# Comprehensive study of Communication Security in the Internet of Things (IoT) in Healthcare

**GROUP 10**
**Group Members**

Ambarish Ravindran (Group leader)

Nitesh Gupta (Deputy leader)

Ravi Nihalani

Vaishnavi Barla

Ting Chen

Sneha Manjunatha

Hanumantha Narayana Harish Pendela

Maitrayee Pingale

Nikhil Lohia

Sushant Sakolkar

**Summary** This project report is for the course CSE 543: Information Assurance and Security. The project focuses on the security aspects of IoT Healthcare Systems by drawing parallels with the IoT architecture. The idea is to understand various security challenges and proposed solutions at each layer of the IoT architecture.

# 1 Contents

**LIST OF FIGURES**



**LIST OF TABLES**

# 2 INTRODUCTION

## 2.1 MOTIVATION AND BACKGROUND

The advent of IoT is changing the face of healthcare in numerous ways. Though IoT can revolutionize the way doctors and patients interact within a healthcare ecosystem, the security aspects of IoT healthcare architecture seems to raise eyebrows and limits its capabilities. The recent attacks on IoT healthcare systems has raised questions about whether the benefits of this architecture outweigh its applicability.

Not only does breach in security threaten a specific device, but in some cases, it gives hackers access to the entire hospitals' system. Like a car hacking instance, this not only poses immediate cyber-threats, but it could have deadly repercussions, as different diabetes patients need varying levels of insulin at different times. A malicious person could hack into these insecure devices and literally kill someone, so it is time that the healthcare industry started taking medical device IoT security more seriously.

Norse and think tank, the SANS Institute released a study showing how some 375 U.S. healthcare organizations were actively compromised in a period from September 2012 to October 2013. The attackers infiltrated internet-connected radiology imaging software, conferencing systems, printers, firewalls, web cameras and mail servers to access patient files and other information.

Though this may seem far-fetched and unlikely to occur, there have been several real-world scenarios where security breaches in IoT Healthcare has led to catastrophic consequences and potentially death.

### 2.1.1 Specific Instances:

One of the most recent and notable kinds of threat in the healthcare industry is the threat to *Johnson & Johnson's Animas One Touch Ping insulin pump*. This insulin pump is special in that it is equipped with a remote control so that users do not need to remove their clothing to give themselves a dose of insulin. The problem with this is that the wireless connection between the remote and the pump is unencrypted, and consequently, highly vulnerable. Because of this, the pump can be hacked within a 25-foot radius of the user, and with the right radio equipment, a hacker can take control of the pump and trigger unauthorized insulin injections.

Cyber risks are evolving from virtual harm to physical harm. An increased risk of bodily harm from hacked medical devices that send a patient's information to a doctor or hospital are common. An example: VP Dick Cheney had received a pacemaker in 2007, famously known as the "Homeland" episode in 2012. A compromised pacemaker killed the fictional VP.

## 2.2 GOALS AND SCOPE

### 2.2.1 How healthcare devices communicate with each other in a fast and secure manner? And How do patients and doctors receive the correct information at the right time, most importantly, in a secure manner?

**Data availability:** This means we need to ensure that health-related data is available and accessible by the doctors and patients whenever required. The requirement for healthcare information to be **available at all times on demand** is critical to lives of individuals and can often be a deciding factor to make major surgical decisions. Considering that patient data is being continually transmitted and modified over time, the need to ensure that accurate and updated information is made available to the doctors and patients at all times is a major focus of the project.

**Data integrity:** One of the major security requirements in healthcare is the need for **accurate patient information** at all times. This poses a major challenge to the IoT architecture of healthcare. Hackers who can gain access to confidential patient information can modify critical patient data such as their blood pressure readings which can lead to catastrophic consequences. Maintaining integrity of patient information forms a major part of our scope of study.

**Data encryption:** Encrypting patient information is an important aspect of security. The idea is to ensure that no third-party software or individual **recognizes confidential and personal information**. There have been many encryption algorithms in practice which are used for multiple applications. Our project focuses on how various encryption algorithms ensure patient information is stored securely on servers and thus confidential data is inaccessible to unauthorized parties.

### 2.2.2 How does the network architecture of IoT healthcare ensure network security across the entire communication channel?

#### 2.2.2.1 Application Layer

- Application layer vulnerabilities.
- Solutions to address the vulnerabilities.
- Encryption Algorithms at Application Layer.
- Sharing and presenting health-related data to the patient.
- Offloading data from software and hardware devices and storing on servers.
- Authorizing subjects to access patient related information.

#### 2.2.2.2 Network Layer

- Authentication
- Authorization
- Encryption protocols
- eHealth Architecture
- Delegated authorization
- Network security protocol

#### 2.2.2.3 Physical Layer

- Authentication in RFID Tagging
- DoS attack in Wireless Sensor Networks
- Authentication in body sensor networks
- Security issues in wireless sensor networks
- Cancellation-Based Friendly Jamming
- Secure links for end-to-end communication

# 3 OVERVIEW

## 3.1 EVALUATION CRITERIA

### 3.1.1 FORMAT FOLLOWED FOR EVALUATING EACH RESEARCH PAPER

**(i) Research Paper:** This is the name of the published research paper that was read and analyzed for the specified topic.

**(ii) Security Topics:** This is the category of the security area to which the paper belongs.

**(iii) Security Issues:** Considering that each security issue is unique in terms of the application under question, we have identified the specific security area addressed by the research paper.

**(iv) Proposed Solution:** This conveys the essence of the paper. The architecture and the approach used in the paper has been detailed here. This includes an understanding of empirical conclusions reached based on practical observations made by authors of the paper.

**(v) Security Challenges:** Although each paper addresses a security concern, it is possible that there are certain areas that require more research to uncover certain nuances as a part of the security area described. These have been listed in this section for the research paper studied.

### 3.1.2 Findings and Analysis for each layer

Involves each group member's understanding of the research paper studied. The anatomy of each research paper is presented in this section based on the reader's understanding and is categorized by giving importance to the following:

1) Architecture proposed in the research paper.
2) Security solutions described by the authors.

### 3.1.3 Security Verticals/Topics

| |
|---|
| Application security in wearable sensors |
| Delegated Authorization |
| Encryption Protocols |
| Authentication and Key Agreement for resource constrained sensors |
| Security threats and solution in Wireless sensor networks |
| RFID Tagging |
| IoT Device Identity Management |

| |
|---|
| IoT and eHealth privacy and security issues in proactive personal eHealth architecture. |
| Policies and authorization to access patient information |
| Security in healthcare applications in IoT environment |
| Application layer defense against vulnerabilities |
| Denial of Service attack |
| Network Security Protocols for IoT Devices |
| Device authentication in Body Sensor Networks and Wireless Sensor Networks |
| Authorization and Access Control Lists |
| Confidential communication in the presence of eavesdropper |
| Secure Protocols in Body Sensor Networks |
| IoT Application Design Security |
| Hardware Security |
| Configuration Security |
| Data Encryption at Application Layer |

### 3.1.4 Recommendations Format

Section 3.1.3 identifies a comprehensive list of security verticals and the objective of this survey is to identify and summarize the available research for each of these verticals.

Our recommendation is structured around identifying three to five security verticals that represents the large part of IoT security and providing the best research and solutions for them from the available research that we have read.

## 3.2 INDIVIDUAL CONTRIBUTIONS

### 3.2.1 Ambarish Ravindran

*Role: Team Leader*

- Organized group meetings and collaborated with team members to discuss and monitor the progress of the project.
- Compiled the final project report based on various categories discussed.
- Researched on different papers specifically in Network Layer for the IoT Healthcare ecosystem.
- Researched on eHealthcare architecture for the IoT network by identifying security aspects in that specific area.
- Researched and analyzed the security architecture described in:

**Research Paper:** Internet of Things: Architectural Framework for eHealth Security, Authors: David Lake, Rodolfo Milito, Monique Morrow and Rajesh Vargheese, RP journal, received: 26 June 2013; Accepted: 8 October, 2013.
**Date done:** March 22nd, 2017.

### 3.2.2 Nitesh Gupta

*Role: Deputy Leader*

- Helped in organizing meetings and collaborated with team members to meet deadlines.
- Researched on classification of vulnerabilities in application layer.
- Researched on papers related to identification of solutions to address the vulnerabilities.
- Researched on papers related to encryption of data being exchanged at the Application layer.

**Research Paper:** Gong, Tianhe, et al. "A medical health-care system for privacy protection based on IoT." Parallel Architectures, Algorithms and Programming (PAAP), 2015 Seventh International Symposium on. IEEE, 2015.
**Date Done:** March 14th, 2017

### 3.2.3 Ravi Nihalani

- Explored various Network Layer Authentication techniques in IoT by reading various IEEE papers and online articles.
- Researched on a Novel Authentication and Key Agreement Protocol for Internet of Things Based Resource Constrained Body Area Sensors on February 25th.
- Researched on a Robust Authentication Scheme for Observing Resources in the IoT environment on March 5th.
- Participated in team meetings and actively coordinated with others throughout the research process.
- Collaborated with the team in a timely fashion to complete the report.

### 3.2.4 Vaishnavi Barla

- Explored various Perception layer security aspects by reading multiple articles and research papers.
- Researched about wireless sensor networks and its security issues.
- Participated in meetings and discussions with teammates specifically working on perception layer.
- Collaborated with team mates for paper research and discussions.
- Read and summarized Jan, Mian Ahmad, et al. "A robust authentication scheme for observing resources in the internet of things environment." By 22nd Feb.
- Read and summarized “Yeh, Kuo-Hui. "A Secure IoT-based Healthcare System with Body Sensor Networks." IEEE Access (2016).” by 10th march.
- Read and summarized “Ng, H. S., M. L. Sim, and C. M. Tan. "Security issues of wireless sensor networks in healthcare applications." BT Technology Journal 24.2 (2006): 138-144.” by 15th march

### 3.2.5 Ting Chen

- Researched papers on various Perception Layer security issues and challenges

- Explored papers on authentication technology and its corresponding security issues
- Researched papers on solutions proposed to authentication and secrecy performance
- Actively participated in group meetings and discussions and also helped to find research papers on other subtopics of perception layer
- Collaborated with group members for research and discussions.
  Research papers:
- Read and summarized “Vidyasagar Potdar, Atif Sharif, Elizabeth Chang. “Wireless Sensor Networks: A Survey.” 2009 International Conference on Advanced Information Networking and Applications Workshops” by Feb 22nd.
  Read and summarized “Cancellation-Based Friendly Jamming for Physical Layer Security, Date of Conference: 4 Dec.-8 Dec.2016, Date Added to IEEE *Xplore*: 06 February 2017 “by 16th March
  An Efficient Authentication and Access Control Scheme for perception layer of Internet of Things, Applied Mathematics & Information Science 2017.
  **Date Done:** 2nd March 2017.

### 3.2.6 Sneha Manjunatha

- Researched about the architecture of the perception layer
- Researched about the RFID/NFC technology and its security issues
- Researched about solutions proposed to mitigate attacks in RFID tags
- Collaborated with teammates for research and to discuss papers
- Actively participated in meetings with members working on Perception layer
- Read and summarized Iqbal, Muhammad A., and Magdy Bayoumi. "A Novel Authentication and Key Agreement Protocol for Internet of Things Based Resource-Constrained Body Area Sensors” by 25th Feb.
- Read and summarized “Zhao, Zhenguo. "A secure RFID authentication protocol for healthcare environments using elliptic curve cryptosystem." Journal of medical systems 38.5 (2014): 46.” by March 8th.
- Read and summarized “Porambage, Pawani, et al. "Two-phase authentication protocol for wireless sensor networks in distributed IoT applications." Wireless Communications and Networking Conference (WCNC), 2014 IEEE. IEEE, 2014.” by March 10th

### 3.2.7 Hanumantha Narayana Harish Pendela

*Role*: Principal Investigator

- Read and summarized "A secure Patient Information Transfer method through Delegated Authorization" by February 20.
- Lead the effort in designing survey and report format.
- Read and summarized "Network Security Protocol for Constrained Resource Devices in Internet of Things" by March 10.
- Prepared recommendation format of the report by March 20
- Added findings and analysis on "Delegated Authorization and Encryption in IoT Network Security Protocols" by March 23
- Added Conclusion and recommendations on "Delegated Authorization and Encryption in IoT Network Security Protocols" by March 24
- Worked with Perception layer team and Application layer team in identifying research references for the survey.
- Contributed to overall report formatting and was responsible for validating the reported research content along with Ambarish.

- Added figures and tables for the references read.

### 3.2.8 Maitrayee Pingale

- Read and summarized "Secure End to End key establishment protocol for resource constrained healthcare sensors in context of IoT" by February 22nd.
- Read and summarized "A Secure Authentication Mechanism for Resource Constrained Devices" by March 5
- Read and summarized "Secure MQTT for Internet of Things (IoT)" by March 15
- Researched about Network layer security in IoT healthcare.
- Researched about Encryption Protocols and Key Based Authentication Protocols used in resource constrained devices to enable secure data flow between different sensors.
- Collaborated with team mates for discussions, research and to compile the report.
- Active participant in the project meetings held to discuss the queries, work-in progress and future milestones.

### 3.2.9 Nikhil Lohia

- Researched on application security in wearable sensors on Feb 06th.
- Researched on hybrid security technologies that can be applied for sensor based systems on March 14th.
- Read several papers to understand how the information in healthcare systems and applications are authorized for access.
- Participated in team meetings and collaborated with other members to complete the report in a timely fashion.

### 3.2.10 Sushant Sakolkar

- Researched areas focusing on application layer security in wearable sensors.
- Read and researched various IEEE papers and online articles related to architecture of IoT in healthcare
- Performed a detailed analysis of integrated Body sensor network from a security standpoint on Feb 08th 2017.
- Analyzed off loader architecture to provide full processing capabilities for security measures in IoT applications on March 16th, 2017.

- **Research Paper:** A Back-end Offload Architecture for Security of Resource-constrained Networks, Jiyong Han and Daeyoung Kim Date of Conference: 31 Oct.-2 Nov. 2016 , Date Added to IEEE *Xplore*: 12 December 2016 BSN-Care: A Secure IoT-Based Modern Healthcare System Using Body Sensor Network, Prosanta Gope and Tzonelih Hwang Published in: IEEE Sensors Journal ( Volume: 16, Issue: 5, March 1, 2016)

  **Date done:** March 22nd, 2017

# 4 DETAILED RESULTS

## 4.1 Research papers for each layer

### 4.1.1 Network Layer

#### 4.1.1.1 Attacks on the Network Layer

Attacks on the network layer specifically occur in two forms i.e.: protocol- and layer-specific compromise.

**1) Standard Protocol Compromise:** An attacker deviates from standard protocols (application and networking protocols) and acts maliciously to threaten service availability, message privacy, integrity, and authenticity.

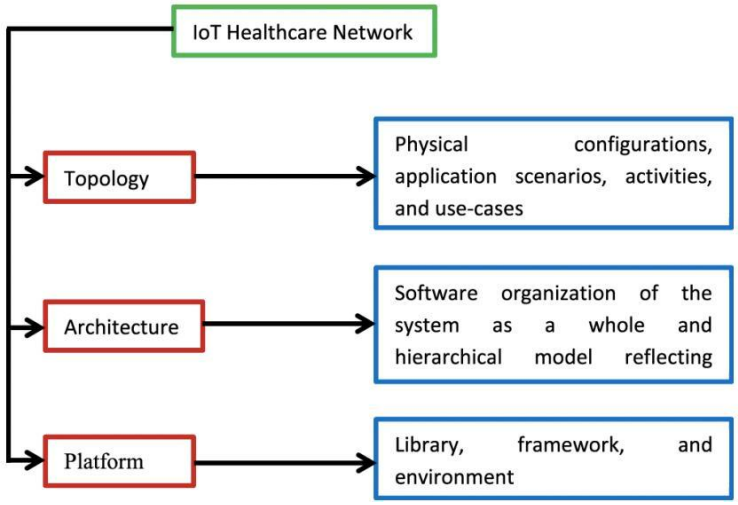



**Figure 1: IoT Healthcare Network Security**

**2) Network Protocol Stack Attack:** As shown in Fig. 1, each layer of the protocol stack proposed by the IETF working group for the IoT network has different types of vulnerabilities that an adversary may exploit to launch malicious activities. To improve the performance of IoT healthcare networks with respect to security, longevity, and connectivity under varying environmental conditions, security should be ensured at each layer of the protocol stack.

#### 4.1.1.2 Current Research in Network Layer

##### 4.1.1.2.1 Internet of Things: An architectural framework for eHealth Security [13]

###### *4.1.1.2.1.1 Security Topics*

IoT and eHealth privacy and security issues in proactive personal eHealth architecture.

###### *4.1.1.2.1.2 Security Issues*

Addressing privacy and security concerns in the IoT Healthcare architecture by integrating it with the model of eHealth.

###### *4.1.1.2.1.3 Proposed Solution*

E-health provides a new method for using health resources - such as information, money, and medicines - and in time should help to improve efficient use of these resources. The Internet also provides a new medium for information dissemination, and for interaction and collaboration among institutions, health professionals, health providers and the public.

**eHealth Characteristics**

The monitoring device's environment is a patient; a living and breathing human being. This change some of the dynamics of the situation. Human interaction with the device means batteries could be changed, problems could be called in to technical support and possibly be resolved over the phone rather than some type of service call. In most cases, the devices on the patient are mobile and not static about location.

The environment for monitoring patients has moved from the hospital healthcare services to a patient's context. M2M/IoT eHealth applications enable remote monitoring of patient health and fitness information, the triggering of alarms when critical conditions are detected, and in some cases the remote control of certain medical treatments or parameters.

**The Integration of IoT and eHealth**

Harnessing the power of Internet of Things for eHealth creates a lot of opportunities to improve outcomes and drive wellness is populations thereby reducing the strain points of today's healthcare system. Some of the most promising use cases of connected e-health include preventive health, proactive monitoring, follow-up care and chronic care disease management.

The changes, uniqueness, opportunities, and complexities of e-health enabled by the power IoT is significant and can be characterized by some of the changes that we anticipate in the ecosystem. They include

- The number of devices that will come online
- The number of devices that will generate information
- The number of decision making points
- The number of entry points into the system
- The number of types of devices
- The number of types of interactions of devices, applications, and processes
- The number of opportunities to leverage the data

**Security Architectural Model Proposed**

To evaluate the security architecture for e-health, the architecture is broken down into multiple sections and the security challenges are evaluated in each of these domains. As depicted in Figure 2, the main domains include endpoint and access, cloud services, partners, and providers.
eHealth applications in an M2M/IoT environment run on several components, including sensor devices and actuators, and networking, processing and storage elements. The overall level of security is upper-bounded by the weakest component in this interactive system. Hence, each component, and the overall system must be designed with security in mind.

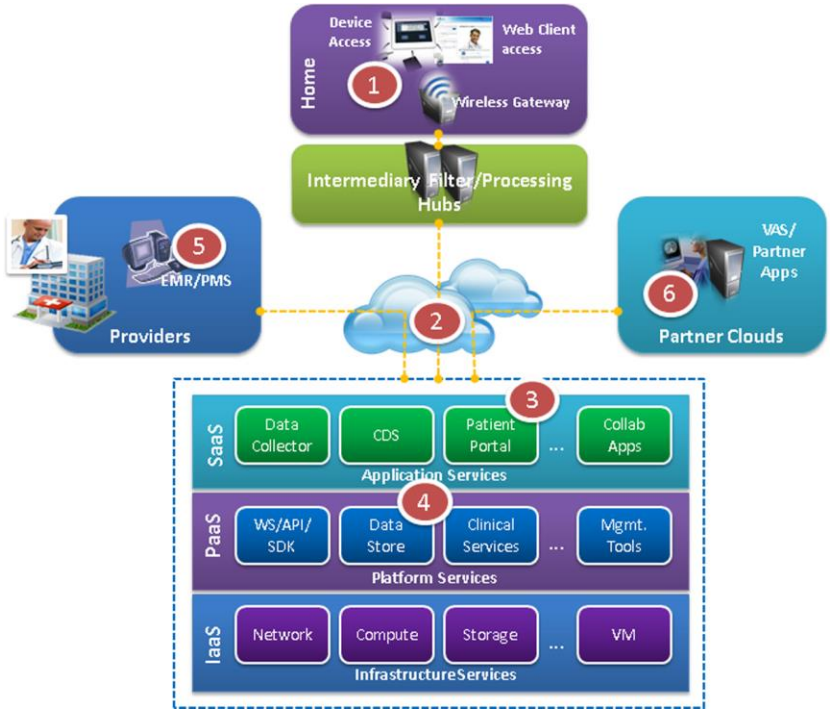



**Figure 2: eHealth Security Domain Touchpoints**

There are three basic attack vectors, and a corresponding attack surface to each vector. Data is the first attack surface, and the communication channels the second one. M2M/IoT brings forth a third, novel attack surface: physical attacks on or through the medical device.

**Real world Scenario illustrating eHealth Security**

Consider a patient with a blood pressure monitoring device, which takes a blood pressure reading every 15 minutes and the device itself or another local device, which has a collector function stores the readings. Once a day the device or collector and the medical facility's application server communicate with each other to transfer the reading to the server. The collector function
could be in the M2M gateway. The readings may be summarized or some other data manipulation technique performed, and then the medical staff reviews the results.

This simple example illustrates **several areas for security to address**

On the device and collector:
• Secure Boot of the device for platform integrity check and boot loader authenticity

• Secure Storage of the secret keys. The storage should be physically tamper resistant and access control protected
• Secure Storage of the data
• Device identification must be a unique identifier within the eHealth context

For the communication channel:
• Mutual Authentication between the eHealth device and the application server and/or the network
• Data Integrity to protect the data from any alteration during the communication session
• Data Confidentiality uses encryption and decryption of data between the secure device and the application server and/or network during data exchanges

In the Ecosystem:
• Key Management of the secret keys in the eHealth
• Cryptographic Support of cryptographic protocols, such as AES and optionally PKI

**Data Storage Security**

The federal information processing standards publication lists the security requirements that need to be satisfied by a cryptographic module utilized within a security system protecting sensitive information and defines four qualitative levels of security.

Level 1: Lowest level of security and allows the software and firmware components of a cryptographic module to be executed on a general-purpose computing system.

Level 2: Enhances the physical security mechanisms by adding the requirement for tamper evidence. This level requires role-based authentication and authorization of an operator to assume specific role and functions.

Level 3: Enhances security to prevent intruder from gaining access to critical security parameters using an identity based authentication mechanisms.

Level 4: Highest level of security and provides a complete envelope of protection around the cryptographic module with the intent of detecting and responding to unauthorized attempts to physical access.

#### *4.1.1.2.1.4 Security Challenge*

The coming of age of eHealth is intrinsically linked to the successful deployment of a secure and privacy-preserving M2M/IoT infrastructure.

### 4.1.1.2.2 A Novel Authentication and Key Agreement Protocol for Internet of Things Based on resource - constrained Body Area Sensors [1].

#### *4.1.1.2.2.1 Security Topics*

Authentication and Key Agreement for resource constrained sensors

#### *4.1.1.2.2.2 Security Issues*

• Healthcare wearable devices are being employed for numerous healthcare applications, ambient assisted living, sports, and fitness applications. Usually a person has more than one device worn-on his body. For

instance, a person can have Fitbit, smartwatch to collect physiological data, sensors to take the blood pressure, pulse oximeter, pedometer, and other implanted sensors.

• Several issues related to security and privacy of user's data come up: How does the gateway (smart phone) authenticate these sensors? How these sensors are paired with gateway? How to balance the user's privacy and usability? Encryption employed cannot be same for all these sensors with varying available resources. The integration of sensors in the Internet must ensure the interoperability, transparency, and flexibility.

##### *4.1.1.2.2.3 Proposed Solution*

• The protocol proposed is a key agreement and authentication protocol to establish a secure E2E channel based on offloading heavy cryptographic functions to the trusted neighboring sensors in the context of IoT. These sensors accompany triaxial accelerometers for correlating their data to find out whether sensors are installed on the body.

• Security analysis and performance evaluations are made to prove that the proposed protocol is secure enough and is lightweight for implanted sensor that has scarce computational and energy resources.

• The Authentication and key agreement protocol proposed here is suitable to protect sensitive health related data in the context of Internet of Things.

##### *4.1.1.2.2.4 Security Challenges*

A comprehensive body area network system for healthcare application has not been implemented yet. More experiments should be performed after integrating this approach with the actual medical sensors accompanying accelerometers installed on the body and ultimately develop a full body area network system for healthcare application in IoT.

#### 4.1.1.2.3 A Robust Authentication Scheme for Observing Resources in the Internet of Things Environment [2].

##### *4.1.1.2.3.1 Security Topics*

Authentication of IoT devices for resource utilization

##### *4.1.1.2.3.2 Security Issues*

• Most of the physical devices in IoT are vendor specific and lack a unified standard, which renders their seamless integration and interoperable operations.
• Another major concern is the lack of security features in these devices and their corresponding products. Most of them are resource-starved and unable to support computationally complex and resource consuming secure algorithms.

##### *4.1.1.2.3.3 Proposed Solution*

•The lightweight mutual authentication scheme proposed here validates the identities of the participating devices before engaging them in communication for the resource observation in a CoAP-based IoT environment by using a single key. The scheme incurs less connection overhead and provides a robust defense solution to combat various types of attacks like eavesdropping, key fabrication, resource exhaustion and denial of service attacks.

• A session key is exchanged between the communicating endpoints. Each client maintains a session key with a given server which ensures that both the parties have been authenticated. The handshake mechanism is employed for client and server authentication. Once authentication is completed, the clients register themselves with the server for resource observation.

The proposed algorithm is a twostep process:

1. Lightweight CoAP-based Authentication Scheme: CoAP is a lightweight alternative of the HTTP protocol for the resource constrained devices, hence simple but robust authentication schemes need to be developed to prolong the network lifetime. Here, the paper proposes an authentication algorithm that is simple in computation but it can be a robust alternative to the Datagram Transport Layer Security (DTLS) due to its ease of implementation, infrastructure and complexity. Both the client and server challenge each other to authenticate themselves. The authentication mechanism completes using four handshake messages (shown in the below diagram) between any client and the server. Each message is comprised of 256 bits except the initial handshake authentication request of the client. Hence the total connection overhead incurred during the authentication session is less than 1024 bits, which is well suited to the IoT-based devices. In this scheme, the authentication is completed using the 128-bit Advanced Encryption Standard (AES) which is sufficient for the energy-constrained devices participating in the IoT paradigm.

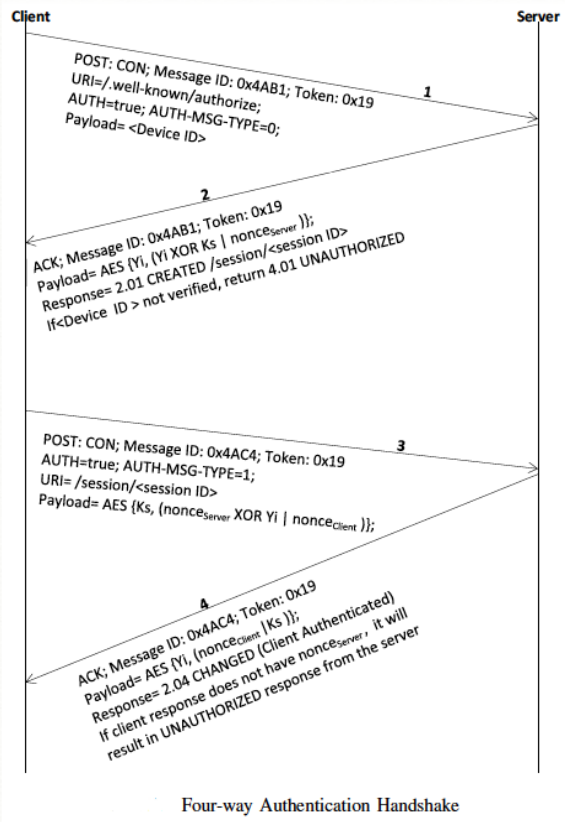



**Figure 3: Four-way Authentication Handshake**

2. Conditional Resource Observation in IoT (Data Transmission): Once authentication is completed, the clients register themselves with the server for resource observation. Each client specifies certain conditions for the notification messages based on their application requirements. The

server notifies the clients once those conditions are fulfilled. This reduces the number of undesirable transmissions which enhances network lifetime and leverages congestion.

#### *4.1.1.2.3.4 Security Challenges*

The scheme proposed in the paper is an efficient solution against eavesdropping, key fabrication, resource exhaustion and denial of service attacks. However, it is not efficient against Sybil attack. In Sybil attack, a single malicious node poses multiple identities to the communicating devices at a given time. These identities are either fabricated or stolen by disabling the legitimate nodes of the network. Hence, a single physical device can harm multiple network resources.

### 4.1.1.2.4 A Secure Patient Information Transfer Method through Delegated Authorization [11].

The proposal is to propose a secure transfer method of patient information collected from IoT devices among hospitals via a delegated user trusted by the patient using an access token issued by a token repository.

#### *4.1.1.2.4.1 Security Topics*

Delegated Authorization

#### *4.1.1.2.4.2 Security Issues*

Any authorized medical personnel can access patient information collected from IoT devices and stored on hospital servers which could lead to leakage of personal information.

#### *4.1.1.2.4.3 Proposed Solution*

The author uses delegated authorization to present a solution for the proposed problem, Patient appoints a delegated user to initiate transfer of patient information from Hospital A to Hospital B. Here the delegated user initially receives an access token from Hospital A when the patient registers the delegated user into Hospital A's network. Now, when the patient is admitted to Hospital B and requires his/her information to be transmitted from Hospital A to Hospital B, the delegated user then initiates a request by authenticating himself/herself(using his/her mobile phone) and sending his/her access token to Hospital A along with the information about Hospital B. Hospital A verifies this access token, and encrypts patient's information using the public key of Hospital B. Hospital B decrypts this information using its own private key. Per the author, only a delegated user can initiate/access patient information collected from various IoT devices by adding an extra layer of security (using access tokens) above the IoT security communication protocols that are used to authenticate and authorize a user.

| **Name** | **Definition** |
|---|---|
| Resource Owner(RO) | A patient who saves medical and healthcare information with Hospital A |
| D-User | An authorized user in trust relationship with RO. |
| Hospital A | A hospital that constantly saves patient information. |
| Hospital B | A hospital visited by patient in an urgent situation. |
| Token, Key Repository | Where Token or Key is stored |
| Mobile Authenticator | Mobile phone authentication service provider |

**Table 1: Actors in the System**

#### *4.1.1.2.4.4 Security Challenges*

Secure transmission of information from one hospital to another is a challenge.

### 4.1.1.2.5 Network Security Protocol for Constrained Devices in Internet of Things [12].

This paper proposes a security protocol for IoT devices that uses minimum processor capacity by giving different bit-streams in each authenticated session for the same data which cannot be predicted by the transmitter itself.

#### *4.1.1.2.5.1 Security Topics*

Network Security Protocols for IoT Devices

#### *4.1.1.2.5.2 Security Issues*

Security protocols built on strong cryptographic algorithms consume a lot of processor's efficiency. IoT devices with limited processor capabilities need some modified secure protocols particularly in healthcare systems where safe and secure transmission of sensitive patient information is of utmost importance. Security, trustworthiness, and privacy are major challenges in IoT and lack of strong security protocols in IoT will enable adversaries to perform attacks with malicious intent.

#### *4.1.1.2.5.3 Proposed Solution*

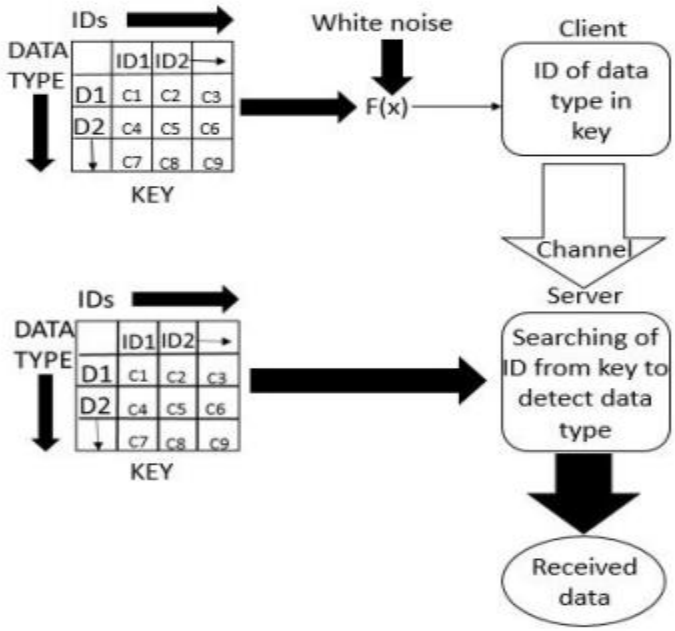



**Figure 4: Protected Exchange of Messages**

The author proposes a secure mechanism for session key generation as shown in the following figure. To allow for a protected exchange of messages between the server and the constrained client device, both entities must share a symmetric key which is the device specific master key. This key may be imprinted in the device via physical contact or by flashing software manually, on the client device.

If the key used is fixed or static the entire key can be reproduced by the hacker and so eavesdropping the content of communication leads to wormhole or black hole attacks in network and hence the short time valid key is to be used. This is achieved by loading the client as well as the server by a shuffling algorithm to generate challenge based session key. The algorithm intakes the current time and challenge to shuffle the master key and accordingly generate new session key.

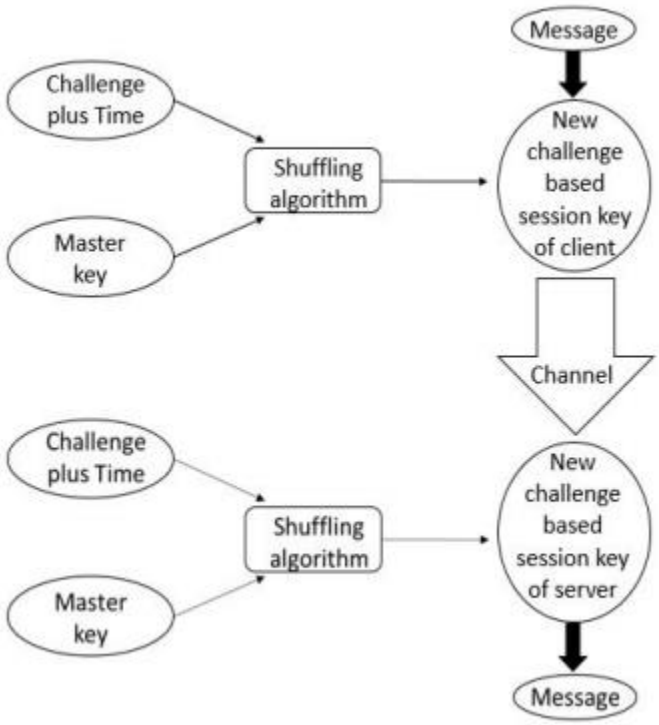



**Figure 5: New Session Key Generation**

This paper adapts different key management scheme as the key can be compromised if the client device is physically hijacked. Few key management models proposed by the paper are

1. The master key and the algorithm which generates session key can be same for different point-to-point communication of client and servers when the physical security assurance of client devices is taken into consideration.
2. The master key is same for all the client devices but the algorithm which generate session key are different so the client device identity is specified by the algorithm which generate session key as well as their UTC and challenge.
3. The master key, as well as the algorithm used to produce session key both are different for different client devices. In this model, the unique algorithm specifies the client device identity, key as well as UTC of the client. This model will provide the best security, but key management is a challenge here.

#### *4.1.1.2.5.4 Security Challenges*

Following figure depicts the security challenges faced by the current light-weight cryptographic protocols.

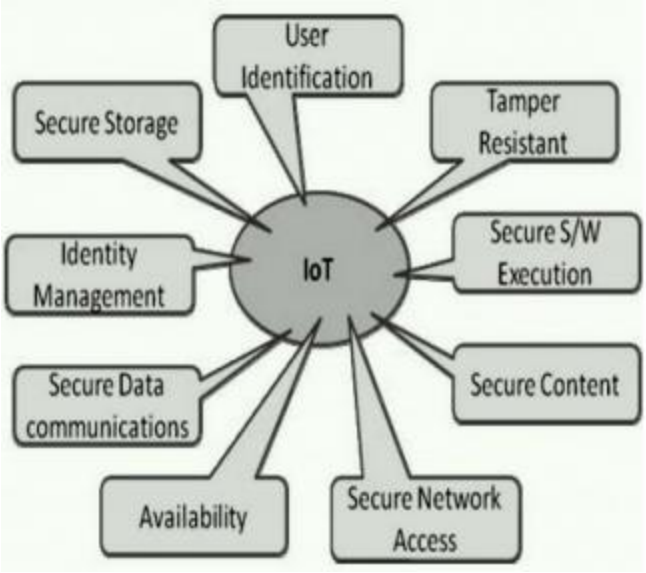



**Figure 6: Security Challenges**

Following are the challenges faced by light-weight cryptographic protocol

- Heterogeneity of devices. Constrained devices will interact with other devices with different API or full-fledged web servers.
- Possible cryptanalytic attack as the messages are transformed in an encrypted form using algorithm based on key for a given authenticated session.
- Authentication used for peer-to-peer networking incurs significant processing and transmission overheads in constrained network environment.

#### 4.1.1.2.6 Secure End to End key establishment protocol for resource constrained healthcare sensors in context of IoT [8].

##### *4.1.1.2.6.1 Security Topic*

Encryption protocol

##### *4.1.1.2.6.2 Security Issue*

Data flowing from and to the devices is more prone to malicious attacks. In Iot, one cannot use conventional security measures to mitigate because of resource constrained devices, unreliable communication links, distributed nature, etc.

##### *4.1.1.2.6.3 Solution Proposed*

This paper proposes an end to end key establishment protocol which is lightweight for a resource constrained devices and still provides same security functionalities like the unconstrained one's. According to this protocol, the heavy cryptographic operations are offloaded to the neighboring trusted devices.

Here both the end devices need to authenticate each other first and then share secret key to communicate encrypted data. For key establishment, it uses asymmetric cryptographic techniques. If a server A wants to communicate with sensor node B which doesn't have any pre-shared secret key with A. The

cryptographic functions required for B are very heavy and hence they are offloaded to neighboring devices. The selection of devices for offloading is done by trustworthiness and resource availability.

#### *4.1.1.2.6.4 Security Challenges*

There is a possibility of Denial of Service attack where a malicious node interrupts by sending redundant message to the sensor node or any device on the IoT network. But this is avoided here as the communication happens only through trusted nodes and devices. This protocol also helps maintain confidentiality of the data flowing between the devices. IPsec, a protocol suite, is used to exchange the shared keys. Here each IP packet is authenticated and encrypted before sending over the network. The communication channel is made secure by use of MAC's. Overheads are reduced as encryption task is offloaded from the resource constrained devices.

Every communication, to and from the trusted nodes, is encrypted and authenticated end to end thus making Man-In-Middle attack and eavesdropping impossible. It keeps list of trusted neighbors and also uses message encryption to prevent the IoT network from Sybil attacks, wherein intruder uses many fake identities to send over wrong information.

### 4.1.1.2.7 Secure MQTT for Internet of Things (IoT) [10].

#### *4.1.1.2.7.1 Security Topic*

Communication protocol

#### *4.1.1.2.7.2 Security Issue*

Devices (sensor, RFID) form the primary part of Internet of Things and security of devices and communication between them is of utmost importance. Existing communication protocol aren't secure enough to prevent malicious attacks.

#### *4.1.1.2.7.3 Proposed Solution*

A secure version of Message Queue Telemetry Transport (MQTT) and Message Queue Telemetry Transport for Sensor Networks (MQTT-SN) are proposed for secure communication between different devices. In the new proposed protocols, security features added to the existing MQTT and MQTT-SN protocols are based on Attribute Based encryption (ABE).

A suggestion was to use SSL/TLS with certificates and session key management. Managing of certificates and key exchanges for every session is little too much and may result in BEAST, CRIME, etc. attacks. Hence a lightweight and scalable security mechanism like ABE is needed. ABE supports broadcast encryption which is a big plus point in IoT. There are two variants of ABE: 1. Ciphertext Policy based ABE 2. Key Policy based ABE.

Proposed Secure MQTT:
An MQTT is based on TCP with Pub-Sub protocol for device to device communication via a broker. The Publisher publishes message under a topic and all the subscribers receive it through the broker. Different message types are used and types are understood by message type value in an MQTT message header.

And variable header of the message header has username and password flag. These values are not encrypted and hence can be an easy prey for an attacker.

| bit | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 |
|---|---|---|---|---|---|---|---|---|
| byte 1 | Message Type | | | | DUP Flag | QoS Level | | Ret |
| byte 2 | Remaining Length | | | | | | | |
| Variable Header | | | | | | | | |
| Payload | | | | | | | | |

**Figure 7: MQTT Header**

A new ABE based secure MQTT is adapted on lightweight Elliptic Curve Cryptography with a proposed new publish service 'Spublish' where message type 0000 is reserved message type.
The publisher publishes an ABE encrypted message using Spublish. The subscribers should have the access policy to decrypt the message.

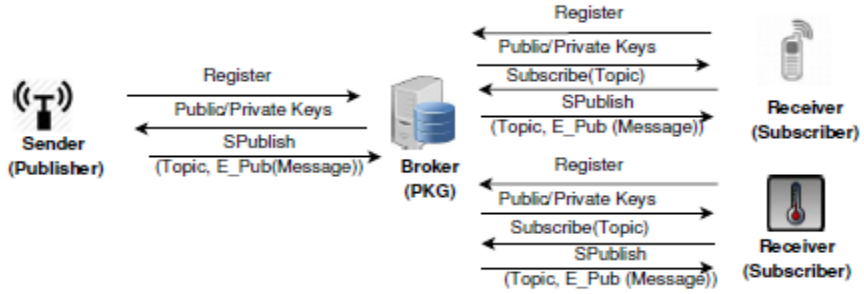



**Figure 8: Architecture of the scheme**

Proposed ABE for SMQTT: The data is encrypted at the sender by using some conditions in accordance of access policy and the receiver will be able to decrypt the message only if it has those access policies. Access policies are conditions having user attributes like feature, property, role, etc.
KP and CP ABE are based on key based or ciphertext based access policies.
Proposed SMQTT Protocol: There are three important roles
1. Publisher - which publishes the data
2. Broker - trusted third party
3. Subscriber - receives the data. The protocol has four phases:
    1. Setup phase: considers registration and key management.
    2. Encrypt phase: encrypting the data
    3. Publish phase: data is published
    4. Decrypt phase: subscriber decrypts the received data

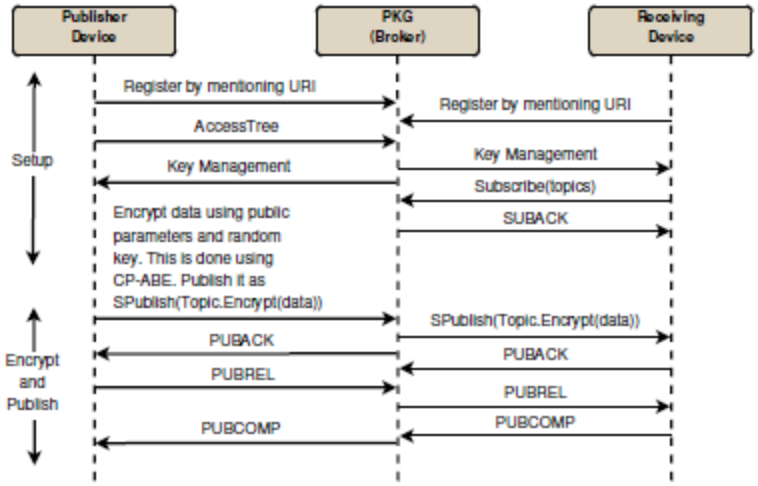



**Figure 9: Proposed SMQTT Protocol**

Proposed Secure MQTT-SN Protocol: This is based on MQTT-SN protocol which is for sensor networks. Publisher uses CP/KP-ABE to encrypt the message, sets the type appropriately and sends to gateway. Gateway converts publish to Spublish and sends to broker. Broker now sends it to the subscribed gateways. Gateways now converts Spublish command to publish and sends to the subscribers which if have correct access policies can decrypt the message.

#### *4.1.1.2.7.4 Security Challenges*

Broker Hijacking: The confidentiality of message is ensured as the encrypted data can be decrypted only with one's with correct access policies. Therefore, no malicious attacker can intercept the data. Thus end to end security concern is out ruled here.

### 4.1.1.2.8 A Secure Authentication Mechanism for Resource Constrained Devices [12].

#### *4.1.1.2.8.1 Security Topics*

Authentication and Key Agreement for resource constrained sensors

#### *4.1.1.2.8.2 Security Issues*

Wireless Sensor Network is one of the key elements in IoT paradigm. Applications which use wireless sensor network collect the data from the sensors over a long time and because of the wireless nature malicious data can be easily injected or during forwarding, content of valid messages can be changed. As the sensors are resource constrained it is difficult to install traditional security measures to prevent such attacks.

#### *4.1.1.2.8.3 Proposed Solution*

The sensors are resource constrained and hence one cannot use traditional security measures to prevent them from being attacked and modify the data. Work around this problem is using broadcast authentication technique. It is a fundamental security service where the sender can broadcast data in a authenticated way to the receiver such that no attacker can make any changes to the data.

There are three categories of tools of authentication: first, signature based authentication mechanisms for Ex. elliptic curve signature. These consume a lot of energy, but they also provide message authentication. But here there are chances of signature-based Denial-Of-Service attack. One-time signature is the second category, which ensures immediate message authentication. It also extends many signatures which can't be forged under chosen message attacks. But only messages can be signed using a single key pair and person can misuse the disclosed information. And the last one is using lightweight symmetric authentication scheme.

**$\mu$TESLA based schemes**

$\mu$TESLA is one of the many proposed symmetric authentication scheme, where authentication key is secret for some time and will be open or disclosed after some time. It is better with resource constrained devices and for key distribution uses key chain mechanism. For sending a message it just must send message authentication code (MAC). Each time interval, divided from transmission time, has an authentication key which is image of next key using random one-way hash function. This authentication key is just to authenticate messages. Here number of intervals gives us authentication delay. But this delay can be forged by DOS attack which will cause buffer overflow.

LEAP based schemes: It provides security by four key establishment. These four keys are

1.Individual authentication key

2. Pairwise key

3.Cluster key and

4.Group key.

Base station and Sensor nodes share a group key while, cluster key is shared by a node and its neighbors and local broadcast messages can be secured with it. Random key is generated by a node which is encrypted in a pairwise key. This is key is then circulated among all the neighbors. The key is the one which is globally shared and is used by base station to encrypt messages to be sent to the group. It has high authentication delay.

**Advanced Authentication mechanism**

It minimizes the authentication delay by giving out the authentication key early when the packets are transferred.

Authentical delay = time of real authentication of messages - time of reception at receiver's buffer

Three factors influencing the delay value are: application sensitivity to the delay, propagation delay and transmission rate. The transmission delay can be given by equation:

$$Dmk = N \times (Dtr + Dk) + Dpr$$

Where, Dmk is the transmission delay

N is no of hops

Dtr is frame transmission delay

Dk is key computation delay

Dpr is propagation delay

This mechanism can be integrated with LEAP and LEAP++ which will result in less authentication delay.

#### *4.1.1.2.8.4 Security Challenges*

In larger sensor networks, there are problems for distribution of key chain commitments while using $\mu$TESLA. Using the new security mechanism which makes use of $\mu$TESLA and delivery time will reduce the impact of Denial-Of-Service attacks but won't remove it totally. Therefore, DOS remains a concern.

## 4.1.2 Perception Layer

### 4.1.2.1 Features of Perception Layer

This is also known as the Device Layer. It includes various kinds of sensors, RFID, ZigBee, etc. This layer collects data from the physical environment. The signals are exposed in the public place. If it lacks effective protection measures, the signals will be monitored, intercepted, and disturbed easily. The most of sensing devices are deployed in the unmanned monitoring sites. The attackers can easily gain access to the equipment, control or physically damage them. (referred to A Survey on the Internet of Things Security)

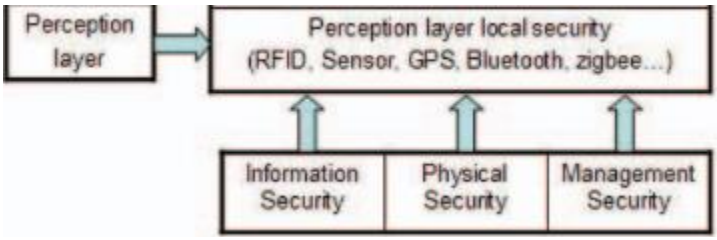



**Figure 10: Perception Layer Architecture**

Some of the security features are as follows:

1) **Node Capture**: the attackers easily control Key nodes such as gateway node. It may leak all information, including group communication key, radio key, matching key etc, and then threats the security of the entire network.

2) **Fake Node and Malicious Data**: The attackers add a node to the system, and input fake code or data. They stop transmitting real data. The sleep of the energy limited node is denied. They consume precious energy of nodes, and potentially control or destroy the entire network.

3) **Denial of Service Attack**: DoS attack is the most common attack in WSN and Internet. It causes loss of network resources, and makes the service unavailable.

4) **Timing Attack**: By analyzing the time required for executing encryption algorithm, to obtain key information.

5) **Routing Threats**: Through cheat, tamper or resend routing information, the attacker can create routing loops, cause, or resist network transmission, extend, or shorten the source path, form the error messages, increase the end-to-end delay, etc.

6) **Replay Attack**: Attacker sends a package which has been received by the destination host, to obtain the trust of system. It mainly used in the authentication processing, and destroy the validity of certification.

7) **SCA (Side Channel Attack)**: Attacker attacks encryption devices, through the side channel leakage information in the process of the device operation, such as time consumption, power consumption, or electromagnetic radiation.

8) **Mass Node Authentication Problem**: The efficiency of mass node authentication needs to be solved in IoT.

#### 4.1.2.2 Current Research in Perception Layer

##### 4.1.2.2.1 An Efficient Authentication and Access Control Scheme for perception layer of Internet of Things [17].

###### *4.1.2.2.1.1 Security Topics*

Authentication and Authorization

###### *4.1.2.2.1.2 Security Issues*

This paper proposed a simple-efficient mutual authentication and secure key establishment based on ECC that adopted ABAC-based authorization method addresses the following security issues:

- Solves the resource-constrained problem of perception layer in IoT
- Prevent malicious attacks by providing a mutual authentication between users and nodes
- Defend against man-in-the-middle attack
- Defend against eavesdropping attack
- Defend against node capture attack
- Mitigate Denial of Service
- Defend against replay attacks

###### *4.1.2.2.1.3 Proposed Solution*

This paper proposed a lightweight ECC to complete the authentication and build a secure session key. In the proposed scheme, through mutual authentication between users and sensor nodes, only legitimate user can have access to resources that is made available and the architecture revolves around this idea. The following figure shows the architecture of this model.

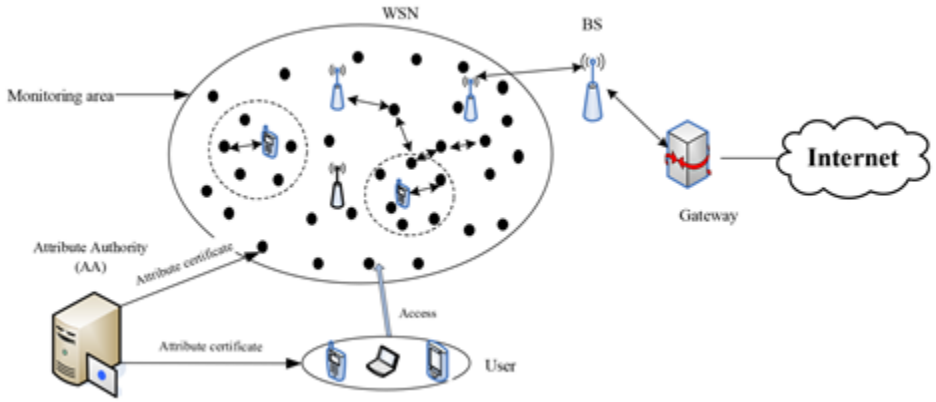



**Figure 11: The structure of perception layer in IoT**

In the above architecture, huge amounts of sensor nodes are deployed in the monitoring area. Sensor nodes connect to the transport layer through sensor subnet manager. The base station gathers data and send command to sensor nodes. User can be notebook computers, mobile phones, personal digital assistant, etc. The Attribute Authority in perception layer creates and manages the attribute information. Users can access resources only with appropriate permissions.

The proposed method adopted a method of ECC-based mutual authentication to establish public-private key pairs. The authentication is divided into two phases: initialization phase and mutual authentication and key establishment phase.

##### *4.1.2.2.1.4 Security Challenges*

The proposed ECC-based authentication and access control policy can efficiently achieve mutual authentication between user and nodes. Mutual authentication secures the communication between user and nodes, which solve the resource-constrained problem of perception layer in IoT. However, this paper adopted an attribute-based access control policy which needs further studies.

#### **4.1.2.2.2** Cancellation-Based Friendly Jamming for Physical Layer Security [16].

##### *4.1.2.2.2.1 Security Topics*

Confidential communications in the presence of an eavesdropper

##### *4.1.2.2.2.2 Security Issues*

- Due to the broadcast nature of wireless medium, wireless networks are exposed to security challenges such as jamming or eavesdropping attacks from adversaries in the wireless network area. This situation will worsen in the forthcoming internet of IoT environments because of the drastically increasing connectivity.
- Current physical layer security(PLS) studies have yet to solve many challenges in real and practical security systems because most of these studies are based on non-realistic assumptions.

This paper proposed a cancellation-based friendly jamming scheme to achieve confidential communications in the presence of an eavesdropper.

##### *4.1.2.2.2.3 Proposed Solution*

This paper proposed a cancellation-based friendly jamming power allocation strategy to achieve confidential communications in the presence of an eavesdropper. Especially, cancellation scheme proposed can cancel jamming interference at the intended receiver by sharing secret keys. This paper work differs from previous studies in that it considered practical cancellation capability. It analyzed interrelationship between the cancellation capability and secrecy performance in terms of probabilistic evaluation. It also quantified the achievable secrecy performance by using the secrecy efficiency function in terms of the outage probability. From the results, the optimal jamming power allocation strategy in the convex optimization form was derived. As a result, cancellation scheme proposed can achieve confidential communications without full/partial CSI and intentional beamforming technique.

It made the following contributions:

- Derived the optimal cancellation capability for the maximum secrecy rate which provides clues to resolve the non-convex problem.

- Designed the optimal jamming power ratio in the limited power budget, which can be realized in the practical system and scenarios.
- The simulation results showed the possibility of the confidential communications, without transmitters having CSI in the practical network environment.

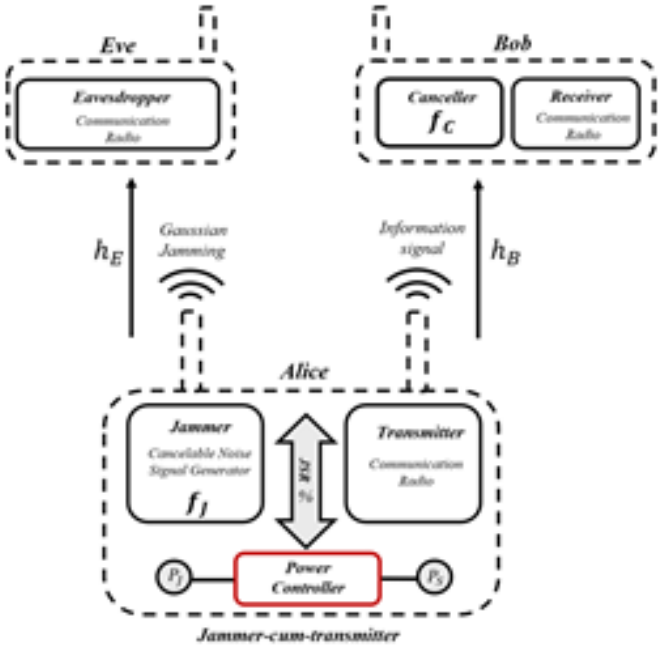



**Figure 12: The system model of the proposed technique. Alice has jammer-cum-transmitter; Bob can cancel jamming interference but Eve cannot.**

#### *4.1.2.2.2.4 Security Challenges*

This paper assumed a single eavesdropper and a pair of transmitter and receiver as the paper focused on the tradeoff between cancellation capability and jamming power ratio for perfect secrecy communication. Secrecy performance in case of multiple eavesdroppers and cooperative jammers needs to be investigated in the future as well as an attempt to design practical jamming signal generators and cancellers by using a universal software radio peripheral.

### **4.1.2.2.3** A Secure RFID Authentication Protocol for Healthcare Environments Using Elliptic Curve Cryptosystem [20].

#### *4.1.2.2.3.1 Security Topics*

RFID Tagging

#### *4.1.2.2.3.2 Security Issues*

Providing an efficient RFID authentication mechanism.

#### *4.1.2.2.3.3 Proposed Solution*

This paper proposes a new design of the authentication scheme. This protocol consists of two phases

1. Setup phase: This phase is used to generate system parameters, private keys and public keys for the server and the tag.
2. Authentication phase: This phase is used by the server and the tag to authenticate each other. The details are as follows:

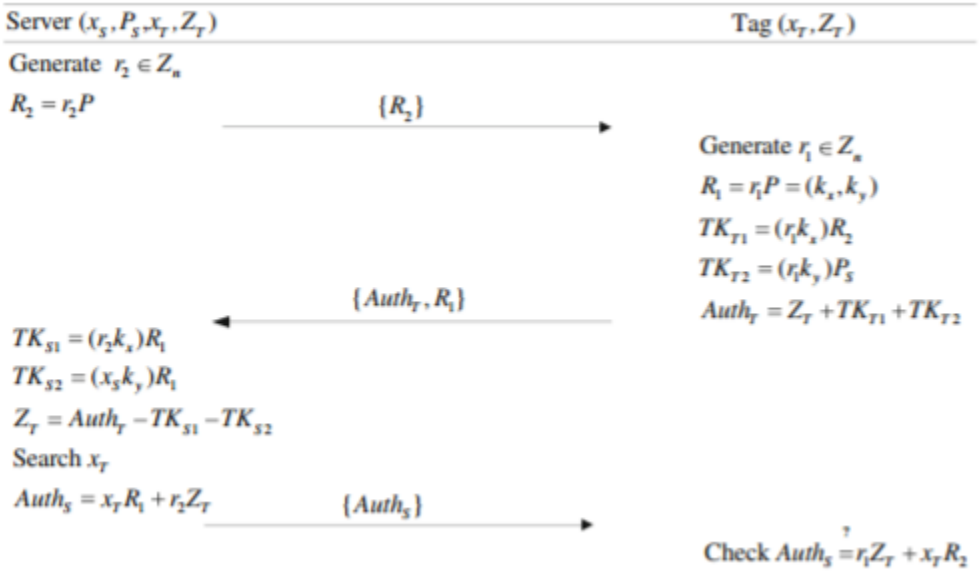



**Figure 13: Authentication phase of proposed protocol**

1. The server generates a random number and computes R = rP. Then the server sends the message to the tag.
2. Upon receiving the message, the tag also generates a random number and computes R=rP= (kx,ky). It also computes another message and an authentication parameter and sends these to the server.
3. Upon receiving these parameters, the server recomputed the message from the authentication parameter and searches for it in the database. If it not present, the server stops the session else it generates a corresponding private key and sends that to the tag.
4. Upon receiving the message the tag checks whether the original message of the tag and the one received from the server matches. If not equal the tag stops the session else the server is authenticated.

#### *4.1.2.2.3.4 Security Challenges*

1. Key compromise problem in the Liao and Hsiao proposed Elliptic curve cryptosystem(ECC).
2. Tag tracking as same identity is used in different sessions.
3. Withstanding the replay attack.

### 4.1.2.2.4 Two-phase Authentication Protocol for Wireless Sensor Networks in Distributed IoT Applications [21].

#### *4.1.2.2.4.1 Security Topics*

Authentication in Wireless Sensor Networks.

#### 4.1.2.2.4.2 Security Issues

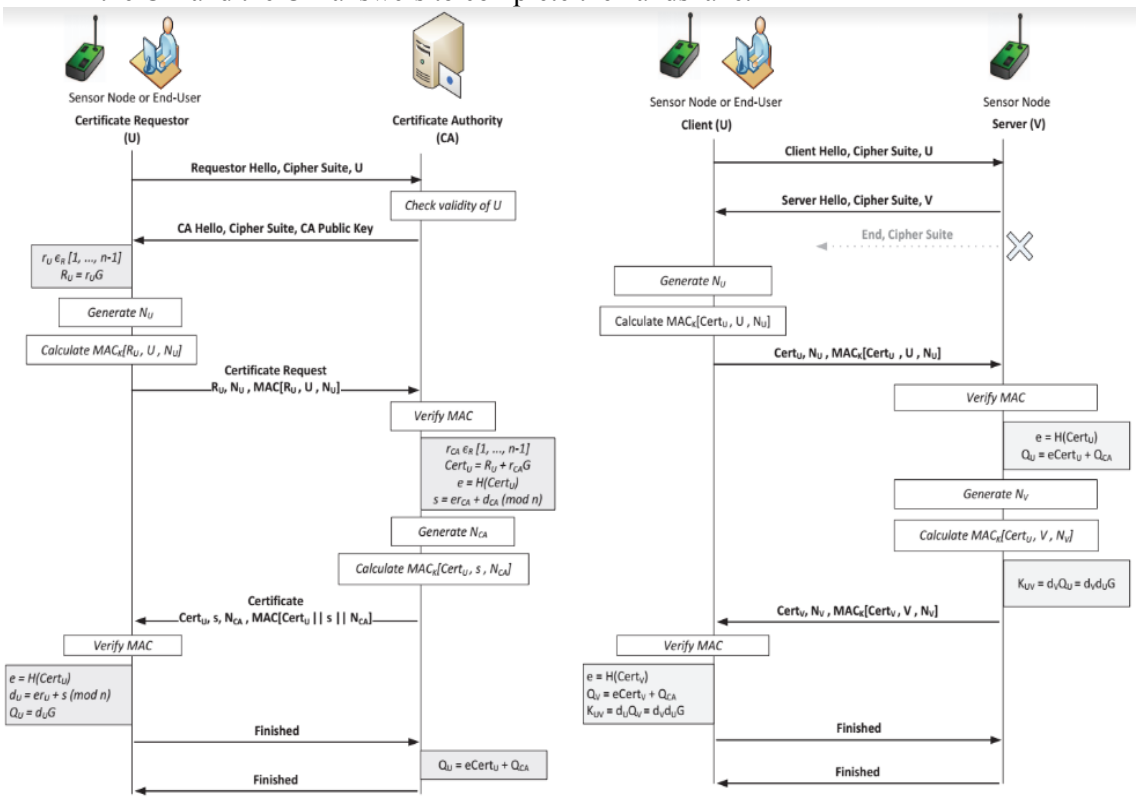
Secure links for end-to-end communication with proper authentication to provide connectivity and the accessibility of distributed IoT.

#### 4.1.2.2.4.3 Proposed Solution

This solution encompasses two phases:

*Registration Phase*: This is used to obtain security credentials from a trusted party. The network edge devices and the end user requests the certification authority(CA) to provide credentials. In the registration flow diagram, the white boxes represent actions performed by the entities and grey represents the user variables.

- The protocol starts with a handshake with a hello message, node identity and cipher suites that are embedded in the sensor nodes and known by the end user. On successful identity verification, the CA agrees to one combination of the cipher suite and sends back a hello message as a public key to approve the initiation of the handshake.
- Upon receiving the message the requestor generates a certificate request EC point and a true nonce and a Message Authentication Code(MAC) value and sends a 'Certificate request to the CA. On validating the CA sends a certificate message with a nonce and a message. On verification, the requestor computes its own private and public keys. A finished message is sent to the CA and the CA answers to complete the handshake.




(a) Flow Diagram of Registration Phase

(b) Authentication Phase (end-to-end authentication)

**Figure 14: Overview of the protocol**

*Authentication phase***:** To establish an authenticated communication, the edge nodes and end-users should have a certificate and specific cipher suites. In the (b) part of the above figure, several message transfers of authentication phase between the client node and the server node are considered. First the client sends a Hello message to the server followed by the cipher suite options and identity. The client only sends the

cipher suites, which has certificates. After a finished message is sent, a secure communication link is established.

#### *4.1.2.2.4.4 Security Challenges*

The major security challenges faced are network entity identity, authentication, access control, and secure communication channel establishment. The proposed protocol should be robust to node mobility and network scalability due to the dynamic behavior of nodes in distributed IoT.
Network heterogeneity and device mobility is another challenge which if not addressed would be a threat to the entire network.

### 4.1.2.2.5 A secure IOT based healthcare system with Body Sensor networks [18].

#### *4.1.2.2.5.1 Security Topics*

Secure protocols in Body Sensor networks

#### *4.1.2.2.5.2 Security issues*

Physical protection for smart objects, maintain data confidentiality, integrity and privacy during data collection among smart objects, Device authentication mechanism, replay attacks.

#### *4.1.2.2.5.3 Proposed solution*

1. Session key is required for secure communication: For secure communication, In traditional methods based authentication mechanisms, a robust session key must be agreed for secure communication among entities. An authentication and login without session key generation will not guarantee security. There are some methods such as SSL/TLS – (secure socket layer and transport layer security) or other security techniques that can achieve robust security after authentication but the computation cost will not make it efficient. Hence session key agreement is essential for entity authentication and secure communication.
2. Inappropriate usage of bitwise exclusive or module must be avoided.
3. GPS information to resist against spoofing attack: The data provided by the body sensor networks should have privacy as it contains sensitive health related data and should have secure functionalities and GPS information is required.
4. Resistance to man in the middle attack: Man-in-the-middle attack can lead to spoofing, improper data and various other problems. An efficient solution for this attack is to embed the identities of all communicating entities into the protocol message for entity authentication. For instance, H(IDi||IDi+1||...) is a possible form of protocol message which can be utilized to perform entity authentication and simultaneously conquer man-in the-middle attacks.

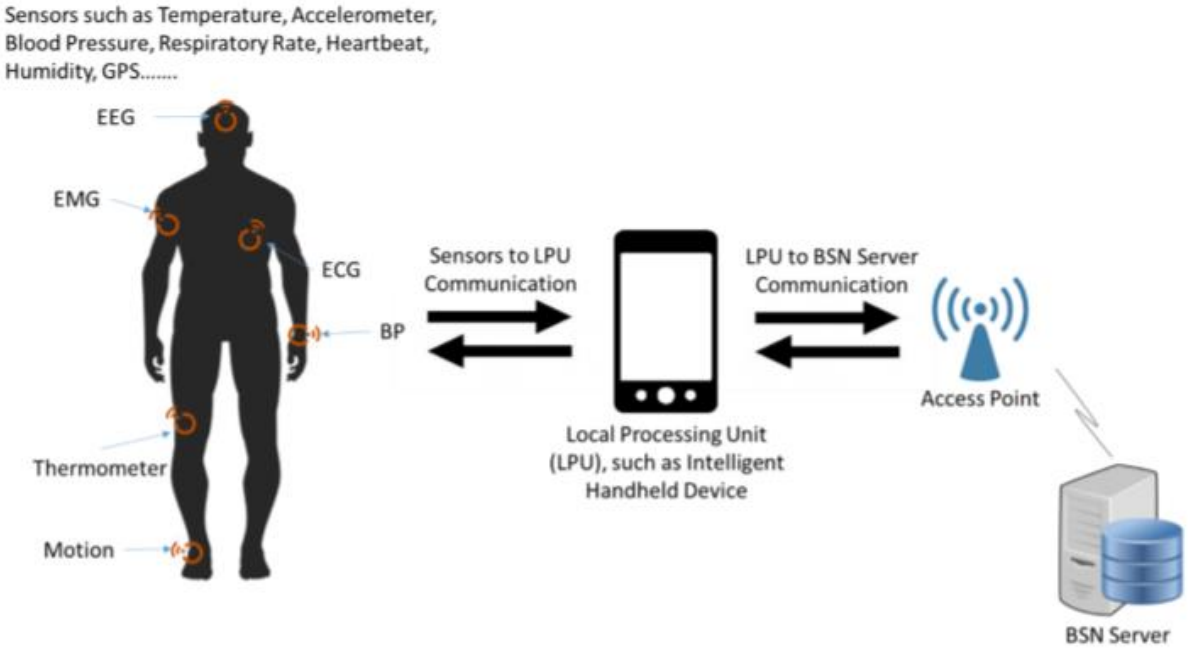



**Figure 15: Underlying IOT based communication architecture of our proposed healthcare system**

The authentication phase among wearable sensors and the processing unit and server: In the authorization scheme, a secret is shared between the server and the wearable and set of unlink-able shadow identities generated by the server are installed into the wearable at the time of system initialization. A sequence number is created to speed up the authentication process and to prevent replay attacks. The sequence number must match every time data is sent or received from the wearable else the server will reject the data and disconnect the connection.

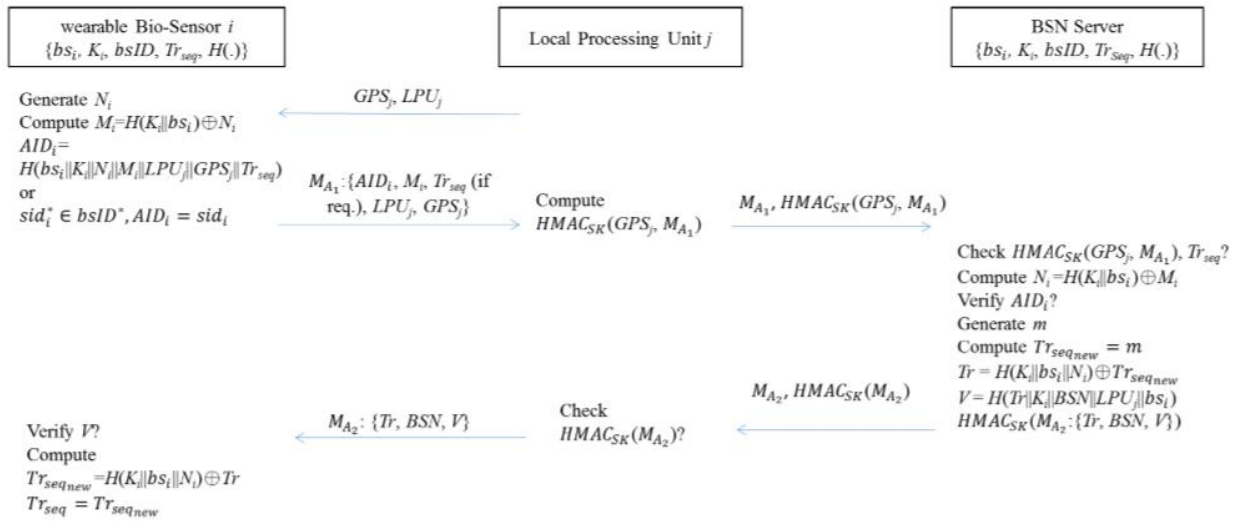



**Figure 16: Authentication phase between local processing unit and BSN server**

The local processing unit sends its identity and GPS information to wearable as an authentication request. The wearable generates a random number and calculates multiple required numbers using hash and

exclusive or operations and sends an authentication request to local processing unit. It then sends the authentication request to the server using HMAC. The server then checks if it is a valid authentication request using the tracing sequence number. If the sequence number is present in its backend, then it is considered a valid authentication else if the server cannot find the number, then it checks for the freshness and validity of the it. If it does not satisfy, then it will ask the wearable to try again with another valid identity. If it satisfies one of the condition, the server will send authentication acceptance to the local processing unit as response message. The local processing unit will then check for the correctness and if it is then updates the sequence number for next authentication session.

#### *4.1.2.2.5.4 Security challenges*

Traditional security protection mechanisms might not be suitable for smart objects (Example: firewalls containing network management control protocols can manage high traffic through internet but is not suitable for smart devices in IOT as they usually possess a specific, defined mission with limited resources to accomplish it.)
During their analysis, four unresolved issues were identified:
1) maximizing the use of available network resources;
2) route management optimization;
3) inter-device based cooperation for load balancing; and
4) security properties such as privacy, authentication, integrity and resistance to new types of attack.

### 4.1.2.2.6 Security issues of wireless sensor networks for healthcare applications [19].

#### *4.1.2.2.6.1 Security Topics*

Security issues in wireless sensor networks

#### *4.1.2.2.6.2 Security issue*

Key management schemes, Denial of service, Routing attacks

#### *4.1.2.2.6.3 Proposed Solution*

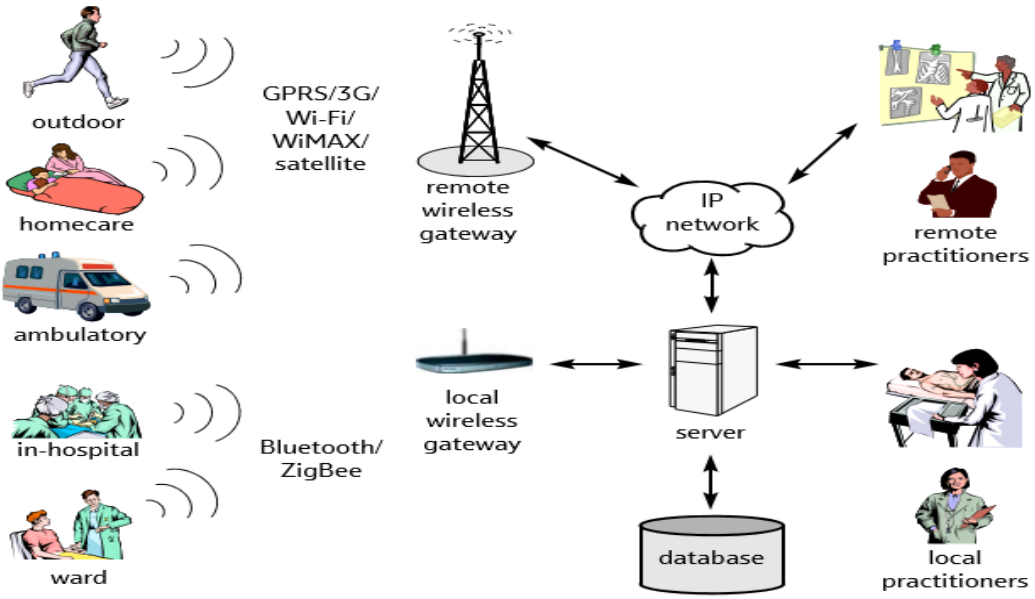



**Figure 17: System architecture of wireless sensor networks in healthcare applications**

Four types of key management scheme have been evaluated on their suitability for various sensor networks — trusted server schemes, public key infrastructure (PKI), key pre-distribution, and autonomous key setup. Trusted server schemes and PKI are well-suited to hierarchical networks in the presence of resourceful gateways, while key pre-distribution and autonomous key set-up are designed for large distributed sensor networks. Elliptic curve cryptography is used for key establishment for sensor nodes.

In the key pre-distribution for distributed sensor networks, three approaches have been studied for efficient distribution to sensor nodes prior to deployment:
• probabilistic distribution will distribute the keys selected randomly by a key pool,
• deterministic processes improve the key-pool and keychains design to provide better key connectivity,
• hybrid mechanism utilizes both probabilistic and deterministic approaches to achieve higher scalability and resiliency.

For the large-scale distributed sensor network, an efficient dynamic key distribution scheme, which could adapt to varying mobility levels, is needed for the healthcare applications. Such a scheme should have minimum dependency on trusted servers, resistance against node capture, support re-keying, and consume minimum storage, computation, and communications resources.
High-level security services should be used as they include secure group communication, intrusion detection and secure data aggregation which are in the form of proactive security mechanisms.

| | Security threats | Security requirement | Possible security solutions |
|---|---|---|---|
| 1 | Unauthenticated or unauthorised access | Key establishment and trust setup | • Random key distribution<br>• Public key cryptography |
| 2 | Message disclosure | Confidentiality and privacy | • Link/network layer encryption<br>• Access control |
| 3 | Message modification | Integrity and authenticity | • Keyed secure hash function<br>• Digital signature |
| 4 | Denial-of-service (DoS) | Availability | • Intrusion detection<br>• Redundancy |
| 5 | Node capture and compromised node | Resilience to node compromise | • Inconsistency detection and node revocation<br>• Tamper-proofing |
| 6 | Routing attacks | Secure routing | • Secure routing protocols |
| 7 | Intrusion and high-level security attacks | Secure group management, intrusion detection, secure data aggegation | • Secure group communication<br>• Intrusion detection |

**Table 2: Wireless sensor networks security threats, requirements and possible solution**

#### *4.1.2.2.6.4 Security challenges*

Resource constrained sensor nodes, uncontrollable environment, and large dynamic network topology. the security architecture demands these to be very lightweight with a reasonable execution time. The environment in which sensors will work are uncontrollable and not trustworthy. Eavesdropping.

## 4.1.3 Application Layer

### 4.1.3.1 Vulnerabilities that makes IoT applications insecure [5]

- **Design Vulnerabilities**
    - **Backdoor Access -** Attackers exploit the loopholes in the application which allows them to bypass the security mechanisms thereby making an unauthorized access which can compromise the patient data.

    - **Authorization Mechanism -** Applications are not secured using multi-layer security which makes them prone to attackers hacking into the application by just simple password break methodologies.
    - **Access to configuration -** Protocols like TFTP protocol are extensively used for booting of diskless workstations and network device management, but does not require any sort of username or password authentication to use its file access ability, giving an intruder possible access to configuration and access information easily, apart from guessing the filenames.
    - **Unsecured data exchange between application and cloud -** Lack of encryption on the data that is being exchanged between the application, cloud and devices using protocols like HTTP, REST etc.
- **Development Vulnerabilities**
    - **Data Handling -** Attackers takes the benefit of poorly handled inputs, unhandled inputs, exceptions, and interleaving of events to break into the application.
    - **Crash due to buffer overflows -** This is the most common type of attack where attacker constantly tries to modify the program's stack which eventually results in abrupt application crash and data loss.
    - **Data overwrite through buffer overflows -** Attackers use this technique by guessing the correct buffer values to overwrite the patient data.
- **Deployment Vulnerabilities**
    - **Server hacking by giving application more privilege -** Attackers use this technique to take the advantage of application granted privilege to hack into the main server from where the application is hosted and can harm the overall system by variating data, disturbing the business and core logics.
    - **Application tampering by installing it on a faulty privileged system -** If local system is having faulty privileges and faulty policies, attackers can use these systems to hack in the application disturbing the local application processing logics.

Health data is considered as top confidential data which makes it important to secure them. Data files can be misused as they contain patient data, patient payment information, patient insurance details. Additionally, they may contain records of high level officials which can be used to harm or kill them.

#### 4.1.3.2 Current Research in Application Layer

##### 4.1.3.2.1 Application Layer Security Issues and Its Solutions [3].

###### *4.1.3.2.1.1 Security Topics*

Application Design Security, Hardware Security, Application Configuration Security.

###### *4.1.3.2.1.2 Security Issues*

Design Vulnerabilities, Development Vulnerabilities, Deployment Vulnerabilities.

###### *4.1.3.2.1.3 Proposed Solution*

**Addressed - Design Vulnerabilities, Development Vulnerabilities**

- The proposed solution addresses design and deployment vulnerabilities.
- Best way to protect application from these attacks relate to strong design principles in application design and implementation phase.
- Applications should make use of the secure facilities available to them in the lower network layers, carefully check received and sent data, pessimist approach of the application like

assumption of communication is prone to attack, necessitating the use of strong authentication and encryption to validate and shield data as it moves across the network.

- Applications should also devise their own security controls, allowing for fine-grained control of privilege to access resources and data, in an ideal world using a mechanism that is candid and strikes a balance between usability and effectiveness.
- Exhaustive logging and audit capability should be a standard feature of any application that handles sensitive or valuable data.
- Testing and assessment is also critical as a control for the application layer. Given the wide variation of both problems and solutions, standard practices will not be able to capture all possible twists and turns in the application environment.
- Developers will often have inconsistent drives and schemas regarding their applications, and in a structured programming environment, mandated code security review and application security testing are critical parts of a secure Software Development Life Cycle.
- User input is a risk to security aspects of the application, so a need to filter the inputs is necessary in each application to avoid exploitation.

**Configuration Exploitation**

- Emphasize hardware security. Intrusion Detection Systems (IDS) can witness data traffic for identified profiles of network activity that can indicate probes for susceptible applications or an imminent or ongoing attack, as well as spotting the presence of undesirable application traffic.
- Many existing host-based firewall systems also contain the means to control the access of applications to the network. This control is useful in avoiding the unauthorized or concealed use of network resources by local programs, as well as providing the conventional layer three and four control functions of a firewall. Many also include basic IDS functionality as well.

**Data Handling, Access to Configuration, Server Hacking, Application Tampering**

Authentication, Authorization, and Accounting (AAA) protocols like TACACS [TACACS] and RADIUS [RADIUS] were initially deployed to provide dial-up PPP [PPP] and terminal server access. Over time, with the growth of the Internet and the introduction of new access technologies, including wireless, DSL, Mobile IP and Ethernet, routers, and network access servers (NAS) have increased in complexity and density, putting new demands on AAA protocols. RADIUS provides the following advantages.

- **Tight security:** RADIUS allows user information to be stored on one host, minimizing the risk of security loopholes.
- **Flexibility:** Using modifiable "stubs," RADIUS can be adapted to work with existing security systems and protocols.
- **RADIUS:** Server may be adapted to your network, rather than adjusting your network to work with RADIUS.
- **Simplified management:** Security information is stored in text files at a central location, the RADIUS server. Adding new users to the database or modifying existing user information can be easily accomplished by editing these text files.
- **Extensive logging capabilities:** RADIUS provides extensive audit trail capabilities, referred to as RADIUS accounting. Information collected in a log file can be analyzed for security purposes, or used for billing. Security aspect is better handled in RADIUS version 2.0 which provides SecurID. The SecurID authentication is based on Security Dynamics' token technology, which authenticates users using a patented time-synchronization method. The RADIUS 2.0 server can forward some or all authentication requests to a SecurID ACE/Server running on the same host as the RADIUS server.

**Design Vulnerabilities, Development Vulnerabilities, Deployment Vulnerabilities**

- Data delivered is in the form of Attribute-Value Pair(AVP).
- Most AVPs are used for delivering data associated with applications that employ Diameter while the protocol uses few itself.

- AVPs may be added arbitrarily to Diameter messages, so long as the required AVPs are included and AVPs that are explicitly excluded are not included. A security association which is an association between two endpoints in a Diameter session is used for security. It allows the endpoints to communicate with integrity and confidentially, even in the presence of relays and/or proxies.
- Protocol provides End-to-End Security Framework. End-to-end security services include confidentiality and message origin authentication. These services are provided by supporting AVP integrity and confidentiality between two peers, communicating through agents.
- End-to-end security is provided via the End-to-End security extension, described in [AAACMS]. The circumstances requiring the use of end-to-end security are determined by policy on each of the peers.
- Security policies, which are not the subject of standardization, may be applied by next hop Diameter peer or by destination realm. For example, where TLS or IPsec transmission-level security is sufficient, there may be no need for end-to-end security. Diameter requires transmission level security to be used on each connection (TLS or IPsec). Therefore, each connection is authenticated, replay and integrity protected and confidential on a per-packet basis.
- Additionally, authenticating each connection as well as the entire session must also be authorized. Before initiating a connection, a Diameter Peer MUST check that its peers are authorized to act in their roles. For example, a Diameter peer may be authentic, but that does not mean that it is authorized to act as a Diameter Server advertising a set of Diameter applications.

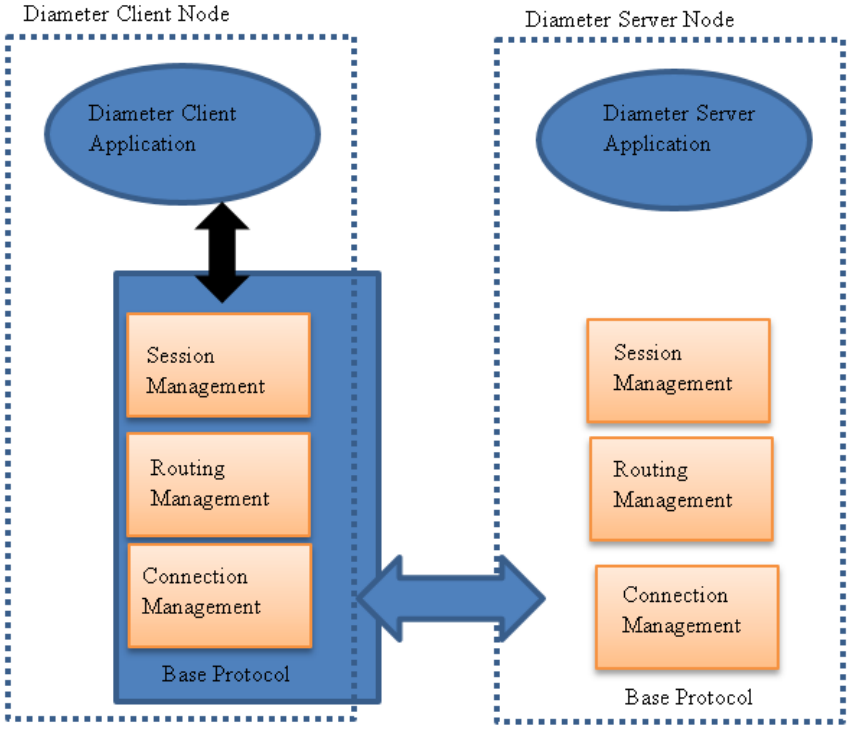



**Figure 18: Diameter Protocol**

#### *4.1.3.2.1.4 Security Challenges*

- Applying good security through the underlying layers (1 and 2 layer), with physical isolation (layer 1), private VLANs (layer two), and firewalls with tight packet filter policies (layers 2 and 3) would seem good but then it would lead to deficiency on the application layer security (layer seven, and often layers six and five), using unpatched server software and poorly written

application and script code. Since the vulnerabilities lie within the application, in a pure seven-layer model it would be an issue to defend against this at the lower levels.

- Some applications may insecurely handle sensitive information by placing it in publicly accessible files or encoding it in "hidden" areas which are trivially displayed, such as in the HTML code of a web form.

#### 4.1.3.2.2 A medical health care system for privacy protection based on IoT [4].

##### *4.1.3.2.2.1 Security Topics*

Data Encryption at Application Layer.

##### *4.1.3.2.2.2 Security Issues*

Unsecured data exchange between application, cloud, and devices.

##### *4.1.3.2.2.3 Proposed Solution*

Two approaches suggested

**Approach 1 - Homomorphic Encryption**

**Use Case -** If a patient needs to measure several physiological data with an expectation of data being invisible to any other entity (Intruder, unprivileged persons or any random patient) on the network.

Based on the above background and requirement, a new homomorphic algorithm for data encryption method during data exchange is suggested which works in a four-way handshake method described as follows.

- **Step 1** Patient inquires data items which is collected encrypted in a matrix which is later transported to the server.
- **Step 2** Maximum and minimum value of each attribute in the data would be stored and difference would be calculated.
- **Step 3** Upon the medial result, matrix from step1 reaches the server, it is right multiplied with the matrix constructed in step 2 and reverted to the patient who inquired.
- **Step 4** As soon as the patient terminal receives the data from server it is decrypted using the inverted matrix.

In an insecure network environment, messages can be easily eavesdropped or tampered by attackers. With homomorphic encryption, attackers can filch transporting data in the communication channel. Attackers cannot calculate matrix, which disables them to achieve authentic data. In addition, even hacking the servers in hospitals remains useless to an attacker because servers do not store or calculate any physiological data of users.

**Approach 2 - An encryption algorithm improved from DES for WSN**

A new encryption algorithm based on the characteristic of WSN is proposed. The algorithm has the advantages of simple implementation, lightweight calculation, and small scale codes.

- **Operations involved in this algorithm**
  - **XOR Operation**
    Repeated XOR operations are used to encrypt. The most important function of repeated XOR operation is to cause an avalanche effect when encrypting the message.
  - **ROL operation**
    Bitwise rotation again for encryption.
  - **Hash operation**

Hash operation aims at messages of fixed-length or flexible-length. Both generate a message digest of 32 bits.

- **Table Initialization**
  The sub key table and the prime table are initialized. The main key has a length of 64 bits.
- **Multiple Encryptions**
  Plain text of 32 bits is subjected to 8 rounds of encryption operations. Finally, the data is encrypted.
- **Encryption algorithm on arbitrary planes of different lengths**
  - Length of the plaintext is recorded las len, and several "0" s are appended to the plaintext in order to make the length up to multiple of 4. 4 bytes of len is added in front of the plaintext.
  - Plaintext with blocks of 32-bit (4 bytes) is encrypted.
  - CBC encryption mode is an option to increase chaos and avoid the same cipher block from the same plain block. The initialization vector is defined as hash(key).

#### *4.1.3.2.2.4 Security Challenges*

- Some problems remain unsolved such as no secure key management.
- Insecure router protocols among plenty of sensor nodes.

### 4.1.3.2.3 Hybrid Security Techniques for Internet of Things Healthcare Applications [7].

#### *4.1.3.2.3.1 Security Topic*

Data encryption over communication

#### *4.1.3.2.3.2 Security Issue*

Data compromise during transmission

#### *4.1.3.2.3.3 Proposed Solution*

Hybrid Cryptography

- Applications need to communicate with each other using standard security techniques for the protection and immunization of databases in IoT.
- Technique involves the following
  - Uses multiple ciphers of different types together to take benefit of the strengths of each type of cryptography.
  - One common approach is to generate a random secret key for a symmetric cipher, and then encrypt this key via an asymmetric cipher using the recipient's public key.
  - The recipient decrypts the secret key first and then uses that key to decrypt the message.
  - Most of the systems use cryptography because it offers various algorithms and it is almost impossible to break because of its complexity.

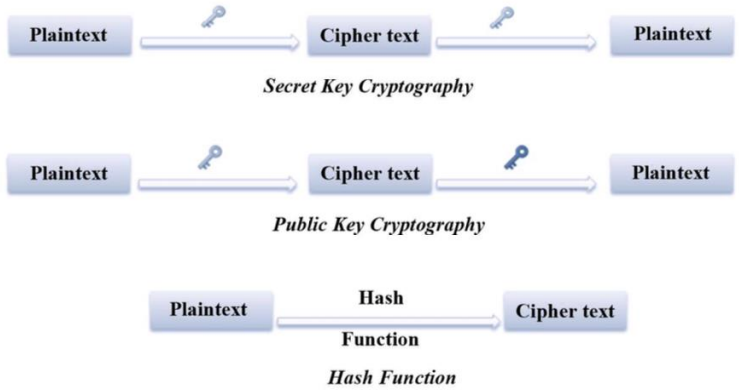



**Figure 19: Cryptographic methods**

- Three types of cryptography
    - **Secret Key Cryptography -** This technique uses the same key for both encryption and decryption.
    - **Public Key Cryptography -** This technique employs a pair of keys. One to encrypt the message and the other to decrypt the message. The advantage of this method is that the public key can be advertised by the owner to anyone who wants it.
    - **Hash Functions -** A hash function creates a fixed size blocks of data by using entry data with variable length. If the data is modified in any way, then the hash function generated will be different. This kind of security measure ensures that the information is transmitted and received exactly the way it was supposed to be. The most common hash algorithms used today are Message Digest (MD) and Secure Hash Algorithm(SHA).
- Hybrid technique has combined benefits and reduce their weakness as much as possible by taking of advantage of one over the other. This can be described briefly as follows
    - The original message's message digest is digitally signed (the digital signature uses RSA algorithm).
    - Symmetric cipher is used to code the original message. The secret key is obtained using a key generator and it is changed periodically.
    - The private key used for symmetric cipher is also coded using RSA algorithm, but with different keys.
    - The coded private key is attached to the encrypted message together with the digital signature.
- Hybrid technique can be applied to the several healthcare applications
    - Remote Monitoring - Can be used to securely capture patient health data from sensors, apply complex algorithms to analyze the data and then send it to several professionals who can make appropriate health recommendations.
    - Physical Activity Monitoring for Aging People - Body sensor networks (BSN) measure vital signs of a patient like the heartbeat, blood pressure, temperature and movements.
    - Chronic Disease Management: - Patients with pulmonary heart diseases and diabetes can be remotely monitored with comprehensive patient statistics.

#### *4.1.3.2.3.4 Security Challenges*

- Publishing new technologies in healthcare applications without considering security makes patient privacy vulnerable; the physiological data of an individual are highly sensitive.
- Extensive use of multiple complex cryptographic functions makes implementation cumbersome and often requires lot of time to establish the architecture.

- The personnel involved in setting the architecture for a healthcare system are expected to have a working knowledge of all cryptographic algorithms. This raises the issue of requiring extensive financial assistance to implement the architecture.

#### 4.1.3.2.4 A virtual PHR (Personal Health Record) authorization system [6].

##### *4.1.3.2.4.1 Security Topic*

Policies and authorization to access patient information

##### *4.1.3.2.4.2 Security Issues*

Secure storage of patient information, maintaining the agile solution for extended periods of time.

##### *4.1.3.2.4.3 Proposed Solution*

IoT by and large alludes the system of heterogeneous hubs from compelled gadgets, for example, little sensors which fundamentally concentrate on single undertaking (e.g. checking) to relatively unconstrained gadgets like cell phones and tablets. Contrasted with conventional system hubs, asset compelled hubs have difficulties to give a consistent correspondence to other hubs of bounty assets.

A virtual PHR (Personal Health Record) system is an entity on the network that consists of

- A non-healthcare component containing health and social information collected by the patient or non-healthcare providers. (Ex. family members, social care providers)
- A medical device component containing health information transmitted from Internet connected medical devices. (Ex. home care systems)
- A healthcare professional component containing information stored into various healthcare information systems. (Ex. primary care and electronic medical records)

The research paper discusses a cloud-based PHR system which has a stringent need of preserving the security and privacy of integrated patient data. The authorization model combines two paradigms

- RBAC - Role based access control
- ABAC - Architecture based access control and thus it forms the RABAC model.

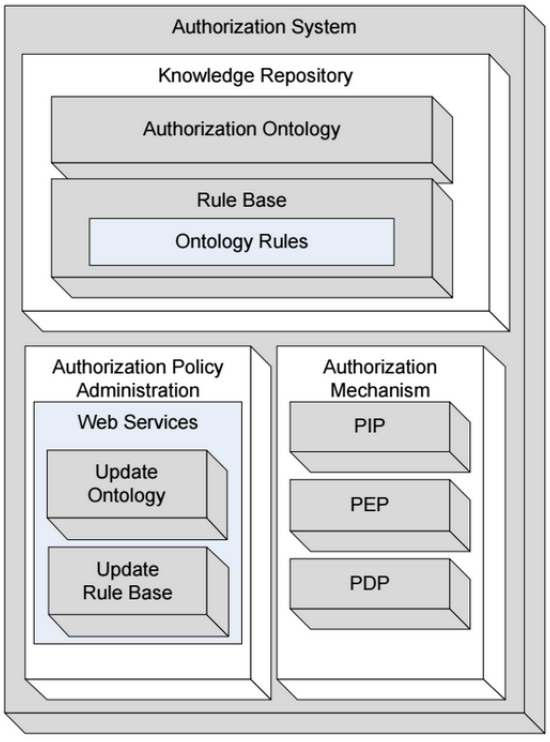



**Figure 20: PHR Authorization System**

**RABAC model**

The RABAC model allows roles to be dynamically assigned to users during each session based on their attributes. Permission filtering policies are used to constrain the available set of permissions associated with the roles activated in each session. Such a type of model eases the role explosion problem as a user can have different roles in different sessions (which subject, in terms of role, can have what access to what objects and under what conditions).

**Architecture**

The figure (20) shows the abstract structure of the virtual PHR authorization system and it consists of 3 major components:

- The knowledge repository
- The authorization policy administration
- The authorization mechanism
  The knowledge repository hosts an authorization ontology and a base rule. It basically defines the relationships between the subjects, the environment, and the related attributes. It automatically infers authorization decisions based on the RABAC model and applies the permissions as well.

The authorization policy administration module uses web services to update the knowledge repository, i.e. it updates the ontology and the rule base.

The authorization mechanism consists of 3 parts.

- **PIP** (Policy information point): receives the subject and environment attribute to create subject-to-role rules and activates roles for the subject.
- **PEP** (Policy Enforcement Point): When the subject requests for data access, PEP creates an authorization request that includes the subject and the roles.
- **PDP** (Policy Decision Point): On receiving the request from PEP, it combines the information on authorization request with ontology information which determines the patient data allowed for the subject. It then decides whether the access should be permitted or denied.

#### *4.1.3.2.4.4 Security Challenges*

1. In this cloud-based virtual PHR environment, the system is implemented as a service which assumes that healthcare systems are laced with interacting services such that it is possible to determine on the fly which information needs to be extracted. The subject, object and environment authorization roles should be recorded and created through an administration module.
2. One of the primary concerns of PHR is that all potential subjects are not known in advance and role definitions are neither complete nor uniform. There cannot be a definite set of subject-to-role assignments.

### 4.1.3.2.5 BSNCare: A Secure IoT-Based Modern Healthcare System Using Body Sensor Network [15].

#### *4.1.3.2.5.1 Security Topic*

Hardware and application layer Security

#### *4.1.3.2.5.2 Security Issues*

Securely feeding BSN data to the database, Resistance to replay and forgery attacks

#### *4.1.3.2.5.3 Proposed Solution*

By and large, BSN comprises of in-body and on-body sensor systems. An in-body sensor arrange permits correspondence between intrusive/embedded gadgets and base station. Then again, an on-body sensor arrange permits correspondence between non-obtrusive/wearable gadgets and an organizer.

Proposed BSN care is a BSN engineering made of wearable and implantable sensors. The possibility of BSN is demonstrated as follows.

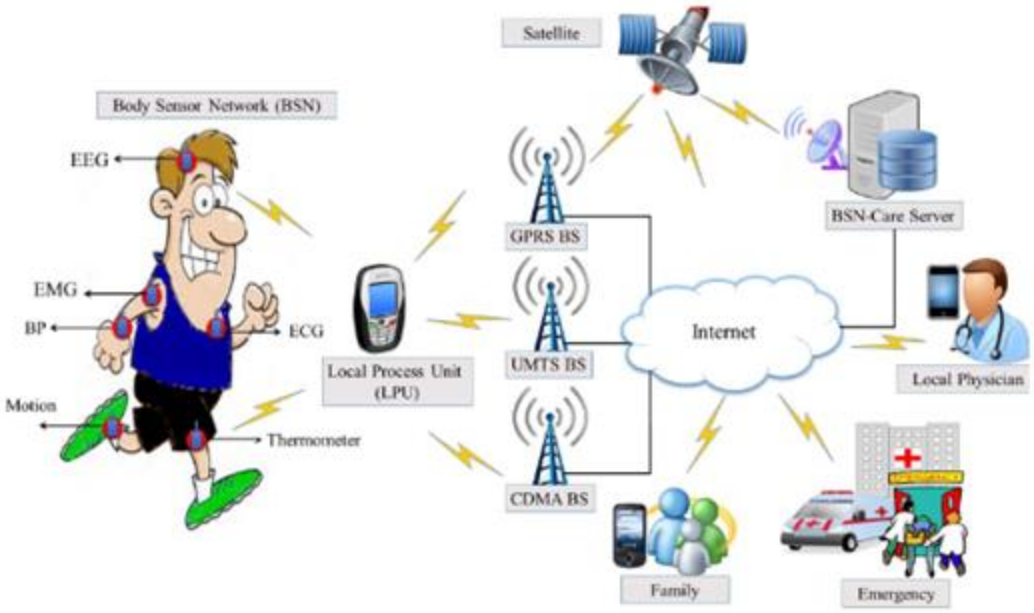



**Figure 21: Secure IoT-based modern healthcare system using BSN**

Here LPU (local process Unit), is the application which is a process initiator. LPU sends periodic updates to BSN-care server and the server needs to confirm identity of LPU to avoid security breach.
The paper suggests 2 mechanisms to address all the security concerns.

**1. Lightweight Anonymous Authentication Protocol.**

There are 2 phases in this protocol

- BSN-Care server issues security qualifications to a LPU through secure channel, this stage is called enlistment stage.
- Before Data transmission from the LPU to BSN-Care server, both the LPU and the server will confirm each other

The mechanism for the protocol is depicted in the image below

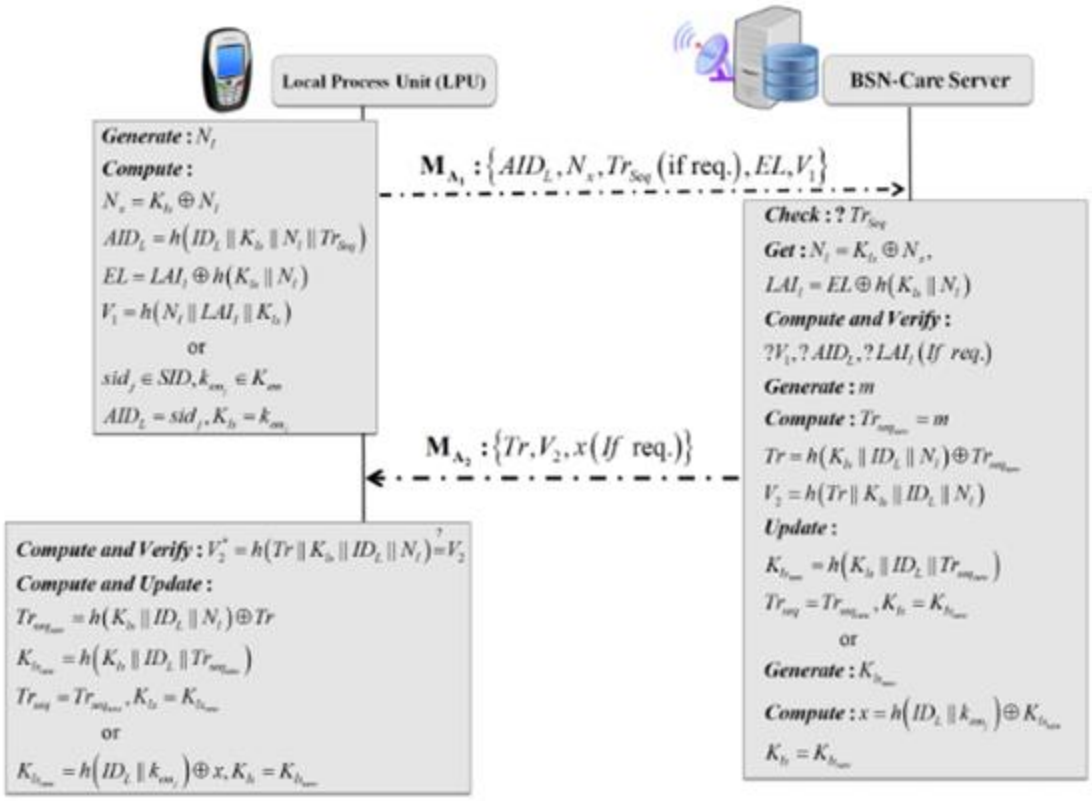



**Figure 22: Lightweight anonymous authentication protocol**

This two way authentication achieves

1. Mutual authentication
2. Anonymity property of the application
3. Secure localization
4. Defeats forgery attacks
5. Reduction in computational overhead

**2. Data Security in BSN care application**

This mechanism addresses questions such as

- How protected and reliable are these clinical gadgets that are worn or embedded?
- How we can guarantee that BSN-Care server got the unaltered information from LPU?
- How do we make sure data security in body sensor network?

For instance, a bio sensor sending ECG flag of a patient is errored or adjusted with the end goal that wrong analysis and treatment are endorsed which may cause death. The approach used here is offset Codebook (OCB). OCB is a block cipher mode of operation that features authenticated encryption.

#### *4.1.3.2.5.4 Security Challenges*

- The need for mutual authentication between the LPU and the BSN-care unit requires extra effort.
- The usage of (shadowID, emergency key) pair in each round may cause excessive storage cost in both the LPU and BSN-Care server. This is to ensure anonymity.

- Lack of smart tracking approach may allow an attacker to send the incorrect location by using false signals. This is a localization challenge.

#### 4.1.3.2.6 A Back-end Offload Architecture for Security of Resource-constrained Networks [14].

##### *4.1.3.2.6.1 Security Topic*

Hardware architecture for application

##### *4.1.3.2.6.2 Security Issues*

Heavy processing load on IoT devices for security.

##### *4.1.3.2.6.3 Proposed Solution*

IoT by and large alludes the system of heterogeneous hubs from compelled gadgets, for example, little sensors which fundamentally concentrate on single undertaking (e.g. checking) to relatively unconstrained gadgets like cell phones and tablets. Contrasted with conventional system hubs, asset compelled hubs have difficulties to give a consistent correspondence other to hubs of bounty assets.
The paper proposes that the architecture to handle security concerns should be offloaded from devices and a backend architecture can be designed to handle those concerns.
**Proposed architecture**

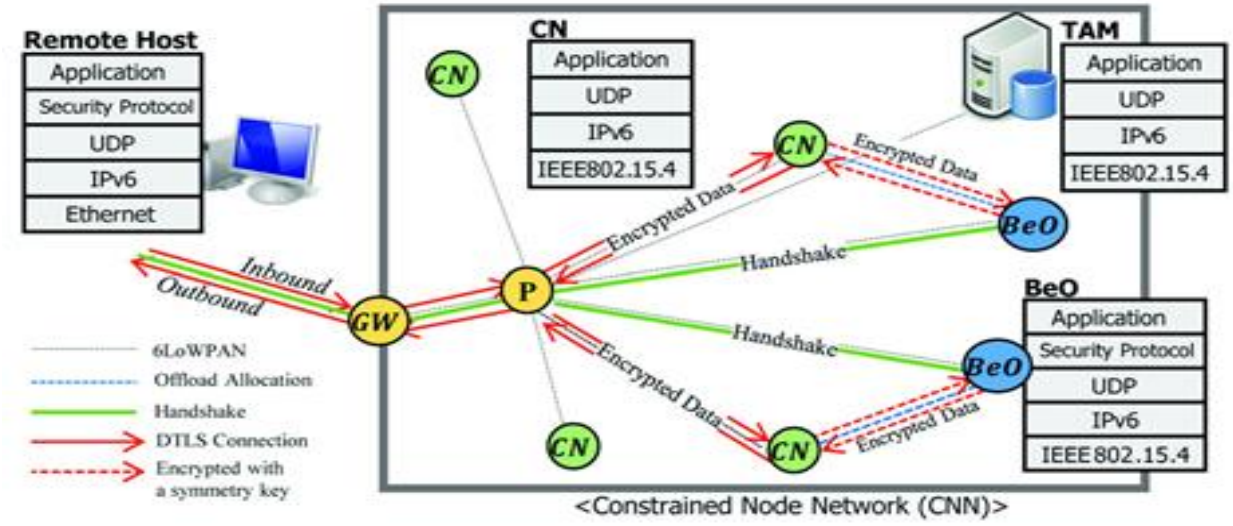



**Figure 23: Back-end offload Architecture for Security.**

The proposed architecture provides datagram transport layer security to applications by back end offloading, that way the application can pretend to be a powerful host with a security protocol without the actual security measures implemented in it. To manage Backend Offloader (BeO), Trust association manager (TAM) is introduced.
When an application(CN) needs security, it joins a network and it automatically registers itself on TAM, then TAM enrolls node id to a list of already joined CNs, for this procedure, it is required that they share a master key to maintain secure communication. Using this key, the packets from CN are offloaded to BeO in secure manner and are provided protected information from a remote endpoint.

BeO supported cipher suites are followed by CNs, thus high level authentication such as public key (PKI) can be employed without CN having to do any processing and the Endpoint authentication is achieved.
The TAM component in proposed architecture plays a vital role of load balancing off loaders, the algorithm that the paper suggests is as follows.

**Algorithm 1** The Load Balancing of BeOs

**procedure** BALANCER($numBeO, \alpha, \beta$)
  **for** every BeOs $k$ **do**
    $load_{BeO_k} \leftarrow \frac{\sum_{i=1}^{numCN} \gamma_i h_i \times load_i}{capacity_{BeO_k}}$
  **end for**
  $load_{avg} \leftarrow \frac{\sum_{k=1}^{numBeO} load_k}{numBeO}$
  **for** every BeOs $k$ **do**
    **if** $load_{BeO_k} \leq \alpha \times load_{avg}$ **then**
      $flag_k \leftarrow 0$ ▷ *idle*
    **else if** $load_{BeO_k} \geq \beta \times load_{avg}$ **then**
      $flag_k \leftarrow$ -1 ▷ *overload*
    **else**
      $flag_k \leftarrow 1$ ▷ *normal*
    **end if**
  **end for**
**end procedure**

**Figure 24: Load Balancing Algorithm**

The proposed architecture also takes care of the session management. To manage multiple connections from several CNs, BeO maintains list of connected CNs and their sessions. The information is used in offloading till the session reaches its completion. There could be scenarios where there are harmful sessions with end-points. If such endpoint is malicious, BeO will stop offloading and it will instruct a CN to drop packets from the host. The CN will blacklist such malicious hosts and will not accept any future connection from those hosts in future.

#### *4.1.3.2.6.4 Security Challenges*

The paper makes few assumptions, if the assumptions get challenged somehow the proposed solution gets compromised. Following are the possible consequences.

- BeO is secure. If the BeO is compromised the integrity of the architecture will be compromised and ultimately it can compromise CNs as well which makes the whole system insecure.
- TAM is secure. If TAM is compromised CNs can't be secure enough as TAM provides proper security assist, which ultimately jeopardizes integrity of proposed architecture.
- End points are assumed to be secure. The end points must be protected and they should be managed by operator working remotely on regular basis.

## 4.1.4 Findings and Analysis

### 4.1.4.1 Network Layer

#### 4.1.4.1.1 eHealth and IoT Security

It is often difficult to come to a consensus on the definition of eHealth and therefore we follow the definition given by the World Health Organization [WHO]: "E-health is the transfer of health resources and health care by electronic means. It encompasses three main areas:
The delivery of health information, for health professionals and health consumers, through the Internet and telecommunications.

This area of eHealth has proven to be a positive revolution in improving public healthcare. A simple example of a patient collecting his blood samples to measure his blood sugar levels suffices to quantify the claim. If the patient can collect his/her blood samples at home, under normal conditions, the readings would certainly be more accurate as opposed to when it is collected at a hospital.

The research paper has focused on how this area of eHealth can be integrated with IoT to effectively contribute to the healthcare industry. The major area of interest throughout the paper is to suggest an architecture that addresses the security concerns prevalent in the IoT healthcare architecture. The areas addressed in the paper are as follows:

1) Interoperable ecosystem of different types of devices, applications, and backend systems to enable the free flow information for precise and timely decision-making.
2) The data flow architecture suggested in the research paper is based on three important factors:
    - Source of data - typically from sensors (either locally cached or sent to upstream systems)
    - Path of data - includes a gateway and intermediate hubs
    - Destination of data - enters a data store in the cloud where it is stored and processed.

The e-health network security architecture involves multiple layers of prevention, detection and response controls as the network spans through different types of networks. These include wireless, wired, enterprise, private and public networks.

- The mobile security reference architecture calls out that the devices that use Wi-Fi and cellular network communications are more accessible and exposed than hardwired devices. The wireless network architecture must consider the protection from various network based threats such as data interception over air, data interception over the network, manipulation of data in transit, connection to untrusted service, jamming and flooding.
- The architecture must enable the tuning of quality of service, which can vary based on the devices and the functionality that is used. For example, a pulse oximeter generates text data, which is largely transparent to the delays in the network. In contrast stethoscope audio streaming can be extremely sensitive to network delay.

#### 4.1.4.1.2 Robust Authentication of sensors and physical devices in IoT

Physical gadgets in IoT are from various sellers and need standard organizations, hampering in consistent reconciliation. In wearable gadgets, a few issues identified with security and protection of client's information come up as how does the gateway (advanced smart phone) authenticate these sensors? How these sensors are matched with gateway? How to adjust the client's protection and ease of use?
To analyze the findings of Authentication in the Network Layer, let's consider the connected healthcare IoT architecture represented below:

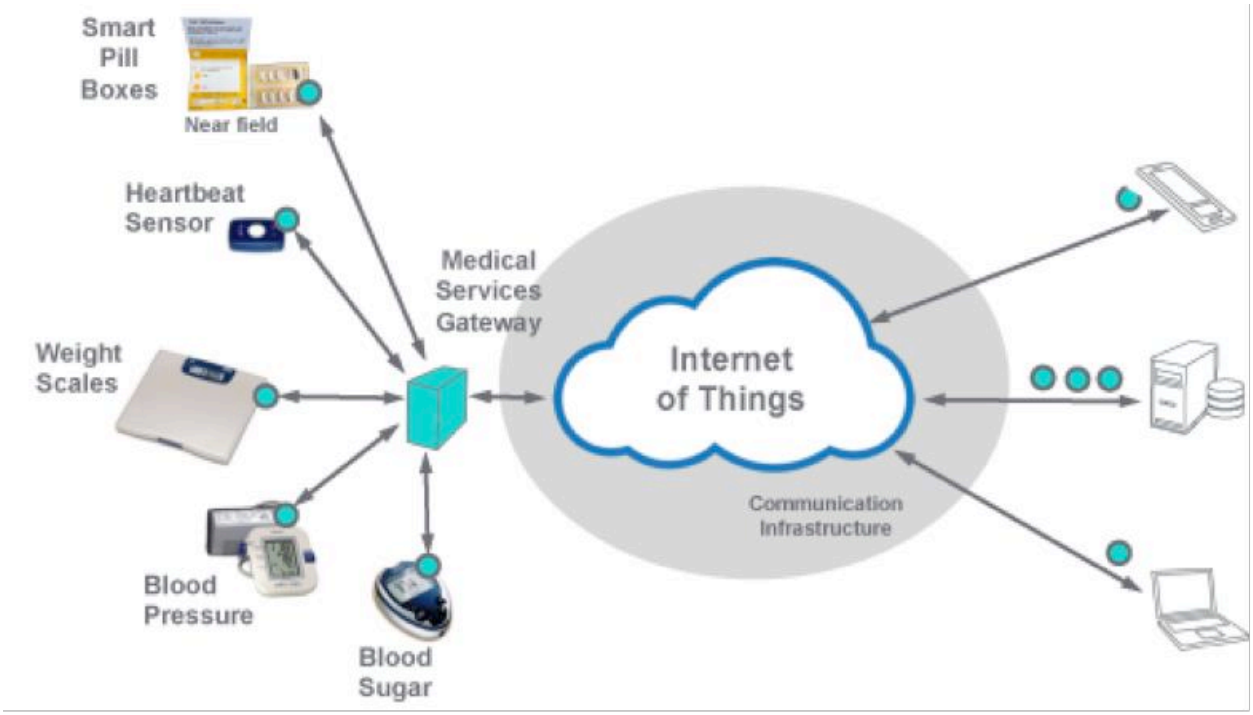



**Figure 25: Connected healthcare IoT architecture**

When sending health data, the various medical devices on the left should authenticate to the local gateway, followed by the gateway authenticating the cloud endpoint. The applications on the right that will analyze and render this health data must also authenticate to the cloud when requesting the data. The only scalable model for all the above authentications is through security tokens. Here, one actor authenticates to another by including a previously obtained token on its messages. The token serves to identify the first actor, enabling the second actor to make an appropriate authorization decision.

For health data, it is important that the clients have control of how their health data is gathered & examined. A capable instrument to empower this kind of control is to require that the client be effectively required all the while, where the distinctive actors above are issued the security tokens utilized for ensuing associations. Without the client's assent, no tokens are issued and no validated communications happen. OAuth 2.0 and OpenID Connect 1.0 are two institutionalized structures for verification and approval that unequivocally bolster the above model. One test is that OAuth and Connect have just been bound to HTTP up until this point.

Just HTTP is insufficient for associations in the Health IoT condition. Another class of conventions guarantees to be more qualified than HTTP viz. MQ Telemetry Transport and Constrained Application Protocol.

The lightweight CoAp-based mutual authentication scheme proposed, approves the identities of the partaking gadgets before connecting with them in correspondence for the asset perception in an IoT domain by utilizing a solitary key. The scheme acquires less association overhead and gives a powerful

protection answer for battle different sorts of assaults like spying, key creation, asset depletion and disavowal of administration assaults.
Additionally, the Authentication convention proposed is a key consent to set up a safe E2E channel in view of offloading overwhelming cryptographic capacities to the confided in neighboring sensors with regards to IoT. Security investigation and execution assessments are made to demonstrate that the proposed convention is sufficiently secure and is lightweight for embedded sensor that has rare computational and vitality assets.

#### 4.1.4.1.3 Delegated Authorization and Encryption in IoT Network Security Protocols

Network protocols provide data security through encryption. But, there is a need for lightweight cryptographic algorithms as current cryptographic schemes hamper the constrained resources of edge devices. Also, key management in network security protocols is a critical to ensure secure data encryption and transmission. Challenges in current cryptographic schemes are analyzed and summarized in the following table.

| | |
|---|---|
| Heterogeneity | Multiple constrained devices with different APIs or full-fledged web servers |
| Malleable encryption algorithm | Conventional protocol allows to send the message transformed in an encrypted form by using algorithm based on key for a given authenticated session |
| Static and non-expiring public private keys | Master key used for encryption must change after a desired interval |
| Pattern analysis attacks on current encryption approaches. | A technique which generates bit-stream according to the message but is not fixed for a given character in a given authenticated session is recommended. |
| Pseudo-random techniques used to generate password, and cryptographic keys are prone to dictionary attacks | Truly random hardware techniques must be used for generating perfect random bit stream for encryption purpose. |
| Processing and transmission overheads incurred in peer-to-peer networking for authentication | Authentication with low overhead, and low usage of processor and RAM of IoT devices is required. |
| Fluctuation of link due to network topology changes due to the movement of medical devices. | Error correction code like hamming code is required. |

**Table 3: Security Challenges**

Secure End to End key establishment protocol for resource constrained healthcare sensors in context of IoT:
IoT is a network of smart devices and services which talk to each other real time. These networks are vulnerable to attacks which will risk the confidential data. Security of the devices is of utmost importance but because of the resource constrained nature traditional security measures can’t be applied. A lightweight, end-to-end key establishment protocol can be made used which will provide security capabilities like unconstrained one's. It makes use of asymmetric cryptographic methods like RSA, DSA etc. and will offload any heavy cryptographic functions to the trusted neighbors.

#### 4.1.4.1.4 A Secure Authentication Mechanism for Resource Constrained Devices:

One can make use of broadcast authentication mechanism for wireless sensor networks which are also resource constrained. This protocol is used with lightweight symmetric authentication scheme like $\mu$TESLA and LEAP based schemes. $\mu$TESLA the authentication key is kept secret for some time and then revealed after a while. Key chain mechanism is used for key distribution in this scheme. A message authentication code (MAC) is sent before sending out a message. LEAP provides security by establishing four keys: individual authentication key, group key, cluster key and pairwise key. The advance authentication mechanism aims to minimize the delay by sending the authentication key early. This mechanism is when integrated with LEAP and LEAP++ result in much lesser authentication delay.

#### 4.1.4.1.5 Secure MQTT for Internet of Things (IoT):

Device communication needs to be secure so as prevent malicious attacks. This is done by using a secure Message Queue Telemetry Transport (SMQTT) protocols which is based on Attribute Based Encryption(ABE) which is lightweight and scalable. The protocol is divided into four phases, setup, encrypt, publish and decrypt. The message is encrypted and published by making use of set of conditions which are based on access policies. This message is decrypted by the subscribers which have access policies.

### 4.1.4.2 Perception Layer

#### 4.1.4.2.1 A Secure RFID Authentication Protocol for Healthcare Environments Using Elliptic Curve Cryptosystem

The paper proposes an efficient authentication protocol. It overcomes various security issues like Key compromise problem (Liao and Hsiao proposed Elliptic curve cryptosystem). It also overcomes the tag tracking as same identity is used in different sessions. It could also withstand the replay attack, provides anonymity, availability, and forward security.
The proposed protocol and Liao et al.'s protocol have the same computational cost and communicational cost. However, Liao and Hsiao's protocol is vulnerable to the key comprise problem and impersonation attack. The proposed protocol could overcome those weaknesses. Therefore, the proposed RFID authentication protocol is more suitable for practical applications and is more applicable for healthcare applications.

#### 4.1.4.2.2 Two-phase Authentication Protocol for Wireless Sensor Networks in Distributed IoT Applications

The paper provides a design and evaluation of an authentication protocol for Wireless Sensor Networks(WSNs) in distributed IoT applications. The edge nodes and end users exploit implicit certificates for mutual authentication, the protocol is lightweight and it supports the heterogeneity of the entities. It has also implemented the scheme and has recorded performance measurements on the high resource restricted sensor nodes along with a security analysis.
The proposed authentication scheme can be easily deployed in the resource constrained devices, along with reasonably high security. Due to the small size of the certificates, it consumes less amount of memory at each sensor node. Since the protocol is based on standard ECC operations, which are supportive for all the sensor nodes irrespective of the manufacturer and can be performed at end-users, it is feasible to deploy in IoT enabled heterogeneous WSN. The proposed authentication scheme supports the new node addition, and mobility of edge devices and end-users. The limitations of the proposed scheme are that with the node certificate, public-private keys and CA's public key the attacker can communicate with a legitimate user. Resistivity for node capturing attacks was not addressed.

#### 4.1.4.2.3 Cancellation-based friendly jamming for physical layer security

Wireless networks are exposed to security challenges such as jamming or eavesdropping attacks due to its broadcasting nature. Especially, in the future internet of things environment, more severe security challenges will appear since the connectivity will be dramatically increased, due to the requirement of IoT realization.
The research paper proposed an optimal power allocation strategy aiming to improve practical physical-layer security, by employing friendly jamming with cancellation for anti-eavesdropping. Particularly, secrecy outage probability was evaluated in the case which incorporates a pair of transmitter-receiver and a passive eavesdropper near the receiver. The author derived the optimized power allocation strategy, hence the required cancellation was improved significantly. Numerical simulation and analytic calculation results showed the interrelationship between jamming power ratio and cancellation capability. Additionally, the achievable secrecy performance has been quantified by using the secrecy efficiency function. Moreover, the proposed scheme can achieve the improved secrecy rate regardless of the availability of eavesdropper channel information.

#### 4.1.4.2.4 An Efficient Authentication and Access Control Scheme for perception

Since sensor nodes have special characteristics, and limitations of the symmetric key cryptography(SKC) such as short length, relatively limited computing, and communications and storage overheads. Existing studies have showed that the authentication and access control of the symmetric cryptosystem is more suitable for the WSN. There are several studies that have proposed various models on user authentication using SKC in wireless sensor network. However, the inability to scale of SKC prompted scholars to propose authentication and access control based on public key cryptography (PKC) to overcome the limitations of SKC. However, neither SKC or PKC provide mutual authentication between nodes and user nor resist Denial of Service attack.
The research paper proposed an authentication and access control method based on attribute. This method provides simple and efficient mutual authentication between users and nodes, and has much lower overheads in storage and communication. For access control policy, it adopted Attribute-based Access Control authorization method which is more flexible and scalable. In addition, the attribute-base control authorization can support both dynamic extension of large scale users and fine-grained access control in the complex system.
Compared with other traditional cryptography, the proposed ECC method provides better performance in that it uses a smaller key size to achieve the same security. For the performance of evaluation, the paper used the computational overhead, which is the computation time required for sensor nodes, to analyze the performance, and it showed that scheme has better performance at the sensor node side.
The proposed method can defend against a wide range of attacks including man-in-the-middle attacks, eavesdropping attacks, node capture attack and replay attack, as well as mitigate Denial of Service.

#### 4.1.4.2.5 A secure IoT Based healthcare system with body sensor networks:

- The paper talks about the various drawbacks and security issues with the body sensor networks.
- It proposes two secure device authentication mechanisms for IoT based healthcare systems relying on body sensor networks.
- There were multiple unresolved issues like route optimization and security properties like authentication and integrity. There were some security requirements such as Session key being required for secure communication and traditional methods cannot be used for those.
- GPS information should be required to resist spoofing attacks and man in the middle attacks can be reduced by using the identity of communication entities.
- The paper proposes an algorithm for secure authentication phase for authorizing a sensor.

#### 4.1.4.2.6 Security issues of wireless sensor networks for healthcare application

A secure sensor network should encompass key establishment and trust set-up, confidentiality and privacy, integrity and authorization, availability, secure routing, secure group management, data aggregation. More attention has been given to robust and efficient key management schemes which serve as the fundamental requirement in encryption and authorization. Various security threats and corresponding possible security solutions are discussed in the paper.

### 4.1.4.3 Application Layer

#### 4.1.4.3.1 Securing application layer against vulnerabilities

Application layer is the top most layer that is directly responsible for interacting with the users even if the lower layers have strict security measures. The research paper focuses on the different security issues in application layer, mapping them to the different vulnerabilities and then coming up with solution.

First, there is a need to identify the areas where an application is prone to attacks i.e. finding out the vulnerabilities and then finding out ways to secure them against those vulnerabilities. The research paper draws out the security issues related to application layer then proposes the solution to address the issues.

Additionally, an important aspect is encryption of the data that is being exchanged between application, devices, and cloud. The research paper focuses on the weakness of existing data encryption algorithm and proposing new algorithms that are better in terms of performance, calculation weight.

#### 4.1.4.3.2 Security techniques in IoT applications

There can be a lot of challenges when handling the data in IoT devices and applications. This data if placed in wrong hands can be dangerous and reveal private information about the patient. Securing and at the same time transmitting this data is a challenge on its own. We have several techniques available which are generally used in modern day networks to ensure security of data but when it comes to healthcare devices we cannot afford it to be expensive. We also need to tradeoff between the memory requirements and power utilization.
The research papers focus on hybrid techniques which throws some light on how the above issues can be addressed. We can use a mixture of two techniques such that the shortcomings of one can be traded with the benefits of other.
We also need to control who can access the patient information and there needs to be authorization and protocols that define who can access what data. One of the research papers propose the concept of a virtual PHR (Personal Health Record) system. The role and architecture based access control system (RABAC) in a PHR system helps in determining which kind of role will be assigned to a subject.
Example: a subject current attribute information consisting of “cardiologist” (medical specialty), “on duty” (time) and “at hospital cardiology department” (location) will result in triggering subject-to-role assignment rule that will assign to the user the role “hospital cardiologist on duty”.

#### 4.1.4.3.3 Security requirements in IoT based healthcare system using Body Sensor Network

In the modern health care environment, the usage of IoT technologies brings convenience of physicians and patients, since technologies are applied to various medical areas (such as real-time monitoring, patient information management, and healthcare management).
Many people have different point of view when it comes to security and that is why it has been defined in many ways. Security is one of the most imperative and crucial aspects of any system. In a broader view, security is a concept like safety of the system.

In this paper, first there is discussion of the body sensor network (BSN) technology where patients are monitored using collection of tiny lightweight and powered wireless sensors nodes. It is one of the core technologies of IoT developments in health care system. If proper security concerns are not considered, the development of this new technology in healthcare applications can very well compromise the patient's privacy.
Then major security requirements and challenges are highlighted in BSN-based modern healthcare system. And then, a secure IoT-based healthcare system using BSN, called BSN-Care, which can efficiently cater to those requirements is proposed in detail.

#### 4.1.4.3.4 Backend offloading architecture to handle security concerns of applications:

Ultimately to protect application layer and consequently the entire application the paper proposes offloading security measure to a remote backend machine which will do the job of securing application using the offloader.
The offloader helps obliged gadgets back-end by dealing with the bundles of handshake method and encoded application information. The heap adjustment of offloaders and the security of offload messages are likewise given in the plan. The proposed engineering permits an amazingly compelled gadget to set up a protected session by using abnormal state validations, for example, open key framework or certificate, without the weight of sending overwhelming security modules. This exploration would be beneficial for inept hubs to bolster security and diminish cost at the same time.

# 5 CONCLUSIONS AND RECOMMENDATIONS

## 5.1 CONCLUSIONS

Based on the available research on various security verticals listed in 3.1.3, following conclusions are drawn for the critical security verticals.

1. The lightweight CoAp-based mutual authentication scheme proposed validates the identities of the participating devices before engaging them in communication for the resource observation in an IoT environment by using a single key.
    - The scheme incurs less connection overhead and provides a robust defense solution to combat various types of attacks like eavesdropping, key fabrication, resource exhaustion and denial of service attacks.
    - Also, the Authentication protocol proposed is a key agreement to establish a secure E2E channel based on offloading heavy cryptographic functions to the trusted neighboring sensors in the context of IoT. Security analysis and performance evaluations are made to prove that the proposed protocol is secure enough and is lightweight for implanted sensor that has scarce computational and energy resources.
2. With application layer being more susceptible to attacks several defense techniques have been identified, choosing the best one is questionable though but with little analysis on the features and cost of the protocols can help in determining. Moreover, if the same protocols can be updated to the existing systems at a lesser cost then that would be a recommended solution. We also need to realize the application usage before applying any protocol as it is unnecessary to add heavy protocols when the application itself is not designed to have those functionalities which are being covered by the protocol.
    - Data Encryption is necessary for every application communicating wirelessly and hence choosing the best and lightweight algorithm is a need of the moment. Because if the algorithms are heavyweight the transmission time will increase drastically which will impact the performance of application and can risk the lives of the patient as each second is critical when we talk about patient data.
3. The IoT architecture in healthcare revolves around how various healthcare applications communicate with each other over a network. This raises multiple concerns over the security of the data as it travels through the network.
    - Beginning from the genesis of the data, the data source, the data travels through various devices such as routers, hubs, and switches. These form an integral part of the IoT Network Layer architecture and the security concerns associated with these devices is often a topic of serious discussion among Information Assurance professionals.
    - The need for network layer security in IoT Healthcare has never been more severe. When a Healthcare architecture becomes a target for a DoS attack or a man-in-the-middle attack, the results are catastrophic ranging from delay in treatments of patients who are in critical conditions to ultimate death of individuals due to inefficient treatment. The Network Layer security issues addressed and solutions proposed in the project provide directions for a safe and secure transfer of pivotal patient information.

4. Strategy of securing IoT Healthcare data can be analyzed under four key steps/questions.
    - What is your “Connected” thing?
        i. There are different types of connected devices and the number and type of devices being used need to be tracked.
    - What data is it creating or using?

        i. Healthcare IoT data can be very complex and when hospitals work with this information, they need to make sure to contextually control access to the data. This means understanding user groups, location-based access, and advanced user rights.
        ii. customized storage zones and repositories ensuring very granular policies can be used.
    - How are patients, doctors, and other hospital staff interacting with the data and the connected thing?
        i. Learning the users, their behaviors, and how they'll be using the IoT device will help building the device security strategy. Data security should be designed around user interaction.
    - How much visibility do we have into the connected things. What about management?
        i. Creating good visibility and management ecosystem for connected devices is crucial for building policies around data security.
        ii. Effective visualization of the network system and the devices connected to it helps in locking down data points and defend against vulnerabilities.
5. IoT as a new technology has been more widely used and is constantly evolving. Even in healthcare applications. The open nature of the information/data media has brought risks to the security of the wireless sensor networks and their collected data.
    - Several techniques can be applied in securing the data transmission between these applications but we need to make sure that it remains cheap and efficient.
    - Apart from the transmission we also need a system on the application level to determine which user can access which information. In an ideal situation, the patient should be in full control of the information that is being shared. There cannot be an exhaustive set of rules to determine which subject has what role. A system needs to be created in such a way that the subjects are assigned roles dynamically based upon the environment they are working in.
6. Perception layer consists of the sensors and technologies that are used to collect, acquire and process data from the physical world. The security issues in the RFID technology is as follows:
    - *Uniform coding*: Currently there is no uniform international encoding standard for RFID tag. this may cause problems that the reader cannot obtain access to the tag information or errors may occur in the reading process.
    - *Node Capture*: Key nodes can be controlled easily by the attackers such as gateway node, where they might get access to all information, including group communication key, radio key, matching key etc., This might threaten the security of the entire network.
    - *Replay Attack*: Attacker sends a package which has been received by the destination host, to obtain the trust of system. It mainly used in the authentication processing, and destroy the validity of certification.
    - *Mass Node Authentication Problem*: The efficiency of mass node authentication needs to be solved in IoT.

    The above research provides us a lightweight authentication protocol which helps identify the tag and the user or a node and server in a distributed IoT system.
7. The traditional methods of security cannot be used generally, as the computation time increases or because of the various overheads. Key management and key distribution are necessary for securely transferring the collected data. Secure routing is necessary and heterogeneous integration technologies are required for handling different formats of data. Cryptographic algorithms are necessary for data security, with limited computing power and storage space. The small size of the sensors should also be taken into consideration. Authentication of the sensors are extremely important as it will allow adversaries to not get into the system and perform any possible attacks.

8. For perception layer security in IoT, ECC-based authentication and the attribute-based access control policy performs better than traditional cryptographic algorithms in securing the data in the open environment of IoT in that it uses a smaller key size to achieve the same security.
    - Through establishing mutual authentication between the user and sensor nodes, only legitimate user can access resources, therefore ensures the security of the communication between user and nodes, and solves the resource-constrained problem of the IoT perception layer.
    - Attribute-based Access Control, based on user attribute certificate in access control authority further restricts the access from subject to object, therefore ensuring data resources to be effectively used and managed within the legal range. ABAC policy is more flexible and achieves fine-grained access control.
    - This proposed method is demonstrated to solve the resource-constrained problem, prevent against man-in-the-middle attack, eavesdropping attack, node capture attack and replay attacks, and mitigate Denial of Service.

## 5.2 RECOMMENDATIONS

Based on the available research on various security verticals listed in 3.1.3, we have come up with following recommendations for the critical security verticals.

1. Specifically, addressing security and privacy issues in eHealth integrated with IoT Healthcare is a great advancement towards securing healthcare systems around the globe. The coming of age of eHealth is intrinsically linked to the successful deployment of a secure and privacy-preserving M2M/IoT infrastructure.
    - The authors have proposed an architecture and framework that support the development and providing of healthcare solutions and at the same time addressing security and privacy issues.
    - The authors have further identified core standards and industry bodies where eHealth-M2M-IoT standardization is in progress. While comprehensive, the list is not exhaustive. In closing, we emphasize that security and privacy for eHealth in the emerging IoT landscape offers serious challenges as well as exciting opportunities to the industry.
2. There is a need for lightweight cryptographic protocols in IoT as the traditional cryptographic algorithms used to defeat attempts of pattern analysis consume lot of processor's efficiency. Devices with limited processor capabilities need some modified protocols. Based on the available research and references, following are some of the best practices that could be adopted into network security protocols for IoT devices.
    - Master key used for encryption must change after a desired interval based on the level of security needed.
    - Ciphertext should not be predictive. For a given plaintext, multiple encryptions should give different cipher texts.
    - Pseudo-random techniques for cryptographic key and password generation should be avoided.
    - Employ error correction codes to handle dynamically changing network topologies.
3. A best way to secure data flowing from resource constrained devices is using and end-to-end encryption protocol. This protocol will offload heavy cryptographic operations to the nearby capable nodes. What happens in here is that the end devices authenticate each other and after that share a secret key for communicating encrypted data. Asymmetric cryptographic methods are used for establishing keys.
    - The offloading of the operations to the nearby devices is done based on the trustworthiness of the device. Denial of service attacks and Man-In-The-Middle attacks are prevented as even the encryption tasks are offloaded to and from trusted devices.

- Device to device communication can be made more secure using secure version of Message Queue Telemetry Transport(MQTT) - SMQTT. This protocol is based on two variants of Attribute Based Encryption (ABE) - Ciphertext based and Key based. The data is encrypted and sent by making use of set of conditions which are based on access policies. Only those receiver nodes will be able to decrypt the message which have proper access policies.

4. The only suitable model for all authentications in Healthcare IoT environment is through security tokens. Here, one actor authenticates to another by including a previously obtained token on its messages. The token serves to identify the first actor, enabling the second actor to make an appropriate authorization decision.
    - For health data, a powerful mechanism to give control to the user of the data that is being shared, is by requiring that the user be actively involved in the process, where the different actors are issued the security tokens used for subsequent interactions. Without the user's consent, no tokens are issued and no authenticated interactions occur.
    - OAuth 2.0 and OpenID Connect 1.0 are two standardized frameworks for authentication and authorization that explicitly support the above model. As HTTP is not enough for interactions in the Health IoT environment, a new class of protocols viz. MQ Telemetry Transport and Constrained Application Protocol is recommended
5. The authentication scheme provides a secure layer for communication between the RFID tag and the user by overcoming the key compromise problem. There should be different protocols which implements the lightweight ECC authentication scheme to include preventive measures against impersonation attack, server spoofing attack, DoS attack and cloning attack.
    - Two-phase authentication protocol in a distributed IoT application is used to secure the communication between the sensor nodes and the end-user in a distributed environment. This approach should have advanced node capture attack prevention protocols to prevent an attacker sending messages to a legitimate user.
    - The utilization of implicit certificates can be proposed to provide access control and multicasting in a large scale distributed system.
6. A proper key authorization of the sensors is required for proper identification and approval and to verify that the sensor is valid. This is helpful to avoid attacks such as eavesdropping, man in the middle attacks and so on. Cryptographic algorithms should be carefully used so that it will avoid possible attacks. The key authorization should be secure. Secure measures must be taken from the architecture point of view to avoid reputation and issues.
7. Applications in healthcare IoT should have a control over who can access what data. This not only increases transparency but also encapsulates information. Example: An ENT specialist should not see the information regarding the patient's heart.
    - This protocol can be followed by maintaining an exhaustive hierarchy of user roles and defining which person is authorized for a piece of information. Different settings could also change a user role. A person could have different access rights in different environment. Hence, these rules should be made under all such scenarios.
    - Sharing information between applications should take advantage of hybrid security techniques such that they take advantage of benefits of one method over the weakness of others. Overall, the applications in IoT require only specific security controls which should be evaluated before implementing them.
8. In ECC-based authentication and the attribute-based access control policy:
    - Through establishing mutual authentication between the user and sensor nodes, only legitimate user can access resources, therefore this ensures the security of the communication between user and nodes, and solves the resource-constrained problem of the IoT perception layer. This approach should be further improved to work in a large

scale IoT environment when billions of things are connected. Furthermore, this approach needs further modification to defend server spoofing attack and cloning attack.

- Attribute-based Access Control that ensures data resources to be effectively used and managed within the legal range are not discussed and implemented in detail, therefore it requires further research on its implementation and limitations.

9. The Offloader architecture can prove to be an excellent solution for IoT devices provided the node ingredients of the Architecture themselves remain secure. So, it is critical that in the Offloader architecture, security of offloader, security of TAM and security of End Points are given highest priority.
10. Diameter Protocol is a one-way solution to various IoT needs it encompasses solutions to all the three categories of vulnerabilities i.e. Design, Development, and Deployment. Not only the new system can be benefitted but also with a minimal cost the existing systems can be upgraded with this model to enhance the application security.
    - Data Encryption remains key to avoid data tampering by the attackers, homomorphic encryption on one hand is protective but is tedious and contains heavy calculations while the new algorithm proposed i.e. Improved from DES from WSN has simple implementation, lightweight calculations, and small scale codes.

# 6 REFERENCES


[1] Iqbal, Muhammad A., and Magdy Bayoumi. "A Novel Authentication and Key Agreement Protocol for Internet of Things Based Resource-Constrained Body Area Sensors." Future Internet of Things and Cloud Workshops.

[2] Jan, Mian Ahmad, et al. "A robust authentication scheme for observing resources in the internet of things environment." Trust, Security and Privacy in Computing and Communications (TrustCom), 2014 IEEE 13th International Conference on. IEEE, 2014.

[3] Raghavendra K, Sumith Nireshwalya. “Application Layer Security Issues and Its Solutions”,IJCSET |June 2012| Vol 2, Issue 6,1266-1269

[4]Gong, Tianhe, et al. "A medical health-care system for privacy protection based on IoT." Parallel Architectures, Algorithms and Programming (PAAP), 2015 Seventh International Symposium on. IEEE, 2015.

[5] John Rouda,“Application layer security, july,25, 2006”

[6] M. Poulymenopoulou, F. Malamateniou, G. Vassilacopoulos, “A virtual PHR authorization system”, IEEE-EMBS International Conference on Biomedical and Health Informatics (BHI), 2014

[7] Lobna Yehia, Ayman Khedr, Ashraf Darwish, “Hybrid Security Techniques for Internet of Things Healthcare Applications”, Advances in Internet of Things, 2015, 5, 21-25

[8] Muhammad A Iqbal, Dr. Magdy Bayoumi, “Secure End to End key establishment protocol for resource constrained healthcare sensors in context of IoT”, IEEE, 2016

[9] Bacem Mbarek, Aref Meddeb, Wafa Ben Jaballah, Mohamed Mosbah, “A Secure Authentication Mechanism for Resource Constrained Devices”, IEEE, 2015

[10] Meena Singh, Rajan MA, Shivraj VL, Balamuralidhar P, “Secure MQTT for Internet Of Things (IoT) ”, IEEE, 2015

[11] Jungsoo Park, Seolah Je, Souhwan Jung et al, “A Secure Patient Information Transfer Method through Delegated Authorization” , IEEE 2016.

[12] Sumit Mishra, “Network Security Protocol for Constrained Resource Devices In Internet Of Things”, IEEE Indicon 2015.

[13] Internet of Things: Architectural Framework for eHealth Security David Lake, Rodolfo Milito, Monique Morrow and Rajesh Vargheese, RP Journals, Received: 26 June, 2013; Accepted: 8 October, 2013.

[14] A Back-end Offload Architecture for Security of Resource-constrained Networks, Jiyong Han and Daeyoung Kim Date of Conference: 31 Oct.-2 Nov. 2016 , Date Added to IEEE *Xplore*: 12 December 2016

[15] BSN-Care: A Secure IoT-Based Modern Healthcare System Using Body Sensor Network, Prosanta Gope and Tzonelih Hwang Published in: IEEE Sensors Journal ( Volume: 16, Issue: 5, March1, 2016)

[16] Cancellation-Based Friendly Jamming for Physical Layer Security, Date of Conference: 4 Dec.-8Dec.2016, Date Added to IEEE *Xplore*: 06 February 2017

[17] An Efficient Authentication and Access Control Scheme for perception layer of Internet of Things, Applied Mathematics & Information Science 2014

[18] Yeh, Kuo-Hui. "A Secure IoT-based Healthcare System with Body Sensor Networks." *IEEE Access* (2016).

[19] Ng, H. S., M. L. Sim, and C. M. Tan. "Security issues of wireless sensor networks in healthcare applications." *BT Technology Journal* 24.2 (2006): 138-144.

[20] Zhao, Zhenguo. "A secure RFID authentication protocol for healthcare environments using elliptic curve cryptosystem." *Journal of medical systems* 38.5 (2014): 46.

[21] Porambage, Pawani, et al. "Two-phase authentication protocol for wireless sensor networks in distributed IoT applications." *Wireless Communications and Networking Conference (WCNC), 2014 IEEE*. IEEE, 2014.