Integration of Lightweight & Energy Efficient Cipher in Wireless Body Area Network Fore-Health Monitoring

Azza Zayed Sultan Al Shamsi

Follow this and additional works at: https://scholarworks.uaeu.ac.ae/all_theses
Part of the Software Engineering Commons

Recommended Citation
https://scholarworks.uaeu.ac.ae/all_theses/474

This Thesis is brought to you for free and open access by the Electronic Theses and Dissertations at Scholarworks@UAEU. It has been accepted for inclusion in Theses by an authorized administrator of Scholarworks@UAEU. For more information, please contact fadl.musa@uaeu.ac.ae.
INTEGRATION OF LIGHTWEIGHT & ENERGY EFFICIENT CIPHER IN WIRELESS BODY AREA NETWORK FOR E-HEALTH MONITORING

Azza Zayed Abdul Aziz Sultan Al Shamsi

This thesis is submitted in partial fulfilment of the requirements for the degree of Master of Science in Software Engineering

Under the Supervision of Professor Ezedin Salem Barka

November 2016
Declaration of Original Work

I, Azza Zayed Abdul Aziz Sultan Al Shamsi, the undersigned, a graduate student at the United Arab Emirates University (UAEU), and the author of this thesis entitled “Integration of Lightweight & Energy Efficient Cipher in Wireless Body Area Network for e-Health Monitoring”, hereby, solemnly declare that this thesis is my own original research work that has been done and prepared by me under the supervision of Professor / Dr. Ezedin Salem Barka, in the College of Information Technology at UAEU. This work has not previously been presented or published, or formed the basis for the award of any academic degree, diploma or a similar title at this or any other university. Any materials borrowed from other sources (whether published or unpublished) and relied upon or included in my thesis have been properly cited and acknowledged in accordance with appropriate academic conventions. I further declare that there is no potential conflict of interest with respect to the research, data collection, authorship, presentation and/or publication of this thesis.

Student’s Signature ___________________________ Date 16/11/2017
Approval of the Master Thesis

This Master Thesis is approved by the following Examining Committee Members:

1) Advisor (Committee Chair): Ezedin Salem Barka  
   Title: Associate Professor  
   Department of Computer Science and Software Engineering  
   College of Information Technology  
   Signature: [Signature]  
   Date: 17/11/2016

2) Member: Zouheir Trabelsi  
   Title: Associate Professor  
   Department of Information Systems and Security  
   College of Information Technology  
   Signature: [Signature]  
   Date: 17/11/2016

3) Member: Mamoun A. Awad  
   Title: Associate Professor  
   Department of Computer Science and Software Engineering  
   College of Information Technology  
   Signature: [Signature]  
   Date: 17/11/2016

4) Member (External Examiner): Huwida Said  
   Title: Associate Professor  
   Department of Technological Innovation  
   Institution: Zayed University  
   Signature: [Signature]  
   Date: 17/11/2016
This Master Thesis is accepted by:

Dean of the College of Information Technology: Professor Omar El-Gayar

Signature [Signature]
Date 15/1/2017

Dean of the College of the Graduate Studies: Professor Nagi T. Wakim

Signature [Signature]
Date 16/1/2017

Copy 8 of 9
Abstract

There is an increase in the diseases of the circulatory system in United Arab Emirates, which makes it the first leading cause of death. This led to a high demand for a continuous care that can be achieved by adopting an emerging technology of e-Health monitoring system using Wireless Body Area Network (WBAN) that can collect patient’s data. Since patient’s data is private, securing the communication within WBAN becomes highly essential. In this research thesis, we propose an architecture to secure the data transmission within the Wireless Body Area Network (WBAN) in e-Health monitoring. More specifically, our proposed architecture encrypts the patient’s sensed data, collected by sensors and sent to a mobile device, using energy efficient and lightweight encryption algorithm (LEA). Our implementation results show that choosing LEA encryption algorithm is the best option for encrypting data that is transmitted from a body-wearable sensor to a mobile device. This approach ensures the security and the privacy of patient’s “critical” data transmitted on WBAN, and is used in e-health monitoring. Our contribution in this research are twofold. First, conducting an extensive study to determine the best cipher that is suitable for WBAN. Second, determining and implementing LEA as the best solution for WBAN in terms of lightweight and energy efficiency which are critical factors in Body Sensor Network.

Keywords: Wireless Body Area Network, WBAN, e-Health, Security, Privacy, Encryption, lightweight encryption algorithm, Low-Energy
الملخص

أوضح من خلال البحث أن هناك زيادة مستمرة لأمراض الدورة الدموية في دولة الإمارات العربية المتحدة، ويعتبر المسبب الرئيسي للوفاة، مما أدى ذلك إلى ارتفاع الطلب على الرعاية المستمرة للمريض في جميع المنشآت الصحية الحكومية و الخاصة، حيث أصبح من الممكن تحقيق هذه الرعاية من خلال التكنولوجيا الحديثة عبر نظام مراقبة صحة المريض إلكترونياً باستخدام شبكة اتصال لاسلكية الجسم (WBAN) التي يمكن جمع بيانات المريض من خلالها، فيما أن بيانات المريض خصوصية، بالتالي فإنه من الضروري وضع أمان للمعلومات المنبعثة من شبكة اتصال لاسلكية الجسم لحفظ كافة معلومات المريض. في هذه الأطروحة البحثية، نقترح بنية لتثبيت نقل البيانات من داخل شبكة اتصال لاسلكية الجسم (WBAN) عند مراقبة الصحة إلكترونياً، وبشكل أكثر تحديثاً، الهيكل المقترح لدينا يقوم بتسهيل بيانات المريض التي جمعتها أجهزة الاستشعار وإرسالها إلى جهاز محمول، وذلك باستخدام خوارزمية تشفير خفيفة في الوزن و ذات كفاءة في استخدام الطاقة (LEA).

لقد أظهرت النتائج عند تنفيذ تجربة تطبيق خوارزمية التشفير التي تم اختيارها أنها أفضل خيار لتسهيل البيانات التي يتم إرسالها من جهاز استشعار يمكن للمريض ارتداؤه إلى جهاز محمول. هذا التطبيق للخوارزمية يضمن أمن وخصوصية البيانات المهمة للمريض، التي يمكن من خلال شبكة اتصال لاسلكية الجسم (WBAN) مشاركتها من شبكة اتصال لاسلكية الجسم (WBAN) مشاركتها من شبكة اتصال لاسلكية الجسم (WBAN) مشاركتها من شبكة اتصال لاسلكية الجسم (WBAN) مشاركتها من شبكة اتصال لاسلكية الجسم (WBAN) مشاركتها من شبكة اتصال لاسلكية الجسم (WBAN) مشاركتها من شبكة اتصال لاسلكية الجسم (WBAN) مشاركتها من شبكة اتصال لاسلكية الجسم (WBAN) مشاركتها من شبكة اتصال لاسلكية الجسم (WBAN) مشاركتها من شبكة اتصال لاسلكية الجسم (WBAN) مشاركتها من شبكة اتصال لاسلكية الجسم (WBAN) مشاركتها من شبكة اتصال لاسلكية الجسم (WBAN) مشاركتها من شبكة اتصال لاسلكية الجسم (WBAN) مشاركتها من شبكة اتصال لاسلكية الجسم (WBAN) مشاركتها من شبكة اتصال لاسلكية الجسم (WBAN) مشاركتها من شبكة اتصال لاسلكية الجسم (WBAN) مشاركتها من شبكة اتصال لاسلكية الجسم (WBAN) مشاركتها من شبكة اتصال لاسلكية الجسم (WBAN) مشاركتها من شبكة اتصال لاسلكية الجسم (WBAN) مشاركتها من شبكة اتصال لاسلكية الجسم (WBAN) مشاركتها من شبكة اتصال لاسلكية الجسم (WBAN) مشاركتها من شبكة اتصال لاسلكية الجسم (WBAN) مشاركتها من شبكة اتصال لاسلكية الجسم (WBAN) مشاركتها من شبكة اتصال لاسلكية الجسم (WBAN) مشاركتها من شبكة اتصال لاسلكية الجسم (WBAN) مشاركتها من شبكة اتصال لاسلكية الجسم (WBAN) مشاركتها من شبكة اتصال لاسلكية الجسم (WBAN) مشاركتها من شبكة اتصال لاسلكية الجسم (WBAN) مشاركتها من شبكة اتصال لاسلكية الجسم (WBAN) مشاركتها من شبكة اتصال لاسلكية الجسم (WBAN) مشاركتها من شبكة اتصال لاسلكية الجسم (WBAN) مشاركتها من شبكة اتصال لاسلكية الجسم (WBAN) مشاركتها من شبكة اتصال لاسلكية الجسم (WBAN) مشاركتها من شبكة اتصال لاسلكية الجسم (WBAN) مشاركتها من شبكة اتصال لاسلكية الجسم (WBAN) مشاركتها من شبكة اتصال لاسلكية الجسم (WBAN) مشاركتها من شبكة اتصال لاسلكية الجسم (WBAN) مشاركتها من شبكة اتصال لاسلكية الجسم (WBAN) مشاركتها من شبكة اتصال لاسلكية الجسم (WBAN) مشاركتها من شبكة اتصال لاسلكية الجسم (WBAN) مشاركتها من شبكة اتصال لاسلكية الجسم (WBAN) مشاركتها من شبكة اتصال لاسلكية الجسم (WBAN) مشاركتها من شبكة اتصال لاسلكية الجسم (WBAN) مشاركتها من شبكة اتصال لاسلكية الجسم (WBAN) مشاركتها من شبكة اتصال لاسلكية الجسم (WBAN) مشاركتها من شبكة اتصال لاسلكية الجسم (WBAN) مشاركتها من شبكة اتصال لاسلكية الجسم (WBAN) مشاركتها من شبكة اتصال لاسلكية الجسم (WBAN) مشاركتها من شبكة اتصال لاسلكية الجسم (WBAN) مشاركتها من شبكة اتصال لاسلكية الجسم (WBAN) مشاركتها من شبكة اتصال لاسلكية الجسم (WBAN) مشاركتها من شبكة اتصال لاسلكية الجسم (WBAN) مشاركتها من شبكة اتصال لاسلكية الجسم (WBAN) مشاركتها من شبكة اتصال L

مباحث البحث الرئيسية: شبكة اتصال لاسلكية الجسم، صحة الإلكترونية، أمن، حماية، شفرة، خوارزمية، خفة وزن، كفاءة طاقية، خوارزمية خفيفة الوزن
Acknowledgements

I have been surrounded by many great people who kept showing me guidance and support through the whole process of writing and experimenting. I am grateful to my advisor, Professor Ezedin S. Barka for his encouragement, patience and support in everything I do. I would like also to thank Professor Mohamed Adel Serhani for his novel paper (Benharref & Serhani, 2014) which enlightened me with the domain area that I want to target and for his effort to help me in the experiment part. Moreover, a special thanks to Eng. Abdulrahman Daher for his time in providing me with the basic knowledge in the hands-on of the Engineering part.

My sincere gratitude goes to my parents, brothers and sisters who never stopped believing in me and in what I do. They always have been there for me and without them I would never have been able to finish my thesis.
Dedication

To my beloved parents, brothers and sisters
Who have been there for me in every phase of my life
# Table of Contents

Title .......................................................................................................................... i
Declaration of Original Work .................................................................................. ii
Copyright .................................................................................................................. iii
Approval of the Master Thesis ................................................................................ iv
Abstract .................................................................................................................... vi
Title and Abstract (in Arabic) ................................................................................... vii
Acknowledgements ................................................................................................... viii
Dedication ................................................................................................................... ix
Table of Contents ..................................................................................................... x
List of Tables ............................................................................................................. xii
List of Figures ........................................................................................................... xiii
List of Abbreviations ............................................................................................... xiv

Chapter 1: Introduction ............................................................................................. 1
  1.1 Overview of Wireless Body Area Network ....................................................... 1
  1.2 Three-Tier WBAN Architecture ..................................................................... 2
  1.3 Differences between WSN and WBAN ......................................................... 3
  1.4 Challenges of WBAN .................................................................................... 6
  1.5 Security Requirements of WBAN ................................................................. 7
      1.5.1 Data Storage Security Requirements .................................................. 9
      1.5.2 Data Access Security Requirements .................................................. 9
      1.5.3 Other Security Requirements .............................................................. 10
  1.6 Problem Statement ....................................................................................... 10
  1.7 Research Objectives ..................................................................................... 11
  1.8 Related Research .......................................................................................... 11
  1.9 Organization of the thesis ............................................................................. 12

  2.1 Description .................................................................................................... 13
  2.2 Target Platform: Sensor Device .................................................................... 14

Chapter 3: Lightweight Encryption Algorithm (LEA) ............................................. 15
  3.1 Overview ...................................................................................................... 15
  3.2 LEA versus Other Ciphers ...................................................................... 15
      3.2.1 Advanced Encryption Standard (AES) ............................................. 18
      3.2.2 Block Ciphers with ARX Structure ............................................... 19
      3.2.3 Lightweight Block Ciphers .............................................................. 20
3.2.4 Stream Ciphers ......................................................... 21
3.3 Specifications of LEA ....................................................... 21
   3.3.1 Notations ............................................................. 21
   3.3.2 Key Schedule ....................................................... 23
   3.3.3 Encryption Procedure ............................................. 25

Chapter 4: Implementation ..................................................... 26
   4.1 Overview .................................................................... 26
   4.2 Device and Experiment Environment .............................. 26
      4.2.1 Intel Curie Microcontroller .................................. 27
      4.2.2 Pulse Sensor ...................................................... 28
      4.2.3 Eclipse ............................................................. 29
      4.2.4 Emscripten ......................................................... 31
      4.2.5 Johnny-Five ......................................................... 33

Chapter 5: Performance Analysis ............................................. 34
   5.1 Overview .................................................................... 34
   5.2 Performance Criteria .................................................. 34
   5.3 Results ....................................................................... 35
   5.4 Scenario ...................................................................... 38
   5.5 Limitations ............................................................... 38

Chapter 6: Conclusion and Future Work ................................... 40

References ........................................................................... 41

List of Publications ............................................................ 47
List of Tables

Table 1: An overview of the differences between WSN and WBAN ......................... 4
Table 2: Major security requirements in WBAN ...................................................... 7
Table 3: LEA versus Other Ciphers .......................................................................... 16
Table 4: Notations used to explain LEA algorithm ..................................................... 21
Table 5: Comparison results between AES and LEA .................................................. 35
List of Figures

Figure 1: A three-tier architecture of WBAN ................................................................. 3
Figure 2: Proposed architecture of secure WBAN for e-Health Monitoring .......... 13
Figure 3: The data flow in the sensor ............................................................................ 14
Figure 4: Round function of LEA .................................................................................. 25
Figure 5: Implementation Diagram .............................................................................. 27
Figure 6: Pulse Sensor plugged into Intel Curie Microcontroller .............................. 28
Figure 7: Pseudo code of the overall implementation ................................................. 29
Figure 8: Import AES and LEA algorithms as libraries to the code ......................... 30
Figure 9: Reading the heart rate from pulse sensor ....................................................... 30
Figure 10: Encrypting the data using AES algorithm .................................................. 30
Figure 11: Encrypting the data using LEA algorithm ................................................... 31
Figure 12: The compiling process in Emscripten ......................................................... 31
Figure 13: Emscripten Command Prompt ..................................................................... 32
Figure 14: The JavaScript output of LEA encryption algorithm ................................. 32
Figure 15: Install the Johnny-Five module ................................................................. 33
Figure 16: Import Johnny-Five as a library to the code ................................................. 33
Figure 17: Energy consumption results of 100 heartrate readings using AES algorithm ........................................................................................................... 36
Figure 18: Energy consumption results of 100 heartrate readings using LEA algorithm ........................................................................................................... 36
Figure 19: Energy consumption results of 100 heartrate readings using AES and LEA algorithms ........................................................................................................... 37
Figure 20: The Microcontroller has a limited power .................................................... 38
# List of Abbreviations

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AES</td>
<td>Advanced Encryption Standard</td>
</tr>
<tr>
<td>BAN</td>
<td>Body Area Network</td>
</tr>
<tr>
<td>BS</td>
<td>Base Station</td>
</tr>
<tr>
<td>BNs</td>
<td>Body Area Network Nodes</td>
</tr>
<tr>
<td>ECG</td>
<td>Electrocardiogram</td>
</tr>
<tr>
<td>EMG</td>
<td>Electromyography</td>
</tr>
<tr>
<td>LEA</td>
<td>Lightweight Encryption Algorithm</td>
</tr>
<tr>
<td>NIST</td>
<td>The National Institute of Standards and Technology</td>
</tr>
<tr>
<td>SpO2</td>
<td>Oxygen saturation sensor</td>
</tr>
<tr>
<td>TEA</td>
<td>Tiny Encryption Algorithm</td>
</tr>
<tr>
<td>WBAN</td>
<td>Wireless Body Area Network</td>
</tr>
<tr>
<td>WSN</td>
<td>Wireless Sensor Network</td>
</tr>
<tr>
<td>ARX</td>
<td>Addition, rotation and XOR</td>
</tr>
</tbody>
</table>
Chapter 1: Introduction

1.1 Overview of Wireless Body Area Network

A Wireless Body Area Network (WBAN) is formally defined by IEEE 802.15 Task Group 6 (IEEE; "IEEE Standard for Local and metropolitan area networks - Part 15.6: Wireless Body Area Networks," 2012) as “a communication standard optimized for low power devices and operation on, in, or around the human body (but not limited to humans) to serve a variety of applications including medical consumer electronics / personal entertainment and other.”

A WBAN is consisted of sensors that can be inbuilt within a small device or added externally (Buratti, Conti, Dardari, & Verdone, 2009; Tubaishat & Madria, 2003). Such a miniaturized low power device can be either worn on top of a human body or exist inside. For communication purposes these kind of devices have a built in radio to enable communication between themselves or to a base station (BS) (Akkaya, Younis, & Youssef, 2007; Shi & Hou, 2009). These devices can sense different kinds of parameters which can be used to monitor a patient’s health and send the readings to the patient or to a medical personnel.

The WBAN can be classified to be either sensor or actuator (Van de Panne & Fiume, 1993). The difference is that, sensor senses different parameters of the body, for instance, heart rate, temperature, blood pressure and blood glucose. On the other hand, the actuators read the sensed data and make a decision or receive a command from the user or medical personnel. For example, the following paper (Benharref & Serhani, 2014) explained three different actions that the actuator can prompt if and only if the readings were out of range. The first action is ‘Warning’ when the reading
is low and it needs to be back to normal so the device prompts an appropriate lifestyle advice to the patient. The second action is ‘Serious’ when the reading is high and the patient needs to see a physician so the device instructs the patient to do so. The final action is ‘Critical’ when the values are so high that the patient needs to be hospitalized; the device will send the geographical location of the patient to the paramedics so the ambulance can reach them as soon as possible. This is just an example of how actuators can be used in our lives.

**1.2 Three-Tier WBAN Architecture**

Figure 1 illustrates a general architecture of WBAN for e-Health monitoring system (M. Chen, Gonzalez, Vasilakos, Cao, & Leung, 2011). It separates the architecture into three components. The architecture and the communication designs for these tiers (Tier-1-Comm design, Tier-2-Comm design and Tier-3-Comm design) can be describes as the following:

The intra-BAN communication (Tier-1-Comm) contains all the BAN Nodes (BNs), such as Electrocardiogram (ECG) which is used to monitor electrical activity of the heart, Oxygen saturation sensor (SpO2) that helps to measure the level of oxygen, and Electromyography (EMG) for monitoring the muscle activity (Saleem, Ullah, & Yoo, 2009).

The inter-BAN communication (Tier-2-Comm) holds all the WBAN controllers to communicate with access points. Usually, the access points are connected to inventory systems, databases and internet so its job to link between Tier-1 and Tier-3. The access points can be a handset such as mobile phones, laptops, PDAs and other devices that is used based on the suitable environment for the patient. For example, phones are most convenient when the patients are moving around however
if they want to monitor their health status in his room or office they can use laptops or any bigger screen devices that can be connected to internet (Syed & Yau, 2013).

The beyond-BAN communication (Tier-3-Comm) includes a number of remote base-stations (e.g. inventory systems and databases) that preserve a patient’s records and provides relevant diagnostic recommendations (Saleem et al., 2009).

<table>
<thead>
<tr>
<th>Sensors</th>
<th>Tier-1-Comm</th>
<th>Tier-2-Comm</th>
<th>Tier-3-Comm</th>
</tr>
</thead>
<tbody>
<tr>
<td>EEG</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ear Sensor</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Blood Pressure</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ECG</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>EMG</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Motion Sensor</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>...</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Intra-BAN Communication   Inter-BAN Communication Beyond-BAN Communication

Figure 1: A three-tier architecture of WBAN

1.3 Differences between WSN and WBAN

There is always a confusion between Wireless Sensor Network (WSN) and Wireless Body Area Network (WBAN). Thus, an overview of the differences between the two is given in Table 1 (Barakah & Ammad-uddin, 2012; M. Chen et al., 2011; Latré, Braem, Moerman, Blondia, & Demeester, 2011; Ramli & Ahm, 2011)
**Table 1: An overview of the differences between WSN and WBAN**

<table>
<thead>
<tr>
<th>Challenges</th>
<th>Wireless Sensor Network</th>
<th>Wireless Body Area Network</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Scale</strong></td>
<td>Monitored environment</td>
<td>Human body (centimeters /</td>
</tr>
<tr>
<td></td>
<td>(meters / kilometers)</td>
<td>meters)</td>
</tr>
<tr>
<td><strong>Node number</strong></td>
<td>Many redundant nodes for</td>
<td>Fewer, limited in space</td>
</tr>
<tr>
<td></td>
<td>wide area coverage</td>
<td></td>
</tr>
<tr>
<td><strong>Result accuracy</strong></td>
<td>Through node redundancy</td>
<td>Through node accuracy and</td>
</tr>
<tr>
<td></td>
<td></td>
<td>robustness</td>
</tr>
<tr>
<td><strong>Node tasks</strong></td>
<td>Node performs a dedicated task</td>
<td>Node performs multiple task</td>
</tr>
<tr>
<td><strong>Node size</strong></td>
<td>Small is preferred, but not important</td>
<td>Small is essential</td>
</tr>
<tr>
<td><strong>Network topology</strong></td>
<td>Very likely to be fixed and static</td>
<td>More variable due to body movement</td>
</tr>
<tr>
<td><strong>Data rates</strong></td>
<td>Homogeneous</td>
<td>Heterogeneous</td>
</tr>
<tr>
<td><strong>Node replacement</strong></td>
<td>Performed easily, nodes even disposable</td>
<td>Replacement of implanted nodes difficult</td>
</tr>
<tr>
<td><strong>Node lifetime</strong></td>
<td>Several years/months</td>
<td>Several years/months, but smaller battery capacity</td>
</tr>
<tr>
<td></td>
<td>Accessible and likely to be replaced more easily and frequently</td>
<td>Inaccessible and difficult to replace in an implantable setting</td>
</tr>
<tr>
<td>---------------------------</td>
<td>-----------------------------------------------------------------</td>
<td>---------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Power supply</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Power demand</strong></td>
<td>Likely to be large, energy supply easier</td>
<td>Likely to be lower, energy supply more difficult</td>
</tr>
<tr>
<td><strong>Energy scavenging source</strong></td>
<td>Most likely solar and wind power</td>
<td>Most likely motion (vibration) and thermal (body heat)</td>
</tr>
<tr>
<td><strong>Biocompatibility</strong></td>
<td>Not a consideration in most applications</td>
<td>A must for implants and some external sensors</td>
</tr>
<tr>
<td><strong>Security level</strong></td>
<td>Lower</td>
<td>Higher, to protect patient information</td>
</tr>
<tr>
<td><strong>Impact of data loss</strong></td>
<td>Likely to be compensated by redundant nodes</td>
<td>More significant, may require additional measures to ensure QoS and real-time data delivery</td>
</tr>
<tr>
<td><strong>Wireless technology</strong></td>
<td>Bluetooth, Zigbee, GPRS, WLAN,…</td>
<td>Low power technology required</td>
</tr>
</tbody>
</table>

The differences stated above, show that the solutions that are suitable for WSN may not be suitable for WBAN, though they share some common challenges. As shown in Table 1, there is a high need for addressing power consumption in WBAN,
while it is not the case in WSN. Moreover, Privacy is a major factor and must be addressed in WBAN and not in WSN.

Regarding the power consumption, WBAN supports minimal power usage so the proposed solution should provide a low power overall design.

Furthermore, WBAN demands a high security level since it collects the vital signs of a patient which considered to be a private data. All the collected info must be protected from any unauthorized access. However, the small memory of the node makes it difficult to use the existing cryptographic algorithms like AES, DES, etc. Such a limitation requires a cryptographic algorithm that can utilize lower memory.

1.4 Challenges of WBAN

WBAN is an emerging technology that has several challenges that need to be taken into account (Patel & Wang, 2010). These challenges are similar to the one faced by Wireless Sensor Network (WSN) (Barakah & Ammad-uddin, 2012); however, there are some important concerns related specifically to the usage of WBAN in healthcare domain.

First, it demands for low energy. Since the size of WBAN is small, it limits the size of the power source which will result in enforcing minimal energy usage. In return the solution that can be implemented in WBAN must be energy efficient to be able to work for a long lifetime (Anastasi, Conti, Di Francesco, & Passarella, 2009; Boulis, Smith, Miniutti, Libman, & Tselishchev, 2012).

Second, managing the interference when multiple WBAN nodes come into range of each other (Zhou, He, Stankovic, & Abdelzaher, 2005). It might result in one node can read the messages of another one which is critical if an actuator node acts
based on a received message from another WBAN. This issue can be solved by using a proper user-authentication service to make sure that the receiver knows that the sender is the right one before taking any needed action (Das, 2009; Yasmin, Ritter, & Guilin, 2012).

Third, providing security to the network of WBAN by preventing any unauthorized access within the network or any manipulation to the packets in transit. This can be solved by user-authentication and data integrity checks (Das, 2009; Li, Lou, & Ren, 2010; Yasmin et al., 2012).

Finally, providing privacy especially when WBAN is dealing with a patient’s record. It is a private data that need to be protected from unauthorized users. Confidentiality issues can be solved by using encryption algorithms (Li et al., 2010).

1.5 Security Requirements of WBAN

The security architecture of the security mechanism should fulfill certain features to be able to implement in WBAN since there are many constraints the need to be taken in consideration. The major security requirements as the following (Ramli & Ahm, 2011):

Table 2: Major security requirements in WBAN

<table>
<thead>
<tr>
<th>Major security requirements</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data storage security requirements</td>
<td>The stored medical data should be private. Providing confidentiality by using Encryption and Access Control List.</td>
</tr>
</tbody>
</table>

Confidentiality
<table>
<thead>
<tr>
<th><strong>Integrity</strong></th>
<th>There should be no unauthorized modification to the content of the patient’s record.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Dependability</strong></td>
<td>Patient’s record must be readily retrievable when there is failure of data erasure happens.</td>
</tr>
<tr>
<td><strong>Data access security requirements</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Access Control</strong></td>
<td>There should be an enforcement of access policy to prevent any unauthorized access.</td>
</tr>
<tr>
<td>(Privacy)</td>
<td></td>
</tr>
<tr>
<td><strong>Accountability</strong></td>
<td>When users of WBAN abuses their device by carrying out unauthorized actions. They should be identified and held accountable.</td>
</tr>
<tr>
<td><strong>Revocability</strong></td>
<td>The privileges of WBAN users or nodes should be deprived in time if they are identified as compromised or behave maliciously.</td>
</tr>
<tr>
<td><strong>Non-repudiation</strong></td>
<td>The source of patient’s record cannot deny about generating that piece of information.</td>
</tr>
<tr>
<td><strong>Other security requirements</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Authentication</strong></td>
<td>The sender of patient’s record must be authenticated and any injection of data from outside the WBAN should be prevented.</td>
</tr>
<tr>
<td><strong>Availability</strong></td>
<td>The patient’s record must be accessible even under denial-of-service (DoS) attacks.</td>
</tr>
</tbody>
</table>
1.5.1 Data Storage Security Requirements

Confidentiality: Is to prevent patients’ data from any leakage. Therefore, if an attacker obtained any confidential information, they will gain nothing since the property of such information is not made available to unauthorized individual or entity.

Integrity: Since patients’ data is critical and any modification to a patient’s record will cause a disaster results that might end up with patient’s death. Consequently, integrity is very important to guarantee that patients’ records cannot be modified and it is complete from any unauthorized change.

Dependability: It is very vital to be able to retrieve patients’ record when there is a failure of data erasure in the system. In such dynamic network system of WBAN, it is mandatory to have a fault tolerance to achieve such requirement.

1.5.2 Data Access Security Requirements

Access Control: Is the enforcement of access policy to prevent any unauthorized access. It provides privacy for information by defining different access privileges to different users. So there will be a control in what kind of information within the patient’s record that a specific user role can access.

Accountability: It is to be held accountable for any carried out actions by users of WBAN. Accordingly, any abuse to the usage of WBAN device, the user should be identified and held responsible.

Revocability: The privileges of a user using WBAN can be removed if the user is identified as a threat to the patient’s data or to the network of WBAN.
Non-repudiation: indicates the users’ who access patient’s records cannot deny receiving a record nor can the user who generate that piece of information deny sending it.

1.5.3 Other Security Requirements

Authentication: It is to verify the identity of a user. For example, the sender of patient’s record must be authenticated so any injection of data from outside the WBAN should be prevented.

Availability: The patient’s record must be accessible even under denial-of-service (DoS) attacks. It should be available all the time when it is needed.

1.6 Problem Statement

There is a published health statistic report in 2013 for the Emirate of Abu Dhabi that is provided by the Statistics Centre - Abu Dhabi (Abu-Dhabi, 2013), which shows that the first leading cause of death in 2013 is the ‘Diseases of the circulatory system’ at a death rate of 45.1 per 100,000 population. Also, the percentage distribution of death caused by the ‘Diseases of the circulatory system’ in 2010 is 26.5% and it increased in 2013 to be 36.7%. Moreover, the statistics presents that the number of patients who were admitted in government hospitals in 2010 was 86,136, while in 2013 it escalated to 119,000 patients.

Based on the above statistics, there is a high demand to have a continuous care about the patients’ status with severe conditions and reduce the consumption of government’s resources. This can be achieved by using the technology for applying e-Health monitoring within the region.
1.7 Research Objectives

With WBAN as an emerging technology that can collect a large amount of data when it placed in or around human body; it proves that it can be helpful to monitor patients. Nevertheless, the collected data is private that makes securing it essential with considering the demand for low power usage.

The paper aims to provide efficient and effective low energy communication and lightweight security algorithm design for e-Health monitoring using WBAN. Therefore, our contribution in this research are twofold. First, conducting an extensive study to determine the best cipher that is suitable for WBAN. Second, determining and implementing the best solution for WBAN in terms of lightweight and energy efficiency which are critical factors in Body Sensor Network. The paper will focus only on the communication between Tier-1 and Tier-2.

1.8 Related Research

There is a progress all over the world in developing wearable devices for health monitoring using WBAN. However, it is difficult to discover solutions that provide security for WBAN. As there are several security protocols in wireless sensor network (WSN).

For example, Security Protocols for Sensor Networks (SPINS) is a set of protocols that accomplish confidentiality, integrity and authenticity in wireless sensor networks and uses several symmetric keys to encrypt the data as well as compute the Message Authentication Code (MAC)(Jang, Lee, Han, & Park, 2011; Saleem, Ullah, & Kwak, 2010). Such protocol originally only for WSN and not for WBAN; however it can be applied in WBAN with low-power computation because of the limited computational resources in WBAN.
Other researchers who implement security protocols for WBAN used biometrics as a security framework for data authentication (Ramli, Ahmad, Abdollah, & Dutkiewicz, 2013). The sender's electrocardiogram (ECG) is considered as the biometric key in the system. As a result, patient’s data is only can be sensed from the patient's WBAN system and therefore it cannot be mixed with other patients’ WBAN.

However the above solution didn’t target confidentiality in WBAN which is the main focus of the thesis paper. There are researchers who implemented cryptographic algorithms in WSN. They did an implementation and performance analysis of AES-128 CBC algorithm for data encryption in WSN (Lee, Lee, & Shin, 2010). As a result, the thesis paper will provide a way to use encryption algorithm in WBAN by using a lightweight encryption and low energy demand algorithm to handle the limitation resources of WBAN.

1.9 Organization of the thesis

The rest of the thesis is organized as follows: Chapter 2 Introduces the proposed design architecture of the energy efficient Lightweight Encryption Algorithm in Wireless Body Area Network for e-Health monitoring. The details about the Lightweight Encryption Algorithm are provided in Chapter 3. Chapter 4 explains the implementation part, followed by experimentation results and performance analysis in Chapter 5. Finally, the conclusion of the thesis and the future work are presented in Chapter 6.

2.1 Description

The proposed design architecture is to provide secure data transmission from sensor to mobile by using energy efficient Lightweight Encryption Algorithm (LEA) in WBAN. The proposed solution will cover the communication between Tier-1 and Tier-2 of the WBAN.

The process is as follows: The patient will be wearing sensors to sense his/her vital signs, such as heart rate, blood pressure, sugar level, temperature, etc. Since patient’s data is private, the readings are encrypted, using an energy efficient lightweight encryption algorithm, to ensure the confidentiality, privacy, and integrity of the patient’s data. After the encryption, the data will be transmitted to mobile phone, or any other mobile device.

![Figure 2: Proposed architecture of secure WBAN for e-Health Monitoring](image-url)
2.2 Target Platform: Sensor Device

![Diagram of sensor data flow]

**Figure 3:** The data flow in the sensor

It is vital to secure the client-side before sending the information to the back-end of the cloud, which contains servers and databases. If the start point was not protected, then this will leave a huge probability that anyone can obtain patients’ data through transmission to a base station. So, even if there was a strong implementation to the rest of the architecture of e-Health monitoring and skipping the first stage, it makes the architecture vulnerable to different attacks.

The sensor that is used in the proposed design architecture is WBAN sensor. The internal architecture of the sensor has limitations which constrains the solution that can be implemented. Therefore, the algorithm should be energy efficient since the power that is supplied is small and replacing the power can be difficult especially if the sensor is implantable. Moreover, the solution should be lightweight to the memory of the sensor because of the memory space limitation. These two parameters must be addressed to be able to achieve the needed goal which is ensuring the confidentiality, privacy, and integrity of the patient’s data for a long lifetime without the need to replace battery or memory.
Chapter 3: Lightweight Encryption Algorithm (LEA)

3.1 Overview

LEA is a new lightweight block cipher that was announced by the Electronics and Telecommunications Research Institute in Korea (Hong et al., 2013). It is very efficient for limited-resource small devices because it has a small code size and consumes low power. LEA has a fast encryption on microprocessors since it uses simple operations like addition, rotation and XOR (ARX). It has three key sizes of 128, 192, 256 bits and a 128-bit block size. The algorithms are represented as LEA-128, LEA-192, LEA-256 based on the utilized key size. LEA is secure against all the existing attacks such as Differential (Biham & Shamir, 1993), Truncated Differential (L. R. Knudsen, 1994), Linear (Matsui, 1993), Zero Correlation (Bogdanov & Wang, 2012), Boomerang (Wagner, 1999), Impossible Differential (Biham, Biryukov, & Shamir, 2005), Integral (L. Knudsen & Wagner, 2002), and Differential-Linear (Biham, Dunkelman, & Keller, 2002).

3.2 LEA versus Other Ciphers

There are many reasons that made LEA the right algorithm to be chosen in the architecture. A better way to know is to compare it against other well-known ciphers that are standard and most widely used as Advance Encryption Standard (AES), or with other block ciphers that share the same ARX operations of LEA, or even with other block ciphers that considered to be lightweight. The comparisons can be explained in the following table and subsections:
Table 3: LEA versus Other Ciphers

<table>
<thead>
<tr>
<th>Cipher name</th>
<th>Vulnerability</th>
<th>Against LEA</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Advanced Encryption Standard (AES)</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AES</td>
<td>Biclique cryptanalysis for AES (128 192, 256) with time complexities $2^{126.1}$, $2^{189.7}$, and $2^{254.4}$ respectively.</td>
<td>It was designed recently with the latest techniques to prevent all existing attacks.</td>
</tr>
<tr>
<td><strong>Block Ciphers with ARX Structure</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tiny Encryption Algorithm (TEA) and the rest of the family (XTEA and XXTEA)</td>
<td>Short block size of 64 bits and 64 more rounds than LEA. There are full round attacks.</td>
<td>LEA has bigger block size of 128,192,256 bits and 24, 28, and 32 rounds respectively which makes it more secured and faster than TEA.</td>
</tr>
<tr>
<td>RC6</td>
<td>It is not exploited well for the parallelism of the modern CPUs.</td>
<td>LEA works well with the modern CPUs.</td>
</tr>
<tr>
<td>HIGHT</td>
<td>It works only for 8-bit processor and does not properly work well</td>
<td>LEA is strong against all existing attacks and it works.</td>
</tr>
</tbody>
</table>
on 32-bit CPUs which is the target in this thesis. well with any CPU size (32-bit or other size)

The full version is vulnerable to biclique cryptanalysis, impossible differential attacks and other techniques.

<table>
<thead>
<tr>
<th>Hash functions</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>More secure against known attacks however the usage of block ciphers and hash functions are different.</td>
<td>-</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Lightweight Block Ciphers</th>
</tr>
</thead>
<tbody>
<tr>
<td>HIGHT, PRESENT, LED and Piccolo</td>
</tr>
<tr>
<td>Shore block size and large number of rounds.</td>
</tr>
<tr>
<td>The full version is vulnerable to biclique cryptanalysis.</td>
</tr>
<tr>
<td>Block Cipher</td>
</tr>
<tr>
<td>-------------</td>
</tr>
<tr>
<td>KLEIN</td>
</tr>
<tr>
<td>PRINCE</td>
</tr>
</tbody>
</table>

### 3.2.1 Advanced Encryption Standard (AES)

AES (Daemen & Rijmen, 1998) was chosen as a standard by The National Institute of Standards and Technology (NIST) in 2000. It is the most widely used because of its good performance on most software and hardware platforms; however, since then cryptanalysis of block ciphers kept searching and developing for ways to break the encryption. As a consequence, there was an attack against the 7-round version of AES-128 (Ferguson et al., 2000) and by then there was only side-channel attacks for the full version of AES.
In 2009, there were several attacks started to target the other version of AES (Biryukov & Khovratovich, 2009; Biryukov, Khovratovich, & Nikolić, 2009). There was a key-recovery attack for the full 14-round of AES-256 with complexities of $2^{131}$ time and $2^{65}$ memory. Moreover, there was a key boomerang attack for the full 14-round of AES-256 with complexities of $2^{99.5}$ time and memory, and AES-192 with complexities of $2^{176}$ time and $2^{123}$ memory. In addition, there was a key recovery attack on the full version of AES (128 192, 256) using biclique cryptanalysis with time complexities $2^{126.1}$, $2^{189.7}$, and $2^{254.4}$ respectively (Bogdanov, Khovratovich, & Rechberger, 2011). On the other hand, LEA is designed recently with the latest techniques of design and analysis. It is resistant against all existing attacks and provides better speed and size than AES (Hong et al., 2013).

### 3.2.2 Block Ciphers with ARX Structure

Tiny Encryption Algorithm (TEA) (Wheeler & Needham, 1994) and the rest of the TEA family (XTEA and XXTEA) are Feistel block ciphers with simple round function and key schedule. These encryptions provide shorter block size of 64 bits and 64 more rounds than LEA, which limits its speed to be less than LEA. Also, there are full round attacks on them (Kelsey, Schneier, & Wagner, 1997; Yarrkov, 2010).

RC6 (Rivest, Robshaw, Sidney, & Yin, 1998) is considered to be faster than AES but it is not exploited well for the parallelism of the modern CPUs which affects its performance.

HIGHT (Hong et al., 2006) is a lightweight block cipher based on 8-bit processor so it does not properly work well for fast encryption on 32-bit CPUs which is the target in this thesis. Additionally, there were several attacks on the full version of HIGHT using biclique cryptanalysis, impossible differential attacks and many other
techniques that have been published (J. Chen, Wang, & Preneel, 2012; Lu, 2007; Song, Lee, & Lee, 2013).

Hash functions use the ARX structure for performance purposes on different platforms (Aumasson, Henzen, Meier, & Phan, 2008; Ferguson et al., 2010). They have a larger block size and key size than other block ciphers which makes them more secure against known attacks. Though it is powerful, but the usage of block ciphers and hash functions are different.

SPECK and SIMON are two new ciphers were published for lightweight encryption (Beaulieu et al., 2014). SPECK is an ARX cipher that has a high performance more than LEA only in 64-bit CPUs whereas LEA is more seemly to 32-bit CPUs. On the other hand, SIMON is made of ANDs, rotations and XORs but its performance in 32-bit and 64-bit CPUs, is slower than LEA.

3.2.3 Lightweight Block Ciphers

HIGHT (Hong et al., 2006), PRESENT (Bogdanov et al., 2007), LED (Guo, Peyrin, Poschmann, & Robshaw, 2011) and Piccolo (Shibutani et al., 2011) require short block size and large number of rounds which make the process of encryption slow. Furthermore, having a short block size, it is not sufficient for huge data size and for some operation modes it can permit security leakage using ciphertext-matching attack.

KLEIN (Gong, Nikova, & Law, 2011) is a cipher that is faster than AES on 8-bit and 16-bit CPUs however the target in this thesis is 32-bit CPUs.
The above ciphers are vulnerable to biclique cryptanalysis that can attack the full version of the encryption (Abed, Forler, List, Lucks, & Wenzel, 2012; Jeong, Kang, Lee, Sung, & Hong, 2012; Song et al., 2013).

CLEFIA (Shirai, Shibutani, Akishita, Moriai, & Iwata, 2007) is a cipher that has same block size and key size of AES with similarity in its software performance but not higher than AES.

PRINCE (Borghoff et al., 2012) is a good performance cipher in both software and hardware implementations nevertheless it has different security goal than the familiar block ciphers.

3.2.4 Stream Ciphers

In spite that there are stream ciphers that are based on ARX operations such as Salsa20 (Bernstein, 2008), there is no comparison between stream ciphers and block ciphers since both are different in the logic that is used for the encryption and decryption. Also, they are used for dissimilar application.

3.3 Specifications of LEA

3.3.1 Notations

The notations and their equivalent descriptions in the following Table 4.

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>$P$</td>
<td>128-bit plaintext, $P = P_0</td>
</tr>
<tr>
<td>$C$</td>
<td>128-bit ciphertext, $C = C_0</td>
</tr>
<tr>
<td>Symbol</td>
<td>Description</td>
</tr>
<tr>
<td>--------</td>
<td>-------------</td>
</tr>
<tr>
<td>$L(x)$</td>
<td>Length of bit sequence $x$.</td>
</tr>
<tr>
<td>$K$</td>
<td>Master key. $K = K_0</td>
</tr>
<tr>
<td>$X^i$</td>
<td>Intermediate value of $i$-th encryption state. $X^i = X^i_0</td>
</tr>
<tr>
<td>$T^i$</td>
<td>Intermediate value of $i$-th key schedule state. $T^i = T^i_0</td>
</tr>
<tr>
<td>$\delta_0, \delta_1, ..., \delta_n$</td>
<td>Constant value used for the key schedule. $n = 3$ where $L(K) = 128$, $n = 5$ where $L(K) = 192$, and $n = 7$ where $L(K) = 256$.</td>
</tr>
<tr>
<td>$r$</td>
<td>Number of round iterations. $r = 24$ where $L(K) = 128$, $r = 28$ where $L(K) = 192$, and $r = 32$ where $L(K) = 256$.</td>
</tr>
<tr>
<td>$RK^i$</td>
<td>192-bit round key used for $i$-th round. $RK^i = RK^i_0</td>
</tr>
<tr>
<td>⊕</td>
<td>XOR operation.</td>
</tr>
<tr>
<td>⊞</td>
<td>Addition modulo $2^{32}$.</td>
</tr>
<tr>
<td>$ROL_i(x)$</td>
<td>$x$-bit left rotation.</td>
</tr>
</tbody>
</table>
3.3.2 Key Schedule

3.3.2.1 Constants

A 32-bit long of 4, 6 and 8 as a constant value for each version of LEA key schedule. Every constant is expressed as follows:

\[ \delta_0 = C3EFE9DB_{16}, \delta_1 = 44626B02_{16} \]

\[ \delta_2 = 79E27C8A_{16}, \delta_3 = 78DF30EC_{16} \]

\[ \delta_4 = 715EA49E_{16}, \delta_5 = C785DA0A_{16} \]

\[ \delta_6 = E04EF22A_{16}, \delta_7 = E5C40957_{16} \]

The constants are generated from the hexadecimal expression of \( \sqrt{766,995} \), where 76, 69, and 95 are ASCII codes for “L”, “E”, and “A”.

3.3.2.2 Key Schedule for 128-bit Key

The key state \( T \) is assigned as \( T_{n-1} = K_n \) where \( 0 \leq n \leq 4 \). The key schedule of LEA-128 is expressed as the following:

\[ T_0^{i+1} \leftarrow ROL_1(T_0^i \oplus ROL_i(\delta_{i \mod 4})) \]

\[ T_1^{i+1} \leftarrow ROL_3(T_1^i \oplus ROL_{i+1}(\delta_{i \mod 4})) \]

\[ T_2^{i+1} \leftarrow ROL_6(T_2^i \oplus ROL_{i+2}(\delta_{i \mod 4})) \]

\[ T_3^{i+1} \leftarrow ROL_{11}(T_3^i \oplus ROL_{i+3}(\delta_{i \mod 4})) \]

\[ RK^i \leftarrow (T_0^i, T_1^i, T_2^i, T_3^i, T_1^i) \]

\[ ROR_i(x) \] \( x \)-bit right rotation.
3.3.2.3 Key Schedule for 192-bit Key

The key state $T$ is assigned as $T_{n-1} = K_n$ where $0 \leq n \leq 6$. The key schedule of LEA-192 is expressed as the following:

$$
T_{0}^{i+1} \leftarrow ROL_{1}(T_{0}^{i} \oplus ROL_{i}(\delta_{i \mod 6}))
$$

$$
T_{1}^{i+1} \leftarrow ROL_{3}(T_{1}^{i} \oplus ROL_{i+1}(\delta_{i \mod 6}))
$$

$$
T_{2}^{i+1} \leftarrow ROL_{6}(T_{2}^{i} \oplus ROL_{i+2}(\delta_{i \mod 6}))
$$

$$
T_{3}^{i+1} \leftarrow ROL_{11}(T_{3}^{i} \oplus ROL_{i+3}(\delta_{i \mod 6}))
$$

$$
T_{4}^{i+1} \leftarrow ROL_{13}(T_{4}^{i} \oplus ROL_{i+4}(\delta_{i \mod 6}))
$$

$$
T_{5}^{i+1} \leftarrow ROL_{17}(T_{5}^{i} \oplus ROL_{i+5}(\delta_{i \mod 6}))
$$

$$
RK^{i} \leftarrow (T_{0}^{i}, T_{1}^{i}, T_{2}^{i}, T_{3}^{i}, T_{4}^{i}, T_{5}^{i})
$$

3.3.2.4 Key Schedule for 256-bit Key

The key state $T$ is assigned as $T_{n-1} = K_n$ where $0 \leq n \leq 8$. The key schedule of LEA-256 is expressed as the following:

$$
T_{6i}^{i+1} \mod 8 \leftarrow ROL_{1}(T_{6i}^{i} \mod 8 \oplus ROL_{i}(\delta_{i \mod 8}))
$$

$$
T_{6i+1}^{i+1} \mod 8 \leftarrow ROL_{3}(T_{6i+1}^{i} \mod 8 \oplus ROL_{i+1}(\delta_{i \mod 8}))
$$

$$
T_{6i+2}^{i+1} \mod 8 \leftarrow ROL_{6}(T_{6i+2}^{i} \mod 8 \oplus ROL_{i+2}(\delta_{i \mod 8}))
$$

$$
T_{6i+3}^{i+1} \mod 8 \leftarrow ROL_{11}(T_{6i+3}^{i} \mod 8 \oplus ROL_{i+3}(\delta_{i \mod 8}))
$$

$$
T_{6i+4}^{i+1} \mod 8 \leftarrow ROL_{13}(T_{6i+4}^{i} \mod 8 \oplus ROL_{i+4}(\delta_{i \mod 8}))
$$

$$
T_{6i+5}^{i+1} \mod 8 \leftarrow ROL_{17}(T_{6i+5}^{i} \mod 8 \oplus ROL_{i+5}(\delta_{i \mod 8}))
$$

$$
RK^{i} \leftarrow (T_{0}^{i}, T_{1}^{i}, T_{2}^{i}, T_{3}^{i}, T_{4}^{i}, T_{5}^{i})
$$
3.3.3 Encryption Procedure

The iterations of LEA-128/192/256 is 24, 28, and 32 rounds respectively. Figure 3 which shows the round function of LEA. At the beginning of the encryption the intermediate state $X$ is set as $X_n^0 = P_n$ where $0 \leq n \leq 4$. The following round function is executed $r$ times.

$$X_0^{i+1} \leftarrow ROL_9((X_0^i \oplus RK_0^i) \boxplus (X_1^i \oplus RK_1^i))$$
$$X_1^{i+1} \leftarrow ROR_5((X_1^i \oplus RK_2^i) \boxplus (X_2^i \oplus RK_3^i))$$
$$X_2^{i+1} \leftarrow ROR_5((X_2^i \oplus RK_4^i) \boxplus (X_3^i \oplus RK_5^i))$$
$$X_3^{i+1} \leftarrow X_0^i$$

The final ciphertext is $C_n = X_n^r$ where $0 \leq n \leq 4$.

Figure 4: Round function of LEA
Chapter 4: Implementation

4.1 Overview

For performance analysis, we have chosen AES to be compared with LEA since AES is the chosen standard by The National Institute of Standards and Technology (NIST) in 2000 and it is most widely used cipher because of its good performance. Furthermore, based on Table 3, if we removed the fact that it is vulnerable to biclique cryptanalysis, it will be the most powerful candidate to LEA.

In the implementation we have used LEA-128 block cipher and AES-128 block cipher both have same block size and key size. The encryption algorithms were implemented in the body sensor network in JavaScript language. The readings of vital sign are encrypted then sent to mobile. After that, the readings are decrypted then showed to the patient. Therefore, confidentiality, privacy and integrity are provided to the patient’s records by implementing encryption algorithm to the data that is being collected by WBAN. The readings that we have in the implementation is heart rate data and the Microcontroller that we used is 32-bit CPU.

4.2 Device and Experiment Environment

We have used the 32-bit Intel Curie Microcontroller as a body sensor hardware device. The Pulse Sensor for heart rate readings. The Eclipse as an integrated development environment tool for software development. The program of e-Health monitoring is written in JavaScript. The Emscripten Low Level Virtual Machine (LLVM) to compile C and C++ code into JavaScript. The Johnny-Five platform to control the Microcontroller using JavaScript.
4.2.1 Intel Curie Microcontroller

The Intel and Arduino has collaborated to design Intel Curie Microcontroller in Arduino 101/Genuino 101 (Arduino). The board has a Low power Intel Microcontroller with onboard a Bluetooth LE capabilities and a 6-axis accelerometer/gyro. The module contains two tiny cores, an x86 (Quark) and a 32-bit ARC architecture core, both clocked at 32MHz. The board operation voltage and DC current per I/O is 3.3 V and 20 mA respectively (Arduino). It is protected against 5 V overvoltage and it is connected to PC using a USB connector for serial communication as it shows in Figure 5. The Intel compiles the uploaded sketches through the Arduino Software (IDE).
As it shows in Figure 5, for the implementation the Genuino 101 board is connected to PC using USB and the StandardFirmataPlus sketch was uploaded from the Arduino Software IDE. The Firmata protocol is used to communicate with microcontroller from software on a host computer (Bocoup, 2012).

4.2.2 Pulse Sensor

In Figure 5 it shows the Pulse Sensor which is used for sensing reliable heart rate readings with amplification and noise cancellation circuitry (Sensor). Also, it is powered with 4 mA current draw at 3.3 V. The Pulse Sensor is connected to the board using 3 pins. The red wire is connected to 3.3 V, the black wire is connected to GND and the purple wire is connected to A0 for the analog signal (Sensor).
4.2.3 Eclipse

Eclipse is an integrated development environment (IDE) tool that is used as a workspace for developers to develop applications in different programming languages and architecture (Foundation, 2016).

The Genuino 101 board was programmed using the Eclipse Mars.2 version release 4.5.2. The developed application was programmed to read the heart rate from the pulse sensor that is connected in the Genuino 101 and then encrypt the data using the cipher algorithms. Both ciphers were imported in the program as library. Figure 7 shows the pseudo code of the overall implementation.

```
Import AES and LEA as libraries to the code
Begin
  Bluetooth Low Energy is active, waiting for connections
  The Microcontroller connects to a mobile using Bluetooth Low Energy
  if connected
    while connected
      Check the heart rate measurement
      Encrypt Data with either AES or LEA
      Send the encrypted data to Mobile
      Decrypt Data with the algorithm that has been used
      Update the sketch with the heart rate measurement
    end while
  else
    Disconnected from Mobile
  end if
end
```

Figure 7: Pseudo code of the overall implementation

The program was written in JavaScript language. The reason to choose JavaScript as the language for the software of e-Health monitoring system, because it is a high level language that enables users to write easily desktop and mobile
applications with less logical errors. The following Figures contain the details of the code in JavaScript.

```javascript
var aesjs = require('aes-js');

var leajs = require('./lea.js');
```

Figure 8: Import AES and LEA algorithms as libraries to the code

```javascript
board.on("ready", function() {

    var sensor = new five.Sensor("A0");

    sensor.scale(0, 100).on("change", function() {

        var heartrate = this.value;

        console.log(heartrate);

    });

});
```

Figure 9: Reading the heart rate from pulse sensor

```javascript
var aes = new aesjs.ModeOfOperation.ebe(key, iv);

var encryptedBytes = aes.encrypt(textAsBytes);

console.log(encryptedBytes);
```

Figure 10: Encrypting the data using AES algorithm
var leaEncryption = lea.js.cwrap('LEA_EncryptBlk', 'number', ['array']);

var encryptedBytes2 = leaEncryption(textAsBytes, key);

console.log(encryptedBytes2);

Figure 11: Encrypting the data using LEA algorithm

4.2.4 Emscripten

Emscripten (Emscripten, 2015) is an Low Level Virtual Machine (LLVM) based compiler that can easily compiles C and C++ into highly-optimizable JavaScript.

Also it can compile codes of other languages to be translated to LLVM bitcode then to JavaScript. It saves time from manually converting native code into JavaScript. It is useful that developers can use many thousands of pre-existing libraries in C/C++ into their applications.

As it presented in Figure 13, to build the JavaScript version of C/C++ code, we specified the C/C++ file name with its extension (either .c or .cpp) then the output name follow with the .js to produce a JavaScript file. Moreover, to make sure that the function in C/C++ file remain available through the conversion, EXPORTED_FUNCTIONS must be added to the command line then followed with the function name.
Figure 13: Emscripten Command Prompt

Figure 14: The JavaScript output of LEA encryption algorithm
4.2.5 Johnny-Five

Johnny-Five (Bocoup, 2012) is a JavaScript platform that is developed at Bocoup. Johnny-Five holds many APIs that can communicate with any hardware platform to execute different kind of projects. These APIs can be used after uploading the Firmata Protocol into the Microcontroller via Universal Serial Bus (USB). In the implementation, after uploading the StandardFirmataPlus sketch into the Genuino 101 board, the Johnny-Five start to communicate between the PC and the board.

To add Johnny-Five into the application of e-Health monitoring system the was written in JavaScript, first it must be installed then imported as a library to the code as it shows in Figure 15 and 16.

![Figure 15: Install the Johnny-Five module](image)

```javascript
var five = require("johnny-five");
```

![Figure 16: Import Johnny-Five as a library to the code](image)
Chapter 5: Performance Analysis

5.1 Overview

We evaluated the performance of AES and LEA Block ciphers on Intel Core i7-3517U powered by 1.90 GHz with 4-GB RAM and 17 Watt. We used 64-bit Windows 10 as an operating system and Eclipse Mars.2 as a workspace to program an e-Health monitoring system using JavaScript and Johnny-Five platform. We used Emscripten 1.35 as a LLVM C/C++ compiler to JavaScript. We have analyzed the performance by measuring the execution time and the energy consumption of both encryption algorithms. For testing purposes to do the analysis, the output of the console log was printed out in a file. The total captured data was 100 heart rate readings for each encryption algorithm.

5.2 Performance Criteria

Throughput is the rate of successful delivery of a processed data over a communication channel. It was measured as the following:

(equation 1)

\[
\text{Throughput} \quad \left( \frac{\text{bytes}}{\text{seconds}} \right) = \frac{\text{Algorithm size in bytes}}{\text{execution time of the algorithm in seconds}}
\]

On the other hand, energy consumption is the energy that is consumed by the encryption algorithm and it was calculated as the following:

(equation 2)

\[
\text{Energy consumption (Joules or Watt } \times \text{Seconds) = Power of the host } \times \text{ execution time of one iteration of the algorithm}
\]
5.3 Results

In Table 5 it presents the comparison between the average results of implementing AES and LEA for 100 heart rate data. It shows that LEA is half the size of AES and the execution time for LEA is 0.000312 seconds while it is 0.000724 seconds for AES. Consequently, LEA is having a higher throughput than AES as it shows in Table 5, the throughput of LEA and AES are 75011.55 byte/seconds and 49823.12 byte/seconds respectively. Also, LEA consumes less energy than AES.

Table 5: Comparison results between AES and LEA

<table>
<thead>
<tr>
<th></th>
<th>AES</th>
<th>LEA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Code size (Byte)</td>
<td>20000</td>
<td>10000</td>
</tr>
<tr>
<td>Block input size (Byte)</td>
<td>16</td>
<td>16</td>
</tr>
<tr>
<td>Execution time (Second)</td>
<td>0.000724</td>
<td>0.000312</td>
</tr>
<tr>
<td>Throughput (Byte/Second)</td>
<td>49823.12</td>
<td>75011.55</td>
</tr>
<tr>
<td>time of execution of one cycle (Second)</td>
<td>7.24005E-05</td>
<td>1.29925E-05</td>
</tr>
<tr>
<td>Energy consumption (Joules)</td>
<td>0.001231</td>
<td>0.000221</td>
</tr>
</tbody>
</table>

The below charts shows the energy consumption of AES, LEA and a comparison between both.
Figure 17: Energy consumption results of 100 heartrate readings using AES algorithm

Figure 18: Energy consumption results of 100 heartrate readings using LEA algorithm
Figure 19: Energy consumption results of 100 heartrate readings using AES and LEA algorithms

As a result of the implementation, LEA encryption algorithm is more lightweight than AES encryption algorithm. Which makes it more convenient for WBAN since it has a limited memory space. Furthermore, Figure 19 shows that LEA encryption algorithm has low energy consumption than AES algorithm which makes it the best solution for WBAN to monitor e-Health.

WBAN has a limited power source as it shows in Figure 20; therefore, it is a must to implement an energy efficient encryption algorithm in it; so it can process for a long time. It is very dangerous to ignore the energy factor in the solutions of WBAN especially if it is implanted in human body which might result in an overheat kind of situation to the sensor.
5.4 Scenario

With the consideration of the values in Figure 19, the scenario is as the following. If there is a patient with a continuous high level of heart rate activity similar to the level of the 19th heart rate in X-axis of Figure 19. Accordingly, the energy that is consumed for 1 heart rate if it was encrypted with AES is 0.01 joules while it is 0.0005 joules if it was encrypted with LEA. So for 10 heart rates with such heart level of activity, AES will consume 0.1 joules while LEA will only consume 0.005 joules.

Therefore, WBAN will consume less energy if the data was encrypted with LEA and the patient will not need to change the power supply as frequent as if the data was encrypted with AES.

5.5 Limitations

The LEA encryption algorithm has been announced by the Attached Institute of ETRI in 2013 (Hong et al., 2013). Since it is a new cipher, therefore it has not been subject to attacks by the community as much as AES encryption algorithm. Consequently, in future it might be vulnerable to new kind of cryptanalysis.
Additionally, the accuracy of the data that have been collected using the pulse sensor can be different if the heart rate sensor that was used in the implementation has a high quality in reading the activity of the heart.
Chapter 6: Conclusion and Future Work

As a conclusion there is a high need to utilize the modern technology of e-Health monitoring using Wireless Body Area Network (WBAN) for a continuous care of patients with critical conditions. WBAN will collect the vital signs of a patient and send it to any mobile device which is connected to a back end servers and databases that can preserve a patient’s records and provides relevant diagnostic recommendations. In the thesis we proposed a design architecture to ensure confidentiality, privacy and integrity to patient’s collected data from WBAN by implementing an encryption algorithm in the sensor. Due to the limitations of WBAN, the chosen algorithm must be energy efficient and lightweight algorithm. The performance results of implementing LEA and AES showed that LEA is better than AES since it is more lightweight, high execution time, high throughput and less energy consumption.

In future, there is an aim to build a security architecture to cover the rest of the communication for WBAN Architecture. The future architecture will cover the communication between Tier-2 and Tier-3 and the databases that hold patients’ data in the cloud.
References


List of Publications
