

A Novel Approach for Smart Healthcare in Secure Cloud of Things

J.Jancy Clarat¹, S.Elakiya², M.Elakkiya³ and A.Manthra⁴

¹Assistant professor, Department of CSE, Arasu Engineering College, Kumbakonam

²⁻⁴UG Student, Department of CSE, Arasu Engineering College, Kumbakonam
jancyclarat17@gmail.com, Elakkiyamurugesan21@gmail.com

Abstract— Cloud computing is growing trend, cloud computing means storing and accessing data and programs over the internet instead of your computer hard drive .the internet of things is simply “A network of internet connected objects able to collect and exchange data “.COT can increase the network life time ,which improves the quality of the existing services .COT networks can be more efficient and flexible .In this paper proposed cot based using the techniques on Steganography and traitor tracing technique, that will be Sensing to the patient abnormal condition .the conditions are HB,TEM,BP in the these three conditions are monitoring to the patients .The information are receive to the Guardian and Doctor by the alert. That information are stored in cloud computing with efficient manner.

Index Terms— steganography, revocation, traitor tracing, cloud of things, internet of things, cloud computing.

I. INTRODUCTION

With the wide adoption of large-scale Internet services and the increasing amounts of exchanged data, the cloud has become the ultimate resort to cater to the ever-growing demand for storage, providing seemingly limitless capacity, high availability and faster access time. Typically, cloud providers build several large-scale data centers in geographically distributed locations. They then rely on data replication as an effective technique to improve fault-tolerance, reduce end-user latency and minimize the amount of data exchanged through the network. Consequently, effective replica management has become one of the major challenges for cloud providers. In recent years, a large body of work has been devoted to address this challenge and, more specifically, to address the problem of replica placement considering several goals, such as minimizing storage costs, improving fault-tolerance and access delays. However, replica placement schemes may result in a large number of data replicas created or migrated over time between and within data centers, incurring significant amounts of traffic exchange. This might happen in several scenarios requiring the creation and the relocation of a large number of replicas: when a new data center is added to the cloud provider’s infrastructure, when a data center is scaled up or down, when recovering from a disaster or simply when replicas are relocated to achieve performance or availability goals.

II. RELATED WORKS

Stephanie Baker et al [2]:Wei Xiang:Machine learning and the development of a secure yet lightweight encryption scheme for cloud storage .Essentially, it can improve access to healthcare resources whilst reducing



Fig .1 cloud architecture

strain on healthcare systems, and can give people better control over their own health at all times. In fact, there are relatively few disadvantages of remote health monitoring. The most significant disadvantages include the security risk that comes with having large amounts of sensitive data stored in a single database[1].

Rizwana Shaikhet al [4] :the RSA key length means that *encryption* will be four times slower, and *decryption* will be eight times slower. RSA encryption is much faster than RSA decryption. The theory says that for a n -bit key, computational effort for encryption is proportional to n^2 , while effort for decryption is proportional to n^3 . The system aims at providing a high degree of patient privacy by providing security by classifying information on the basis of their sensitivity levels. However, may also raise many security challenges associated with identity management, authentication, access control, trust management.[2]

Aamir Shahzad ,1 Yang Sun Lee et al [3] :the system's security requirements are fulfilled through the implementation of AES algorithm .application programmable interfaces to develop customized applications, on either private or public cloud computing platform.s several challenges, such as to carry the remotely located information and the remote connectivity issues, mainly present in the healthcare systems.

A privacy-aware cloud-assisted healthcare monitoring system via compressive sensing

C. Wang, B. Zhang, K. Ren, J. M. Roveda, C. W. Chen, and Z. Xu[6]

Wireless sensors are being increasingly used to monitor/collect information in healthcare medical systems. For resource-efficient data acquisition, one major trend today is to utilize compressive sensing, for it unifies traditional data sampling and compression. Despite the increasing popularity, how to effectively process the ever-growing healthcare data and simultaneously protect data privacy, while maintaining low overhead at sensors, remains challenging. To address the problem, we propose a privacy-aware cloud-assisted healthcare monitoring system via compressive sensing, which integrates different domain techniques with following benefits. By design, acquired sensitive data samples never leave sensors in unprotected form. Protected samples are later sent to cloud, for storage, processing, and disseminating reconstructed data to receivers. The system is privacy-assured where cloud sees neither the original samples nor underlying data. It handles well sparse and general data, and data tampered with noise. Theoretical and empirical evaluations demonstrate the system achieves privacy-assurance, efficiency, effectiveness, and resource-savings simultaneously.

HCPP: Cryptography based secure EHR system for patient privacy and emergency healthcare

J. Sun, X. Zhu, C. Zhang, and Y. Fang[8]

Privacy concern is arguably the major barrier that hinders the deployment of electronic health record (EHR) systems which are considered more efficient, less error-prone, and of higher availability compared to traditional paper record systems. Patients are unwilling to accept the EHR system unless their protected health information (PHI) containing highly confidential data is guaranteed proper use and disclosure, which cannot be easily

achieved without patients' control over their own PHI. However, cautions must be taken to handle emergencies in which the patient may be physically incompetent to retrieve the controlled PHI for emergency treatment. In this paper, we propose a secure EHR system, HCPP (Healthcaresystem for Patient Privacy), based on cryptographic constructions and existing wireless network infrastructures, to provide privacy protection to patients under any circumstances while enabling timely PHI retrieval for life-saving treatment in emergency situations. Furthermore, our HCPP system restricts PHI access to authorized (not arbitrary) physicians, who can be traced and held accountable if the accessed PHI is found improperly disclosed. Last but not least, HCPP leverages wireless network access to support efficient and private storage/retrieval of PHI, which underlies a secure and feasible EHR system.

Patient controlled encryption: Ensuring privacy of electronic medical records

J. Benaloh, M. Chase, E. Horvitz, and K. Lauter[7]

Personal health records are integral to self-managed healthcare, but patient-controlled access comes with serious concerns that require a better balance of personalization, privacy protection, and security controls. The Web extra at <http://youtu.be/yb29cOXeoKY> is an audio recording of Alf Weaver interviewing Jingquan Li about his article "Ensuring Privacy in a Personal Health Record System" and balancing personalization, privacy, and security.

Scalable and secure sharing of personal health records in cloud computing using attribute- based encryption,

M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou[10]

Cloud computing has become an integral part of the operation of health. However, there are major security and privacy issues in terms of accessing medical records from the hybrid cloud environment. In this paper, a new secure hybrid Electronic Health Record system is proposed. In this framework, two efficient encryption methods are combined for fine grained access control and protection of data privacy. Multi-authority and Key-based encryption schemes are used for the encryption of each part of health records after dividing those records using a vertical partitioning method. Multi-authority encryption schemes are primarily used in the Public Domains (PUDs), while Key-based encryption schemes are prevalent in Personal Domains (PSDs). Together, they provide; secure data access and authentication of users. Implementation is facilitated using Windows Azure Cloud Computing platform.

Securing personal health records in cloud computing: Patient-centric and _ne-grained data access control in multi-owner settings,

M. Li, S. Yu, K. Ren, and W. Lou[5]

PHR(Personal health Record) is a model which is using for exchange the health information of patient. Generally PHR system is operate by the third party for storage purpose like cloud storage purpose. Though there are a lot of concerns over privacy like PHI that can be show to servers & unauthorized users of the third party. Before outsourcing the PHR data, PHR data encryption is very important for the security reasons. In this paper, we are working over enhancing the security of PHR by implementation of DWT that is based over Steganography. Steganography is that process in which information can be hided in a picture. Steganography has the ability of inserting more information into one image. PHR data will be hided in one image by Steganography. In the Steganography encryption & decryption process will be executed by DWT. In this paper, we are working for hiding the PHR data into a single image for the security reasons. For hiding the PHR data into an image, Wavelet based Steganography is proposed in this paper. In the results, Elapsed time and Error rate get reduce up to 80-90%.

The main objective of the work are described as below [1]:

Nowadays, the research in this field is heading towards the integration of Cloud Computing and Internet of Things. This amalgamation is referred to as Cloud of Things (CoT), which is a new paradigm that exploits the integration of two different and popular technologies – the Internet of Things and the Cloud – to promote Future Internet applications. Although both IoT and Cloud are two different and independent technologies, there is a need to integrate them to complement each other and be able to support pervasive and ubiquitous computing. To ensure the data security a concept of traitor tracing and revocation has been used from which the attackers of the medical data can be traced using traitor tracing technique and the traitor has been blocked using the revocation algorithm. The records of the patients are stored using the Steganography technique which ensures the security of the records up to the core.

III. LITERATURE SURVEY

S.NO	PAPER NAME	YEAR	ALGORITHM	MERITS	DEMERITS
1	Securing E-healthcare records on Cloud Using Relevant data	2017	Cryptography algorithm	To attain smooth flow of information within a healthcare infrastructure, Electronic Health Records are used.	Attribute based encryption is used to achieve encryption.
2	Private Predictive Analysis on Encrypted Medical Data	2018	Conventional encryption	possible application scenarios for homomorphic encryption in order to ensure privacy of sensitive medical data.	it makes this prediction while handling only encrypted data
3	Applying Encryption Algorithm for Data Security in Cloud Storage	2018	encryption/decryption algorithm	It provides IT services as on-demand services, accessible from anywhere, anytime and by authorized user.	Data security in cloud storage is a major obstacle limiting its spread.
4	Real-Time Cloud-Based Health Tracking and Monitoring	2012	Classification Algorithm	medical systems are now more efficient and scalable in processing, such as storage and access, the medical information with minimal development costs.	but most of them have a number of limitations, such as network setup and configuration issues;
5	Patient Health Monitoring System Using Cloud Based Processing	2016	Convolution Neural network	Alert signal is sent to caretaker in case of emergency. This system is easy to setup with low power consumption and high performance.	This system uses GSM network so can be used even in rural areas where broadband facility is not available.
6	HealthCare Monitoring and Alerting System Using Cloud Computing	2013	priority ranking algorithm	Keeping in view this scenario we are proposing a health care system which will be integrated with cloud computing.	Due to this issue there is a paradigm shift from need based health monitoring to preventive health monitoring service.
7	Cloud based Intelligent Healthcare Monitoring System	2014	Steganography	The computing device enables the delivery of accurate medical information anytime anywhere by means of internet.	The computing device enables the delivery of accurate medical information anytime anywhere by means of internet.
8	A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security	2013	Encryption algorithm	Encryption can provide a means of securing information.	the art of cryptography has become more complex in order to make information
9	Survey on Integration of Cloud Computing and Internet of Things Using	2017	Machine learning algorithm	Cloud computing provides infinite computation and storage through a shared pool of	the consequential issues regarding reliability, performance, security and

	Application Perspective			resources.	privacy.
10	Internet of Things for Smart Healthcare: Technologies, Challenges, and Opportunities	2017	Machine learning	In terms of short-range communications standards, it was learned that Bluetooth Low Energy .	The most significant drawback of using cloud is that it introduces security risks.

IV. METHODOLOGY

PHP originally stood for personal home page. Its development began in 1994 when the Danish/Greenlandic programmer Rasmus Lerdorf initially created a set of Perl scripts he called 'Personal Home Page Tools' to maintain his personal homepage, including tasks such as displaying his résumé and recording how much traffic his page was receiving. He rewrote these scripts as C programming language Common Gateway Interface (CGI) binaries, extending them to add the ability to work with web forms and to communicate with databases and called this implementation 'Personal Home Page/Forms Interpreter' or PHP/FI. PHP/FI could be used to build simple, dynamic web applications. Lerdorf released PHP/FI as 'Personal Home Page Tools (PHP Tools) version 1.0' publicly on June 8, 1995, to accelerate bug location and improve the code. This release already had the basic functionality that PHP has today. This included Perl-like variables, form handling, and the ability to embed HTML. The syntax was similar to Perl but was more limited and simpler, although less consistent. A development team began to form and, after months of work and beta testing, officially released PHP/FI 2 in November 1997.

A new major version has been under development alongside PHP 5 for several years. This version was originally planned to be released as PHP 6 as a result of its significant changes, which included plans for full Unicode support. However, Unicode support took developers much longer to implement than originally thought, and the decision was made in March 2010 to move the project to a branch, with features still under development moved to trunk.

Changes in the new code include the removal of register_globals, magic quotes, and safe mode. The reason for the removals was that register_globals had given way to security holes, and the use of magic quotes had an unpredictable nature, and was best avoided. Instead, to escape characters, magic quotes may be replaced with the addslashes() function, or more appropriately an escape mechanism specific to the database vendor itself like mysql_real_escape_string() for MySQL. Functions that will be removed in future versions and have been deprecated in PHP 5.3 will produce a warning if used.

PHP currently does not have native support for Unicode or multibyte strings; Unicode support is under development for a future version of PHP and will allow strings as well as class, method, and function names to contain non-ASCII characters.

PHP interpreters are available on both 32-bit and 64-bit operating systems, but on Microsoft Windows the only official distribution is a 32-bit implementation, requiring Windows 32-bit compatibility mode while using Internet Information Services (IIS) on a 64-bit Windows platform. As of PHP 5.3.0, experimental 64-bit versions are available for MS Windows.

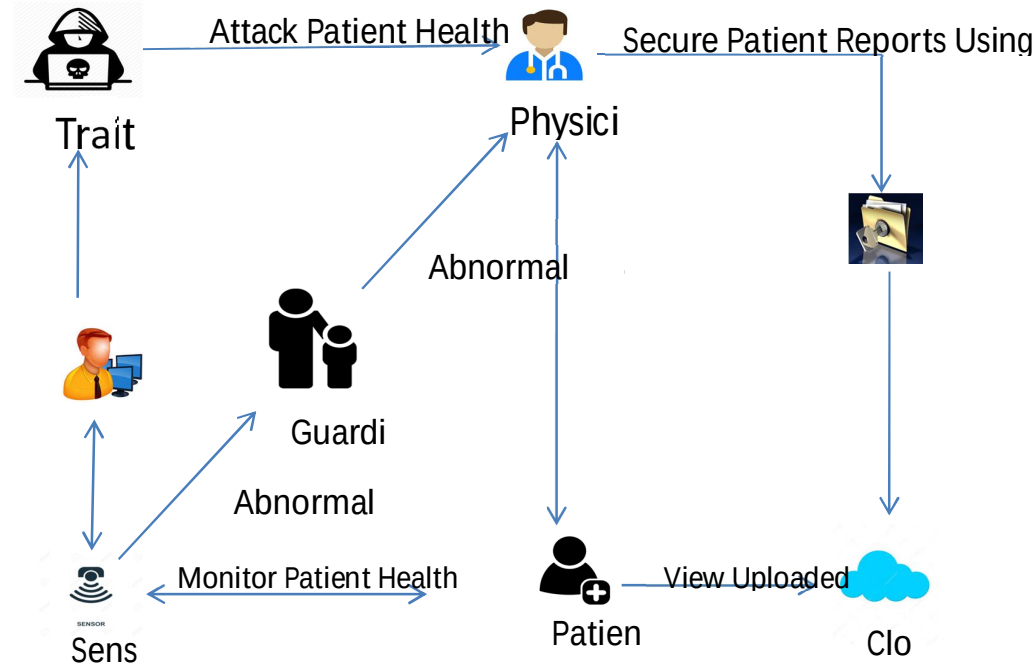
V. SECURITY

The PHP interpreter only executes PHP code within its delimiters. Anything outside its delimiters is not processed by PHP (although non-PHP text is still subject to control structures described within PHP code). The most common delimiters are <?php to open and ?> to close PHP sections. <script language="php"> and </script> delimiters are also available, as are the shortened forms <? or <?=(which is used to echo back a string or variable) and ?> as well as ASP-style short forms <% or <%= and %>. While short delimiters are used, they make script files less portable as support for them can be disabled in the PHP configuration, and so they are discouraged. The purpose of all these delimiters is to separate PHP code from non-PHP code, including HTML.

The first form of delimiters, <?php and ?>, in XHTML and other XML documents, creates correctly formed XML 'processing instructions'. This means that the resulting mixture of PHP code and other markup in the server-side file is itself well-formed XML.

Variables are prefixed with a dollar symbol and a type does not need to be specified in advance. Unlike function and class names, variable names are case sensitive. Both double-quoted (") and heredoc strings allow the ability to embed a variable's value into the string. PHP treats newlines as whitespace in the manner of a free-form

language (except when inside string quotes), and statements are terminated by a semicolon. PHP has three types of comment syntax: /* */ marks block and inline comments; // as well as # are used for one-line comments. The echo statement is one of several facilities PHP provides to output text (e.g. to a web browser). In terms of keywords and language syntax, PHP is similar to most high level languages that follow the C style syntax. if conditions, for and while loops, and function returns are similar in syntax to languages such as C, C++, Java and Perl.



VI. IMPLEMENTATION

Index

```
<?php
session_start();
include("include/dbconnect.php");
include("encrypt_msg.php");
extract($_REQUEST);
$msg="";
$cdte=date("d-m-Y");
$ip = $_SERVER['REMOTE_ADDR'];
/////MAC Address/////
ob_start();
//Get the ipconfig details using system command
system('ipconfig /all');

// Capture the output into a variable
$mycom=ob_get_contents();
// Clean (erase) the output buffer
ob_clean();

$findme = "Physical";
//Search the "Physical" | Find the position of Physical text
$pmac = strpos($mycom, $findme);

// Get Physical Address
```

```

$mac=substr($mycom,($pmac+36),17);
////////////////////////////////////

////alert/////
$q1=mysql_query("select * from request where status=1");
while($r1=mysql_fetch_array($q1))
{

$d=(strtotime($r1['edate'])-strtotime($cdate))/(60*60*24);
    if($d<=3)
    {
        $message="Reminder: Your Medicines available in $d days, so buy your medicines";
        $q2=mysql_query("select * from patient where uname='".$r1['uname']."'");
        $r2=mysql_fetch_array($q2);

        $mobile=$r2['mobile'];
        //echo          '<iframe          src="http://pay4sms.in/sendsms/?token=
b81edee36bcef4ddbba6ef535f8db03e&credit=2&sender=
RandDC&message='.$message.'&number=91'.$mobile.'" style="display:block"></iframe>';
        //mysql_query("update request set status=2 where id='".$r1['id']."'");
    }
}
////////////////////////////////////

if(isset($btn))
{
    $pass1=bin2hex(Encode($pass,"xyz"));
    $uname=strtoupper($uname);
    $query = mysql_query("select * from patient where uname='".$uname.'" && pass='$pass1'");
    $num = mysql_num_rows($query);
    if($num==1)
    {
        $otp=rand(1000,9999);
        mysql_query("update patient set otp='$otp',log_st=0 where uname='$uname'");
        $_SESSION['uname']=$uname;
        $_SESSION['pass']=$pass;
        //header("location:verify1.php");
        ?>
        <script language="javascript">
        window.location.href="verify1.php";
        </script>
        <?php
        }
        else
        {

            $qry1=mysql_query("select * from patient where uname='$uname'");
            $row=mysql_fetch_array($qry1);
            $mobile=Encode(hex2bin($row['mobile']),"xyz");//$row['contact'];
            $message="Someone access your account! IP:$ip,Mac:$mac";
            mysql_query("update patient set log_st=log_st+1 where uname='$uname'");
            if($row['log_st']<2)
            {

                $msg="Invalid User!";
            }
        }
    }
}

```

```

        else
        {
            echo          '<iframe          src="http://pay4sms.in/sendsms/?token=
b81edee36bcef4ddbba6ef535f8db03e&credit=2&sender=
RandDC&message='.$message.'&number=91'.$mobile.'" style="display:none"></iframe>';
        ?>
        <script language="javascript">
            alert("Access Denied!");
        </script>
        <?php
        }
    }
}

?>
<html>
    <head>
        <title><?php include("include/title.php"); ?></title>
        <style type="text/css" title="layout" media="screen">
            @import url("style.css");
            .style1 {color: #000000}
        </style>

        <style type="text/css">
        <!--
        .style4 {color: #FFFFFF; font-weight: bold; }
        -->
        </style>
    </head>
    <div id="content">
        <?php include("include/rightcontent.php"); ?>
        <div id="left">
            <h1>Patient Login </h1>
            <?php if($act=="success") { ?><p class="msg2">Registered Success..</p><?php } ?>
            <form name="" action="" method="post">
                <table width="306" height="164" border="0">
                    <tr>
                        <th align="left" class="bg1" scope="col">Patient ID </th>
                        <th align="left" class="bg1" scope="col"><input type="text" name="uname"></th>
                    </tr>
                    <tr>
                        <th align="left" class="bg1" scope="col">Password</th>
                        <th align="left" class="bg1" scope="col"><input type="password" name="pass"></th>
                    </tr>
                    <tr>
                        <th align="left" class="bg2" scope="col">&nbsp;</th>
                        <th align="left" class="bg2" scope="col"><input type="submit" name="btn"
value="Login"></th>
                    </tr>
                    <tr>
                        <th align="left" class="bg2" scope="col">&nbsp;</th>
                        <th align="left" class="bg2" scope="col"><a href="register.php">Register here </a></th>
                    </tr>
                </table>
                <p class="msg"><?php echo $msg; ?></p>
            </form>

```

<p> </p>
 <div class="col"><div class="fcol"></div>
 </div>

VII. KEY GENERATION ALGORITHM

(A^*, MK, PK) : Except for the attributes which are in A^* (suppose that can be checked efficiently), if the negation of remaining attributes are not the negated attributes of $N(S^*)$, this algorithm will generate the private components for user with which the users can decrypt the ciphertext and obtain the data. By utilizing the LSSS to obtain the shares $\{\lambda_i\}$ of the secret α . We also select a $r_i \in \mathbb{Z}_{p1}$ for each i . For each i , x_i is positive, we have: $D(1)_i = g^{\lambda_i} \cdot T(x_i)^{r_i}$, $D(2)_i = g^{r_i}$. The fine-grained attribute revocation performs under the set of positive attributes. At first, choose t, ξ_i from $\mathbb{Z}_{p1}$ and Y_0 from G_{p3} randomly. Then compute: $D(3)_i = g^{tY_0}$, $D(4)_i = g^{at+c} ID_{\mu_i+ti\xi_iY_i,1}$, $D(5)_i = g^{\xi_iY_i,2}$. Then we can achieve the key component for positive attribute x : $D_i = (D(1)_i, D(2)_i, D(3)_i, D(4)_i, D(5)_i)$. For each i , x_i is negated, we have: $D(6)_i = g^{\lambda_i+r_i}$, $D(7)_i = V(x_i)^{r_i}$, $D(8)_i = g^{r_i}$. Then we can get the key component for negated attribute x_0 : $D_i = (D(1)_i, D(2)_i, D(6)_i, D(7)_i, D(8)_i)$. For all of the shares i , the private key D for decryptor to decrypt the ciphertext is made up of D_i . To encrypt a message $M \in G_2$ under a set of attributes, the sender chooses a random value $s \in \mathbb{Z}_p$, and compute ciphertext E with the following steps: (1) $E_1 = (g_1, g_2)$; (2) $E_2 = g^s$; (3) $\{E_3 = T(s_i)\}_{i \in A}$; (4) Current time tt ; (5) Ciphertext $E = (E_1, E_2, \{E_3\}_{i \in A}, tt)$.

VIII. CONCLUSION AND FUTURE WORK

Cloud and IoT are extensively applied in several information technology applications such as healthcare and smart cities. However, reliable CoT-based services – particularly, highly delay-sensitive services such as Healthcare – require energy-efficient CoT architectures. This paper surveyed CoT architectures, platforms, and their implementation in Healthcare. Furthermore, the paper explained the CoT related issues, in brief, since it mainly investigated the energy efficiency issues with the more relevant proposals in detail. This investigation showed that the majority of the proposals were not concerned about energy efficiency when dealing with IoT Cloud scenarios. Therefore, efficient solutions for obtaining energy efficiency in both data processing and transmission are still required. Moreover, the new solutions should balance the trade-offs amongst energy efficiency, quality of service (QoS), and performance. A future work will be an energy-efficient CoT-based model for Healthcare monitoring in different scenarios such as in-home and mobile patients. Specifically, our future work will propose an energy-aware allocation strategy for such application scenarios.

REFERENCES

- [1] Australian Institute of Health and Welfare, "Australia's Health," 2014. [Online].
- [2] S. Patel, H. Park, P. Bonato, L. Chan, and M. Rodgers, "A review of wearable sensors and systems with application in rehabilitation," *Journal of Neuroengineering and Rehabilitation*, vol. 9, no. 21, 2012.
- [3] H. Qi, S. S. Iyengar, and K. Chakrabarty, "Multi-resolution data integration using mobile agents in distributed sensor networks," *IEEE Transactions on Systems, Man and Cybernetics Part C: Applications and Rev.*, vol. 31, no. 3, pp. 383-391, 2001.
- [4] R. Rajagopalan, C.K. Mohan, K. Mehrotra, and P.K. Varshney, "Multiobjective mobile agent routing in wireless sensor networks," *Proc. IEEE congress on Evolutionary Computation*, vol. 2, 2005.
- [5] L. Tang and W. Xianpeng, "A hybrid multiobjective evolutionary algorithm for multiobjective optimization problems," *IEEE Trans. on Evolutionary Computation*, vol. 17, no. 1, 2013, pp. 20-45.
- [6] W.R. Heinzelman, A.P. Chandrakasan, and H. Balakrishnan, "An application-specific protocol architecture for wireless microsensor networks," *IEEE Trans Wireless Communications*, October 2002, pp. 660-670.
- [7] O. Younis and S. Fahmy, "HEED: a hybrid, energy-efficient, distributed clustering approach for ad hoc sensor networks," *IEEE Transactions on Mobile Computing*, vol. 3, no. 4, Dec 2004, pp. 366- 79.
- [8] S. Lindsey, C. Raghavendra, and K.M. Sivalingam, "Data gathering algorithms in sensor networks using energy metrics," *IEEE Trans. Parallel and Distributed Systems*, vol. 13, no. 9, September 2002, pp. 924-935.
- [9] T. Watteyne, I. Aug'e-Blum, M. Dohler, and D. Barthel, "Anybody: a self-organization protocol for body area networks," in *Proceedings of the ICST 2nd international conference on Body area networks*, ser. BodyNets '07. ICST, Brussels, Belgium, Belgium: Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, 2007, pp. 6:1-6:7.
- [10] B. Lo and G. Yang, "Key technical challenges and current implementations of body sensor networks," *Proc. 2nd International Workshop on Body Sensor Networks (BSN 2005)*, 2005.

- [11] S. M. Riazul islam, daehan kwak, m. Humaun kabir, m. Hossain, and kyung-sup kwak, "the internet of things for health care: a comprehensive survey," *ieee access*, vol. 3, pp. 678–708, 2015.
- [12] A. Sawand, S. Djahel, z. Zhang, and f. Nait-abdesselam, "multidisciplinary approaches to achieving efficient and trustworthy ehealth monitoring systems," 2014 *ieee/cic international conference on communications in china, iccc 2014*, pp. 187–192, 2015.
- [13] Koubaa and e. Shakshuki, "cloud of things: integration of iot with cloud computing," *robots and sensor clouds*, vol. 36, pp. 77–94, 2015.
- [14] S. Distefano, g. Merlino, and a. Puliafito, "enabling the cloud of things," *proceedings - 6th international conference on innovative mobile and internet services in ubiquitous computing, imis 2012*, pp. 858–863, 2012.
- [15] A. Botta, w. De donato, v. Persico, and a. Pescapé, "integration of cloud computing and internet of things: a survey," *future generation computer systems*, vol. 56, pp. 684–700, 2016.