in the training dataset.

5.2.2 Monitoring

The monitor phase gathers information from the connected devices. It uses a continuous cycle to monitor activities a user and the device channel characteristics thereof.

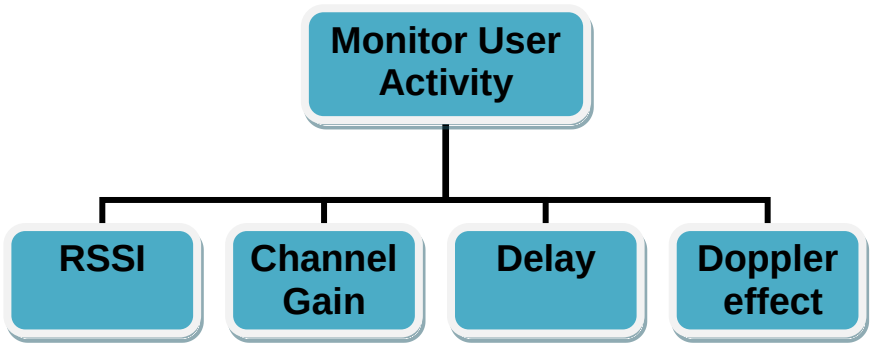

Figure 6 Monitoring Activity Module

. The purpose of the monitoring is to collect those small information pieces, which are then utilized to reveal an adaptation need. The target of the monitoring is on the channel characteristics between the device and the gateway that will be manifested due to the various activities of the user. The monitoring stages involves in collecting low level communication signals to a user physiological pattern. These collected input signals are filtered and relevant set of channel characteristics; the same as listed in the bootstrapping stage are selected. These selected features are used as a parameter to build user behavioral patterns. Later at the analyze stage the pattern generated in this stage will be are compared with historical patterns of the corresponding device to see if any deviation exists.

5.2.3 Analyze

The analyze module computes the monitored features and evaluate a security risk in that particular instance. Privacy and security risks such as risk associated with a log-in attempt, loss of data, hacking, impersonation, eavesdropping, extraction of data, patient endangerment, etc. can be analyzed.

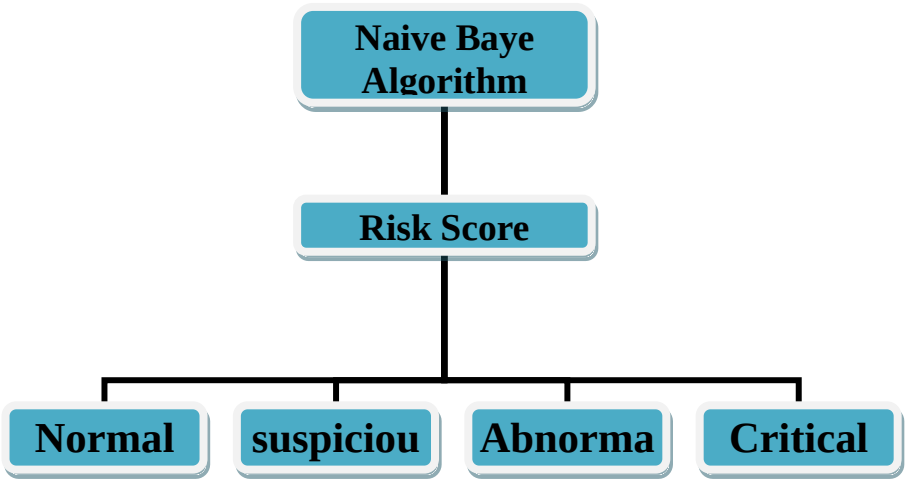

Figure 7 Analysis Module

The naïve Bayes machine learning algorithm is once again used to evaluate the changes in the individual device/user characteristics given the knowledge base build in

the bootstrapping stage. The result of the evaluation is a classification of the user activity and a probability score related to the classification. The probability score is used to indicate if there is a security risk and identify the level of the risk.

Once the risk level is established, decision will be made on to choose which authentication method is suitable. We use a naïve Bayesian network classifier to classify the user pattern related to a particular device. The classes used to classify those collected features are the same classes used in bootstrapping stage 2.

5.2.4 Adapt

The Adapt model plans how to adapt to the authentication level for the observed risk. It is a decision whether to elevate the authentication level and to select the suitable authentication protocol for the selected authentication level. If the risk score of a given user behavioral pattern exceeds normal risk threshold, authentication level is automatically elevated and the user/device maybe required going through a higher level of authentication method. Each of the method is assigned authentication strength. The initial authentication strength for a user is zero. Each time the user/device performs some activity its activity will be classified and a risk level assigned to it. This may rank through Normal, Suspicious, Abnormal and Critical. Authentication decision is performed according to the risk levels as depicted in Table 6.

If the risk level is Normal no action is needed, if the risk level is abnormal a node is requested to authenticate again, if the risk level is suspicious a node is held in Time out and requested to re-authenticate with one of the higher level of authentication types listed in Table 1, Section 2.1 such as PIN or token, and finally if the risk level is critical the user/device is rejected.

5.3 Candidate Authentication policy

If the risk score for a user’s behavioral pattern exceeds normal risk threshold, authentication controls are automatically elevated and the user/device maybe required going through a higher level of authentication method. Each of the method is assigned authentication strength. The initial authentication strength for a user is zero. Each time

the user/device performs some activity its activity will be evaluated and a risk level assigned to it. This may rank through Normal, Suspicious, Abnormal and Critical. Authentication decision is performed according to the risk level. If the risk level is normal no action is needed, if the risk level is abnormal a node is requested to authenticate again and if the risk level is suspicious a node is hold in time out and requested to authenticate with a shared key and finally if the risk level is critical the user/device is rejected.

Table 7 Level of Risk and related Security Policy

Risk Level	**Authentication Decision**			
	Level 1	Level 2	Level 3	Level 4
Normal	No Action			
Suspicious		Re-authentication		
Abnormal			Time out and Re-Authentication	
Critical				Reject

The last step in the adaptation stage is the implementation of the authentication decision. However, before executing the selected authentication protocol the system must compare the resource need of the authentication protocol with the available resource of the device performing the client authentication task. In a situation where the device implementing the authentication protocol is a resource constrained to perform the authentication task, the system will search for a node with available resource to perform the task (offloading) as depicted in Fig. 2.

5.4. CASE STUDY: eHealth In Smart Home

The term “Smart Home” is generally used to refer to a home equipped with electronically controlled devices with security and convenience. These wide arrays of devices are interconnected to form a network, which can communicate with each other and with the user to provide service and create an interactive space. One of the services in Smart Home is eHealth and WBAN is one of the means to provide health services in Smart Home. Health monitoring system in Smart Home is depicted in Fig. 3.

A WBAN system contains a set of physiological and environmental monitoring sensor nodes. These sensors are capable of collecting body vital signs and contextual information at a certain interval and send them to concentrator node for further processing. In this Thesis it is assumed that all sensors in WBAN can send data through wireless channel.

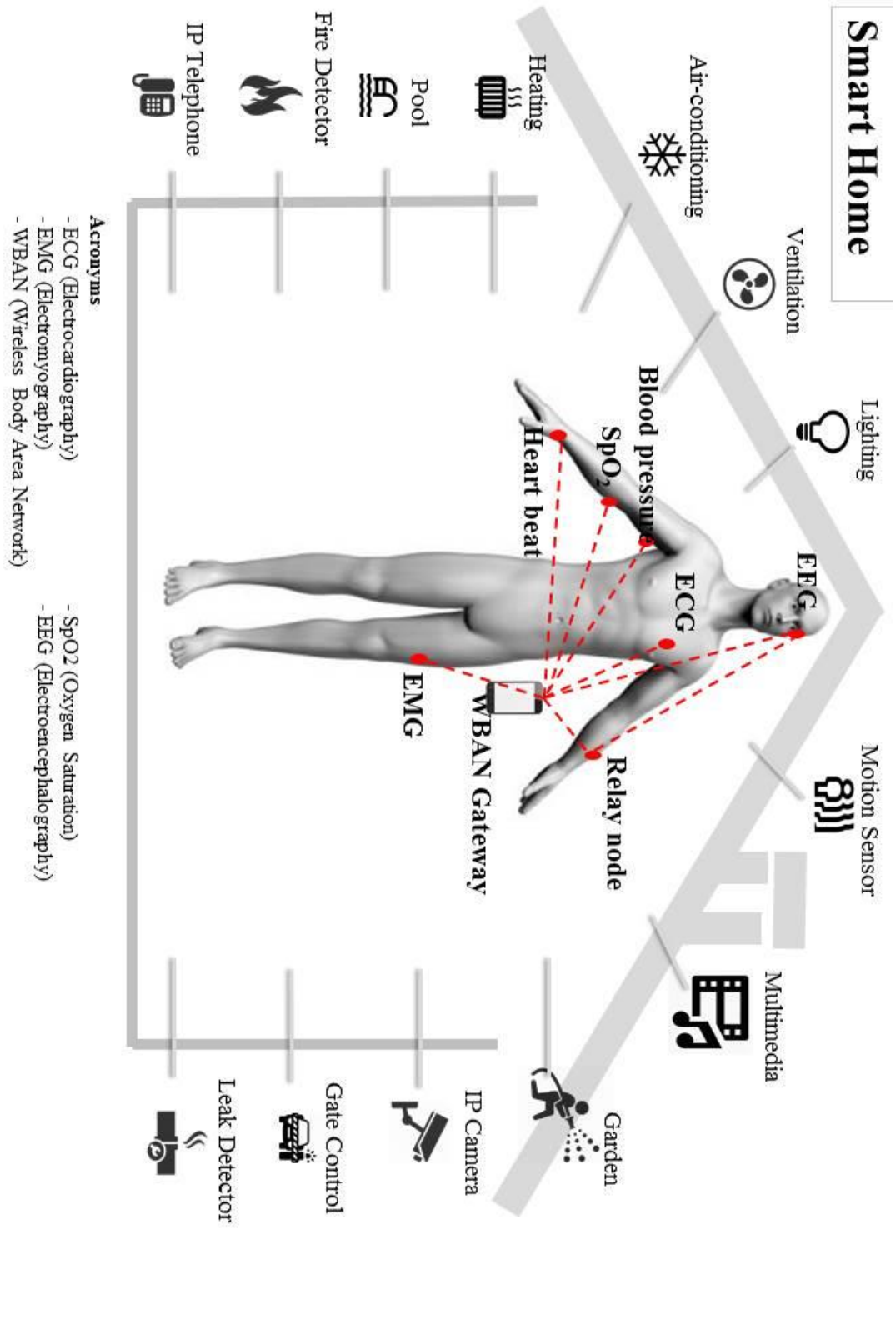

Figure 8 WBAN in Smart Home Scenari

At the physical and network layer, devices in WBAN will typically organize in a star topology where each node directly communicates with a network hub. This is the traditional approach in most WBANs, with the network hub being a dedicated network controller or, more recently, a smartphone. The hub will also act as the gateway for accessing external services (i.e., the Internet, other devices inside the smart home or device in proximity of the WBAN).

All Sensor nodes in WBAN system needs to get authenticated in order to establish a communication channel with the gateway. In this Thesis the focus is the authentication of sensor node to the gateway. In this case study, and as mentioned earlier, the risk associated with a log-in attempt, loss of data, hacking, impersonation, eavesdropping, extraction of data, patient endangerment, etc. will be analyzed.

The communication scenario

- A WBAN system contains a set of physiological and environmental monitoring sensor nodes. These sensors are capable of collecting body vital signs and contextual information at a certain interval and send them to concentrator node for further processing. In this thesis, it is assumed that all sensors in WBAN can send data through wireless channel.
- At the physical and network layer, devices in WBAN will typically organize in a star topology where each node directly communicates with a network hub. This is the traditional approach in most WBANs, with the network hub being a dedicated network controller or, more recently, a smartphone. The hub will also act as the gateway for accessing external services (i.e., the Internet, other devices inside the smart home or device in proximity of the WBAN).
- All Sensor nodes in WBAN system needs to get authenticated in order to establish a communication channel with the gateway. In this thesis the focus is the authentication of sensor node to the gateway.

CHAPTER SIX

6. Conclusion and Future Work

In this thesis, we proposed a novel risk-based adaptive authentication model for IoT in Smart Home eHealth to identify the activities of the user and to verify the validity of the sensor nodes. The model uses a naïve Bayes machine learning algorithm to classify the channel characteristics variation between sensor nodes and their gateway. According to the observed variation of channel characteristics, the model assess the risk to determine the probability of the device in question being compromised, Based on the risk score obtained from the assessment the model selects an authentication decision suitable for the particular risk score. Furthermore the selected authentication decision resource need is compared with the available resource of the authenticator device and incase of scarcity in the available resource, the authentication process is offloaded to a device with available resource.

Our future work includes further development of the model for calculating the channel characteristics and to validate the model by predicating risks using the naïve Bayes classification.

References

[1] O. Ojo and O. Adigun, "A Grid Enabled Framework for Ubiquitous Healthcare Service Provisioning," in *Advances in Grid Computing*: InTech, 2011.

[2] J. Y. Khan and M. R. Yuce, "Wireless body area network (WBAN) for medical applications," *New Developments in Biomedical Engineering. INTECH*, 2010.

[3] R. V. Sampangi, S. Dey, S. R. Urs, and S. Sampalli, "A security suite for wireless body area networks," *arXiv preprint arXiv:1202.2171*, 2012.

[4] P. Kumar, A. Gurtov, J. Iinatti, M. Ylianttila, and M. Sain, "Lightweight and Secure Session-Key Establishment Scheme in Smart Home Environments," *IEEE Sensors Journal*, vol. 16, no. 1, pp. 254-264, 2016.

[5] P. P. Gaikwad, J. P. Gabhane, and S. S. Golait, "3-level secure Kerberos authentication for Smart Home Systems using IoT," in *Next Generation Computing Technologies (NGCT), 2015 1st International Conference on*, 2015, pp. 262-268: IEEE.

[6] S. Z. Reyhani and M. Mahdavi, "User authentication using neural network in smart home networks," *International Journal of Smart Home*, vol. 1, no. 2, pp. 147-154, 2007.

[7] K. Han, J. Kim, T. Shon, and D. Ko, "A novel secure key paring protocol for RF4CE ubiquitous smart home systems," *Personal and ubiquitous computing*, vol. 17, no. 5, pp. 945-949, 2013.

[8] Y. Li, "Design of a key establishment protocol for smart home energy management system," in *Computational Intelligence, Communication Systems and Networks (CICSyN), 2013 Fifth International Conference on*, 2013, pp. 88-93: IEEE.

[9] B. Vaidya, D. Makrakis, and H. T. Mouftah, "Device authentication mechanism for smart energy home area networks," in *Consumer Electronics (ICCE), 2011 IEEE International Conference on*, 2011, pp. 787-788: IEEE.

[10] S. N. Ramli, R. Ahmad, M. F. Abdollah, and E. Dutkiewicz, "A biometric-based security for data authentication in wireless body area network (wban)," in *Advanced Communication Technology (ICACT), 2013 15th International Conference on*, 2013, pp. 998-1001: IEEE.

[11] D. He, S. Zeadally, N. Kumar, and J.-H. Lee, "Anonymous authentication for wireless body area networks with provable security," *IEEE Systems Journal*, 2016.

[12] Y.-P. Kim, S. Yoo, and C. Yoo, "DAoT: Dynamic and energy-aware authentication for smart home appliances in Internet of Things," in *Consumer Electronics (ICCE), 2015 IEEE International Conference on*, 2015, pp. 196-197: IEEE.

[13] K. H. Wong, Y. Zheng, J. Cao, and S. Wang, "A dynamic user authentication scheme for wireless sensor networks," in *Sensor Networks, Ubiquitous, and Trustworthy Computing, 2006. IEEE International Conference on*, 2006, vol. 1, p. 8 pp.: IEEE.

[14] Q. Chang, Y.-p. Zhang, and L.-l. Qin, "A node authentication protocol based on ECC in WSN," in *Computer Design and Applications (ICCDA), 2010 International Conference on*, 2010, vol. 2, pp. V2-606-V2-609: IEEE.

[15] R. Hummen, H. Shafagh, S. Raza, T. Voig, and K. Wehrle, "Delegation-based Authentication and Authorization for the IP-based Internet of Things," in *Sensing, Communication, and Networking (SECON), 2014 Eleventh Annual IEEE International Conference on*, 2014, pp. 284-292: Ieee.

[16] S. Gerdes, O. Bergmann, and C. Bormann, "Delegated Authenticated Authorization for Constrained Environments," in *Network Protocols (ICNP), 2014 IEEE 22nd International Conference on*, 2014, pp. 654-659: IEEE.
[17] N. Zhao, A. Ren, M. U. Rehman, Z. Zhang, X. Yang, and F. Hu, "Biometric Behavior Authentication Exploiting Propagation Characteristics of Wireless Channel," *IEEE Access*, vol. 4, pp. 4789-4796, 2016.
[18] N. Zhao *et al.*, "Double threshold authentication using body area radio channel characteristics," *IEEE Communications Letters*, vol. 20, no. 10, pp. 2099-2102, 2016.
[19] R. Fantacci, F. Chiti, and L. Maccari, "Fast distributed bi‐directional authentication for wireless sensor networks," *Security and Communication Networks*, vol. 1, no. 1, pp. 17-24, 2008.
[20] P. Banerjee, T. Chatterjee, and S. DasBit, "LoENA: Low-overhead encryption based node authentication in WSN," in *Advances in Computing, Communications and Informatics (ICACCI), 2015 International Conference on*, 2015, pp. 2126-2132: IEEE.
[21] K. Han, T. Shon, and K. Kim, "Efficient mobile sensor authentication in smart home and WPAN," *IEEE Transactions on Consumer Electronics*, vol. 56, no. 2, 2010.
[22] B. Mbarek, A. Meddeb, W. B. Jaballah, and M. Mosbah, "A secure authentication mechanism for resource constrained devices," in *Computer Systems and Applications (AICCSA), 2015 IEEE/ACS 12th International Conference of*, 2015, pp. 1-7: IEEE.
[23] S. Zhu, S. Setia, and S. Jajodia, "LEAP+: Efficient security mechanisms for large-scale distributed sensor networks," *ACM Transactions on Sensor Networks (TOSN)*, vol. 2, no. 4, pp. 500-528, 2006.
[24] G. Caparra, M. Centenaro, N. Laurenti, S. Tomasin, and L. Vangelista, "Energy-based anchor node selection for IoT physical layer authentication," in *Communications (ICC), 2016 IEEE International Conference on*, 2016, pp. 1-6: IEEE.
[25] Y. Zhao and Y. Hao, "A subject-specificity analysis of radio channels in wireless body area networks," *Engineering Journal*, vol. 15, no. 3, 2011.
[26] R. Ma, H.-H. Chen, Y.-R. Huang, and W. Meng, "Smart grid communication: Its challenges and opportunities," *IEEE Transactions on Smart Grid*, vol. 4, no. 1, pp. 36-46, 2013.
[27] M. T. Gebrie and H. Abie, "Risk-based adaptive authentication for internet of things in smart home eHealth," in *Proceedings of the 11th European Conference on Software Architecture: Companion Proceedings*, 2017, pp. 102-108: ACM.
[28] S. Sarma, D. L. Brock, and K. Ashton, "The networked physical world–proposals for engineering the next generation of computing, commerce & automatic identification," *Auto-ID Center White Paper*, 2000.
[29] !!! INVALID CITATION !!! (15-22).
[30] L. C. De Silva, C. Morikawa, and I. M. Petra, "State of the art of smart homes," *Engineering Applications of Artificial Intelligence*, vol. 25, no. 7, pp. 1313-1321, 2012.
[31] F. K. Aldrich, "Smart homes: past, present and future," in *Inside the smart home*: Springer, 2003, pp. 17-39.
[32] A. M. Khattak, Z. Pervez, S. Lee, and Y.-K. Lee, "Intelligent Healthcare Service Provisioning Using Ontology with Low-Level Sensory Data," *TIIS*, vol. 5, no. 11, pp. 2016-2034, 2011.
[33] S. Bhardwaj, T. Ozcelebi, J. Lukkien, and C. Uysal, "Resource and service management architecture of a low capacity network for smart spaces," *IEEE Transactions on Consumer Electronics*, vol. 58, no. 2, 2012.
[34] C. Bormann, M. Ersue, and A. Keranen, "RFC 7228: Terminology for Constrained-Node Networks," ed: May, 2014.

[35] K. S. Kwak, S. Ullah, and N. Ullah, "An overview of IEEE 802.15. 6 standard," in *Applied Sciences in Biomedical and Communication Technologies (ISABEL), 2010 3rd International Symposium on*, 2010, pp. 1-6: IEEE.
[36] C. Otto, A. Milenkovic, C. Sanders, and E. Jovanov, "System architecture of a wireless body area sensor network for ubiquitous health monitoring," *Journal of mobile multimedia*, vol. 1, no. 4, pp. 307-326, 2006.
[37] S. Movassaghi, M. Abolhasan, J. Lipman, D. Smith, and A. Jamalipour, "Wireless body area networks: A survey," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 3, pp. 1658-1686, 2014.
[38] M. M. Alam and E. B. Hamida, "Wearable Wireless Sensor Networks: Applications, Standards, and Research Trends," *Emerging Communication Technologies Based on Wireless Sensor Networks: Current Research and Future Applications*, p. 59, 2016.
[39] S. Al-Janabi, I. Al-Shourbaji, M. Shojafar, and S. Shamshirband, "Survey of main challenges (security and privacy) in wireless body area networks for healthcare applications," *Egyptian Informatics Journal*, vol. 18, no. 2, pp. 113-122, 2017.
[40] S. S. Javadi and M. Razzaque, "Security and privacy in wireless body area networks for health care applications," in *Wireless networks and security*: Springer, 2013, pp. 165-187.
[41] F. Shahzad, M. Pasha, and A. Ahmad, "A Survey of Active Attacks on Wireless Sensor Networks and their Countermeasures," *arXiv preprint arXiv:1702.07136*, 2017.
[42] H. Deng, X. Sun, B. Wang, and Y. Cao, "Selective forwarding attack detection using watermark in WSNs," in *Computing, Communication, Control, and Management, 2009. CCCM 2009. ISECS International Colloquium on*, 2009, vol. 3, pp. 109-113: IEEE.
[43] J. S. Chen *et al.*, "Constructing hierarchical spheres from large ultrathin anatase TiO2 nanosheets with nearly 100% exposed (001) facets for fast reversible lithium storage," 2010.
[44] I.-S. Jeon, J.-I. Lee, and M.-J. Tahk, "Homing guidance law for cooperative attack of multiple missiles," *Journal of guidance, control, and dynamics*, vol. 33, no. 1, pp. 275-280, 2010.
[45] Y. Yu, R. Govindan, and D. Estrin, "Geographical and energy aware routing: A recursive data dissemination protocol for wireless sensor networks," 2001.
[46] S. Madria and J. Yin, "SeRWA: A secure routing protocol against wormhole attacks in sensor networks," *Ad Hoc Networks*, vol. 7, no. 6, pp. 1051-1063, 2009.
[47] V. Rosello, J. Portilla, Y. Krasteva, and T. Riesgo, "Wireless sensor network modular node modeling and simulation with VisualSense," in *Industrial Electronics, 2009. IECON'09. 35th Annual Conference of IEEE*, 2009, pp. 2685-2689: IEEE.
[48] M. A. Hamid, M. Rashid, and C. S. Hong, "Routing security in sensor network: Hello flood attack and defense," *IEEE ICNEWS*, pp. 2-4, 2006.
[49] J. R. Douceur, "The sybil attack," in *International Workshop on Peer-to-Peer Systems*, 2002, pp. 251-260: Springer.
[50] J. Newsome, E. Shi, D. Song, and A. Perrig, "The sybil attack in sensor networks: analysis & defenses," in *Proceedings of the 3rd international symposium on Information processing in sensor networks*, 2004, pp. 259-268: ACM.
[51] N. Kim, H. Lim, H. Park, and M. Kang, "Detection of multicast video flooding attack using the pattern of bandwidth provisioning efficiency," *IEEE Communications Letters*, vol. 14, no. 12, pp. 1170-1172, 2010.
[52] M. Fallah, "A puzzle-based defense strategy against flooding attacks using game theory," *IEEE transactions on dependable and secure computing*, vol. 7, no. 1, pp. 5-19, 2010.
[53] S. Sadasivam and P. Moulin, "On estimation accuracy of desynchronization attack channel parameters," *IEEE Transactions on Information Forensics and Security*, vol. 4, no. 3, pp. 284-292, 2009.

[54] M. J. Covington, M. Ahamad, I. Essa, and H. Venkateswaran, "Parameterized authentication," in *European Symposium on Research in Computer Security*, 2004, pp. 276-292: Springer.
[55] R. Hulsebosch, M. Bargh, G. Lenzini, P. Ebben, and S. Iacob, "Context sensitive adaptive authentication," *Smart Sensing and Context*, pp. 93-109, 2007.
[56] M. Mana, M. Feham, and B. A. Bensaber, "SEKEBAN (secure and efficient key exchange for wireless body area network)," *International Journal of advanced science and technology,* vol. 12, pp. 45-60, 2009.
[57] N. Khernane, M. Potop-Butucaru, and C. Chaudet, "BANZKP: A secure authentication scheme using zero knowledge proof for WBANs," in *New Technologies for Distributed Systems (NOTERE), 2016 13th International Conference on*, 2016, pp. 1-6: IEEE.
[58] S. A. Chaudhry, M. S. Farash, H. Naqvi, and M. Sher, "A secure and efficient authenticated encryption for electronic payment systems using elliptic curve cryptography," *Electronic Commerce Research,* vol. 16, no. 1, pp. 113-139, 2016.
[59] T. Goriparthi, M. L. Das, and A. Saxena, "An improved bilinear pairing based remote user authentication scheme," *Computer Standards & Interfaces,* vol. 31, no. 1, pp. 181-185, 2009.
[60] X. Cao, X. Zeng, W. Kou, and L. Hu, "Identity-based anonymous remote authentication for value-added services in mobile networks," *IEEE Transactions on Vehicular Technology,* vol. 58, no. 7, pp. 3508-3517, 2009.
[61] K. Y. Choi, J. Y. Hwang, D. H. Lee, and I. S. Seo, "ID-based authenticated key agreement for low-power mobile devices," in *Australasian Conference on Information Security and Privacy*, 2005, pp. 494-505: Springer.
[62] S. S. Al-Riyami and K. G. Paterson, "Certificateless public key cryptography," in *International Conference on the Theory and Application of Cryptology and Information Security*, 2003, pp. 452-473: Springer.
[63] S. Raza, D. Trabalza, and T. Voigt, "6LoWPAN compressed DTLS for CoAP," in *Distributed Computing in Sensor Systems (DCOSS), 2012 IEEE 8th International Conference on*, 2012, pp. 287-289: IEEE.
[64] P. Kinney, "Zigbee technology: Wireless control that simply works," in *Communications design conference*, 2003, vol. 2, pp. 1-7.
[65] S. Petersen and S. Carlsen, "WirelessHART versus ISA100. 11a: The format war hits the factory floor," *IEEE Industrial Electronics Magazine,* vol. 5, no. 4, pp. 23-34, 2011.
[66] Z. Shelby, K. Hartke, and C. Bormann, "The constrained application protocol (CoAP)," 2014.
[67] N. Modadugu and E. Rescorla, "The Design and Implementation of Datagram TLS," in *NDSS*, 2004.
[68] D. Hardt, "The OAuth 2.0 authorization framework," 2012.
[69] S. Emerson, Y.-K. Choi, D.-Y. Hwang, K.-S. Kim, and K.-H. Kim, "An oauth based authentication mechanism for iot networks," in *Information and Communication Technology Convergence (ICTC), 2015 International Conference on*, 2015, pp. 1072-1074: IEEE.
[70] H. Abie, R. M. Savola, J. Bigham, I. Dattani, D. Rotondi, and G. Da Bormida, "Self-healing and secure adaptive messaging middleware for business-critical systems," *International Journal on Advances in Security,* vol. 3, no. 1&2, 2010.
[71] R. M. Savola, H. Abie, and M. Sihvonen, "Towards metrics-driven adaptive security management in e-health IoT applications," in *Proceedings of the 7th International Conference on Body Area Networks*, 2012, pp. 276-281: ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering).
[72] R. M. Savola and H. Abie, "Metrics-driven security objective decomposition for an e-health application with adaptive security management," in *Proceedings of the International Workshop on Adaptive Security*, 2013, p. 6: ACM.

[73] A. B. Torjusen, H. Abie, E. Paintsil, D. Trcek, and Å. Skomedal, "Towards run-time verification of adaptive security for IoT in eHealth," in *Proceedings of the 2014 European Conference on Software Architecture Workshops*, 2014, p. 4: ACM.
[74] H. Abie and I. Balasingham, "Risk-based adaptive security for smart IoT in eHealth," in *Proceedings of the 7th International Conference on Body Area Networks*, 2012, pp. 269-275: ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering).
[75] K.-H. Yeh, C. Su, C.-L. Hsu, W. Chiu, and Y.-F. Hsueh, "Transparent authentication scheme with adaptive biometrie features for IoT networks," in *Consumer Electronics, 2016 IEEE 5th Global Conference on*, 2016, pp. 1-2: IEEE.
[76] M. Kim and K. Chae, "Adaptive Authentication Mechanism using Node Reputation on Mobile Medical Sensor Networks," in *Advanced Communication Technology, 2008. ICACT 2008. 10th International Conference on*, 2008, vol. 1, pp. 499-503: IEEE.
[77] J. Spooren, D. Preuveneers, and W. Joosen, "Leveraging Battery Usage from Mobile Devices for Active Authentication," *Mobile Information Systems*, vol. 2017, pp. 1-14, 2017.
[78] D. Hintze, E. Koch, S. Scholz, and R. Mayrhofer, "Location-based risk assessment for mobile authentication," in *Proceedings of the 2016 ACM International Joint Conference on Pervasive and Ubiquitous Computing: Adjunct*, 2016, pp. 85-88: ACM.
[79] A. Hurkała and J. Hurkała, "Architecture of Context-Risk-Aware Authentication System for Web Environments," 2014.
[80] I. Traore, I. Woungang, M. S. Obaidat, Y. Nakkabi, and I. Lai, "Online risk-based authentication using behavioral biometrics," *Multimedia tools and applications*, vol. 71, no. 2, pp. 575-605, 2014.
[81] L. Li, X. Zhao, and G. Xue, "Unobservable Re-authentication for Smartphones," in *NDSS*, 2013.
[82] H. Gascon, S. Uellenbeck, C. Wolf, and K. Rieck, "Continuous Authentication on Mobile Devices by Analysis of Typing Motion Behavior," in *Sicherheit*, 2014, pp. 1-12.
[83] M. Sarvabhatla and C. S. Vorugunti, "A Secure Biometric-Based User Authentication Scheme for Heterogeneous WSN," in *Emerging Applications of Information Technology (EAIT), 2014 Fourth International Conference of*, 2014, pp. 367-372: IEEE.
[84] M. Hamdi and H. Abie, "Game-based adaptive security in the Internet of Things for eHealth," in *Communications (ICC), 2014 IEEE International Conference on*, 2014, pp. 920-925: IEEE.
[85] M. A. Ferrag, L. A. Maglaras, H. Janicke, and J. Jiang, "Authentication Protocols for Internet of Things: A Comprehensive Survey," *arXiv preprint arXiv:1612.07206*, 2016.
[86] S. Prameela and P. Ponmuthuramalingam, "A robust energy efficient and secure data dissemination protocol for wireless body area networks," in *Advances in Computer Applications (ICACA), IEEE International Conference on*, 2016, pp. 131-134: IEEE.
[87] M. Rizk and M. Mokhtar, "An efficient authentication protocol and key establishment in dynamic WSN," in *Information Communication and Management (ICICM), International Conference on*, 2016, pp. 178-182: IEEE.
[88] V. Brik, S. Banerjee, M. Gruteser, and S. Oh, "Wireless device identification with radiometric signatures," in *Proceedings of the 14th ACM international conference on Mobile computing and networking*, 2008, pp. 116-127: ACM.
[89] W. C. Suski II, M. A. Temple, M. J. Mendenhall, and R. F. Mills, "Using spectral fingerprints to improve wireless network security," in *Global Telecommunications Conference, 2008. IEEE GLOBECOM 2008. IEEE*, 2008, pp. 1-5: IEEE.

[90] K. B. Rasmussen and S. Capkun, "Implications of radio fingerprinting on the security of sensor networks," in *Security and Privacy in Communications Networks and the Workshops, 2007. SecureComm 2007. Third International Conference on*, 2007, pp. 331-340: IEEE.
[91] L. Shi, M. Li, S. Yu, and J. Yuan, "BANA: body area network authentication exploiting channel characteristics," *IEEE Journal on selected Areas in Communications,* vol. 31, no. 9, pp. 1803-1816, 2013.
[92] A. Kalamandeen, A. Scannell, E. de Lara, A. Sheth, and A. LaMarca, "Ensemble: cooperative proximity-based authentication," in *Proceedings of the 8th international conference on Mobile systems, applications, and services*, 2010, pp. 331-344: ACM.
[93] A. Scannell, A. Varshavsky, A. LaMarca, and E. De Lara, "Proximity-based authentication of mobile devices," *International Journal of Security and Networks,* vol. 4, no. 1-2, pp. 4-16, 2009.
[94] Z. Li, W. Xu, R. Miller, and W. Trappe, "Securing wireless systems via lower layer enforcements," in *Proceedings of the 5th ACM workshop on Wireless security*, 2006, pp. 33-42: ACM.
[95] N. Patwari and S. K. Kasera, "Robust location distinction using temporal link signatures," in *Proceedings of the 13th annual ACM international conference on Mobile computing and networking*, 2007, pp. 111-122: ACM.
[96] A. Domazetovic, L. J. Greenstein, N. B. Mandayam, and I. Seskar, "Estimating the Doppler spectrum of a short-range fixed wireless channel," *IEEE Communications Letters,* vol. 7, no. 5, pp. 227-229, 2003.
[97] B. L. W. H. Y. Ma and B. Liu, "Integrating classification and association rule mining," in *Proceedings of the fourth international conference on knowledge discovery and data mining*, 1998.
[98] R. Lippmann, "An introduction to computing with neural nets," *IEEE Assp magazine,* vol. 4, no. 2, pp. 4-22, 1987.
[99] I. H. Witten, E. Frank, M. A. Hall, and C. J. Pal, *Data Mining: Practical machine learning tools and techniques*. Morgan Kaufmann, 2016.
[100] R. Caruana and A. Niculescu-Mizil, "Data mining in metric space: an empirical analysis of supervised learning performance criteria," in *Proceedings of the tenth ACM SIGKDD international conference on Knowledge discovery and data mining*, 2004, pp. 69-78: ACM.
[101] J. Han, J. Pei, and M. Kamber, *Data mining: concepts and techniques*. Elsevier, 2011.
[102] S. M. Weiss and C. A. Kulikowski, *Computer systems that learn: classification and prediction methods from statistics, neural nets, machine learning, and expert systems*. Morgan Kaufmann Publishers Inc., 1991.
[103] R. Kohavi and G. H. John, "The wrapper approach," in *Feature extraction, construction and selection*: Springer, 1998, pp. 33-50.
[104] E. Frank, L. Trigg, G. Holmes, and I. H. Witten, "Naive Bayes for regression," *Machine Learning,* vol. 41, no. 1, pp. 5-25, 2000.
[105] F. Sebastiani, "Machine learning in automated text categorization," *ACM computing surveys (CSUR),* vol. 34, no. 1, pp. 1-47, 2002.