International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 06 Issue: 07 | July 2019 www.irjet.net p-ISSN: 2395-0072

Cloud Data Authentication for Health Monitoring System Using IoT Technology

Sandeep Kumar DC[1], Dr. M.N. Sreerangaraju[2]

[1]*M.Tech student, Dept of ECE, Bangalore Institute of Technology*
[2]*Professor, Dept of ECE, Bangalore Institute of Technology*

Abstract - *The sensors which are sensitive in nature data is generated and heterogeneous in nature. Cloud-server is maintained by various service provider by the internet. Data which will of be transmitted have the mutual authentication between server and the wireless sensor networks. The essential objective was to build up a solid patient observing framework utilizing IoT so that the doctors monitor their patients, who are either hospitalized or at home utilizing an IoT based incorporated social insurance framework with the perspective on guaranteeing patients are thought about better. A cell phone based remote social insurance checking framework was created which can give ongoing on the web data about physiological states of a patient for the most part comprises of sensors, the information procurement unit, microcontroller (i.e., Arduino), and customized with a product (i.e., JAVA).The comprehensively utilized Real-Or-Random(ROR) model based completed an unmistakable close examination for the correspondence and tally costs close-by security and worth highlights which shows its ampleness on the other hand with the other existing plans of its portrayal.*

***Key Words*: Data Authentication, IoT, spo2 sensor microcontroller, heart rate sensor.**

1. INTRODUCTION

Distributed computing and Internet of Things (IoT) are two promising innovations which have picked up a great deal of consideration in the ongoing years. The two innovations can be received to assemble significant parts of things to come Internet .The Cloud IoT worldview is considered as a worldview where both cloud and IoT can be incorporated together to give better administrations including the social insurance applications utilizing the wearable gadgets..

1.1 SYSTEM MODEL

Authentication

Authentication is used by a server when the server needs to know exactly who is accessing their information or site. Authentication is used by a client when the client needs to know that the server is system it claims to be. In authentication, the user or computer has to prove its identity to the server or client. Usually, authentication by a server entails the use of a user name and password. Other ways to authenticate can be through cards, retina scans, voice recognition, and fingerprints. Fig1 shows the architecture for smart wearable devices-based healthcare system.

Authorization

Authorization is a process by which a server determines if the client has permission to use a resource or access a file. Authorization is usually coupled with authentication so that the server has some concept of which the client is that is requesting access. The type of authentication required for authorization may vary; passwords may be required in some cases but not in others.

Encryption

Encryption involves the process of transforming data so that it is unreadable by anyone who does not have a decryption key. The Secure Shell (SSH) and Socket Layer (SSL) protocols are usually used in encryption processes. All data in SSL transactions is encrypted between the client (browser) and the server (web server) before the data is transferred between the two. All data in SSH sessions is encrypted between the client and the server when communicating at the shell.

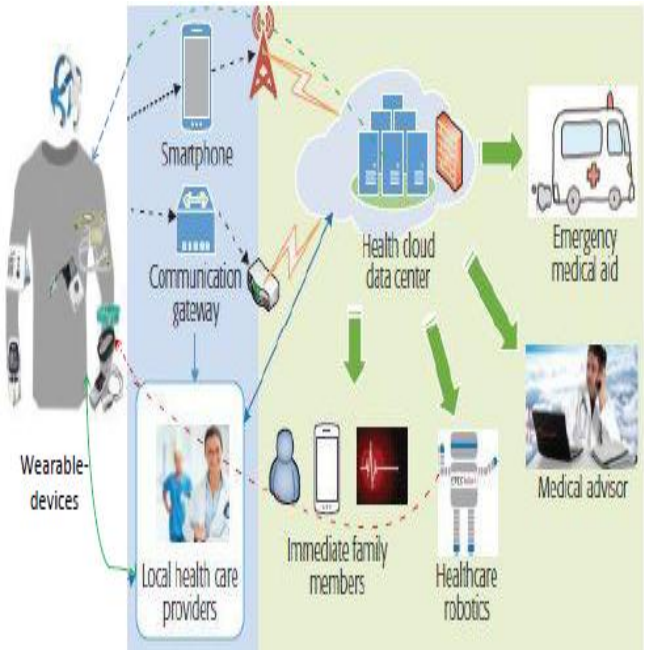


Fig1. Architecture for a smart wearable devices-based healthcare system

1.2 THREAT MODEL

Hazard showing is a method for overhauling framework security by recognizing goals and vulnerabilities, and a short time later describing counter measures to thwart, or ease the effects of, risks to the structure. In this system we are using DY threat model properties:

Stateless parties: The basic on the sensible get-togethers is that they are stateless: the messages transmitted by a party at each development of the show are a segment of their beginning information and the message they essentially got.

Simultaneous execution: The enemy can begin a tracking number of show executions, including diverse blueprints of social affairs, where every player can participate in several synchronous executions.

Open key cryptography and foundation: It is recognized that an open table (X,Ex) containing the name and open key of each client is wholeheartedly accessible. The fundamental learning of every client contains this table; despite the client confuse unscrambling key Dx.

In such way, the model considered here is more far reaching than the computational model considered at the time, which concentrated on single show execution. The computational cryptography framework began watching out for the important issue of simultaneousness.

2. MOTIVATION

It is difficult for the clinics, hospitals and healthcare organizations/institutes to provide free services including free hospitalization charges due to the rise in the cost of medical expenses. To reduce the hospitalization costs and to save hospitalization time, it is essential to design an information system that can manage utilization and efficiency improvement, quality, and most importantly the healthcare system's security .Under such a system, a remote user (e.g., a doctor) can monitor remotely a patient by means of observing the data collected by the wearable devices worn by the patient. However, since the data is private and sensitive, it should not be revealed to an adversary. This necessitates in proposing a cloud-based user authentication scheme to maintain a secret session key among an authorized user and an accessible wearable device after their successful mutual authentication with the help of the CoT C.

Table -1 Description of the symbols.

Symbol	Description
BRC	BigData Registration center
CoTC	Cloud of things Center
SNj	Wearable sensor
Ui	User

3. PROPOSED AUTHENTICATION

The proposed arrangement includes four phases, to be explicit: 1) setup 2) enlistment action 3) login and 4) dynamic wearable sensor extension. For protection of replay ambush, we apply the current timestamps of the structure. To suit this, all the individuals in the framework are synchronized with their timekeepers. This supposition that is a reasonable doubt as it is associated in various progressing approval plans. The documentations close by their portrayals recorded in is utilized in the proposed arrangement.

SETUP PHASE

In setup phase 1st we will choose the secret key K for the things / data which are storing in cloud to enhance the security then different master key and identity will be given to the sensor node after that secret key is calculated

$$SKcc - snj = h(K||MKsnj)$$

And there will be corresponding secret credentials for each SNj. And device also selects cryptography collision resistant, where l is the bit length of hash output.

$$h: \{0,1\} * \rightarrow \{0,1\}2$$

Finally cloud things store the information.

REGISTRATION PHASE

Registration phase will be 2 modes one for medical services and other for patient through secure channel and can be done only once.

LOGIN AND AUTHENTICATION PHASE

In this phase both patient and the doctor can be mutually authenticate each other and at the end session key is established between Ui and SNj. By using Ui and SCj an identity and password ID and PW will established.
SCi gives the particular sensor identity.

DYNAMIC SENSOR EXTENSION

For interfacing new wearable sensor node say new SNj , in the existing system all the security action taken place by BRC. All the sensors data will be collected in the dynamic extension SNj new calculation will be applied to the sensor data for security purpose.

4. SECURITY ANALYSIS

Therefore, security testing is to see the dangers in the framework and measure its potential vulnerabilities. It in addition helps in perceiving all conceivable security hazards in the framework and help structures in fixing these issues through coding. ... Costly weakness remediation costs, which are at their apex after creation.

A. MECHANISMS

For the analysis of the security in this project we are using 2 mechanisms

1. ROR model and
2. ECC algorithm

ROR model: Random oracles are typically used as an ideal replacement for cryptographic hash functions in schemes where strong randomness assumptions are needed of the hash function's output. Such a proof generally shows that a system or a protocol is secure by showing that an attacker must require impossible behavior from the oracle, or solve some mathematical problem believed hard in order to break it. The formal security part of the proposed course of action has been delineated with the assistance of the completely adjusted ROR model. In this model, we think about three people, unequivocally a client Ui, and a wearable sensor focus SNj and the CoTC. Data encryption is the main concept in the project because nowadays data hacking became very big issue so for that we are using ROR model. The Medical data parameter is stored in IoT thingspeak platform from thingspeak will download the data file which will be n number of file select the recent file & signature will be applied where file can be read & modified that file will be encrypted. CoTC sends session key to Ui(doctor) where Ui has to login & enter session key generated by CoTC hence recent file will automatically decrypted by ROR model by selecting recent file.

ECC algorithm: Elliptic Curve Cryptography (ECC) is a way to deal with oversees open key cryptography subject to the arithmetical structure of elliptic bends around confined fields. Elliptic bends are in like way utilized in two or three whole number factorization calculations that have applications in cryptography, for example, Lenstra elliptic curve factorization. The major favored position guaranteed by ECC is a more minor key size, decreasing farthest point and transmission necessities, for example that an elliptic bend get-together could give a relative segment of security directed by a RSA-based framework with a gigantic modulus and correspondingly more prominent key – e.g., a 256-bits ECC open key should give comparable security to a 3072-bits RSA open key. Key age is a noteworthy part where we have to deliver both open key and private key. The sender will encode the message with gatherer's open key and the recipient will unscramble its private key. Directly, we have to pick a number 'd' inside the extent of 'n'. Using the going with condition we can deliver the open key.

$$Q = d * P$$

ENCRYPTION

Give 'm' a chance to be the message that we are sending. We need to address this message on the bend. This have all around execution subtleties. All the progression investigates on ECC is finished by an affiliation called certicom.

Consider 'm' has the point 'M' on the curve 'E'. Inconsistently select 'k' from [1 - (n-1)]. Two figure structures will be made enabled it to be C1 and C2.

$$C1 = k*P$$
$$C2 = M + k*Q$$

DECRYPTION

We have to get back the message 'm' that was send to us,

$$M = C2 – d * C1$$

M is the original message, that we have send. How does we get back the message,

$$M = C2 – d * C1$$

'M' can be represented as 'C2 – d * C1'

$$C2 – d * C1 = (M + k * Q) – d * (k * P)$$

(C2 = M + k * Q and C1 = k * P)

$$= M + k * d * P – d * k *P$$ (canceling out k * d * P)

$$= M \text{ (Original Message)}$$

B. SECURITY FUNCTIONALITY

Keep up a vital separation from unapproved access as far as possible and business or individual information (affirmation) Consider structure clients accountable for activities they perform (non-renouncing) Shield a framework from association intrusions and different breaks that effect nature of association .In a perfect world, reasonably finished security instruments will additionally be Simple to oversee Direct to structure clients Interoperable crosswise over application and attempt limits.

In security systems, authentication is distinct from authorization, which is the process of giving individuals access to system objects based on their identity. Authentication merely ensures that the individual is who he or she claims to be, but says nothing about the access rights of the individual.

The mutual authentication among Ui, CoTC and SNj is achieved through the following three cases:

Case1: CoTC checks session key to authenticate Ui.

Case2: SNj checks secret key to authenticate CoTC directly, and session key by Ui from the records and it also validates the match indirectly.

Case3: Ui checks ID and Password to authenticate SNj directly.

To establish the session key and CoTC indirectly therefore, mutual authentication between Ui and SNj is preserved and both the participants Ui and SNj compute the valid session key.

5. BLOCK DIAGRAM

The wellbeing checking sensors are utilized to gather wellbeing related information for example for information procurement. Correspondence should be possible by controller for sending information on web remotely. Information handling has been done at server. All information gathered and accumulated at server point. To get wellbeing related data in reasonable organization it very well may be appeared on site page for example information the executives .The outcomes gathered from

sensor are examined for example in the event that irregular conduct has been distinguished „ at that point crisis plan initiated to advise the Doctor about patient's wellbeing . So it lessens basic conditions in Hospital

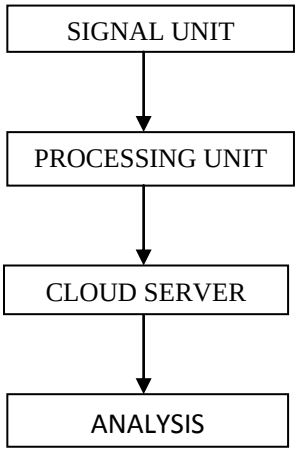


Fig2: flowchart of the information process

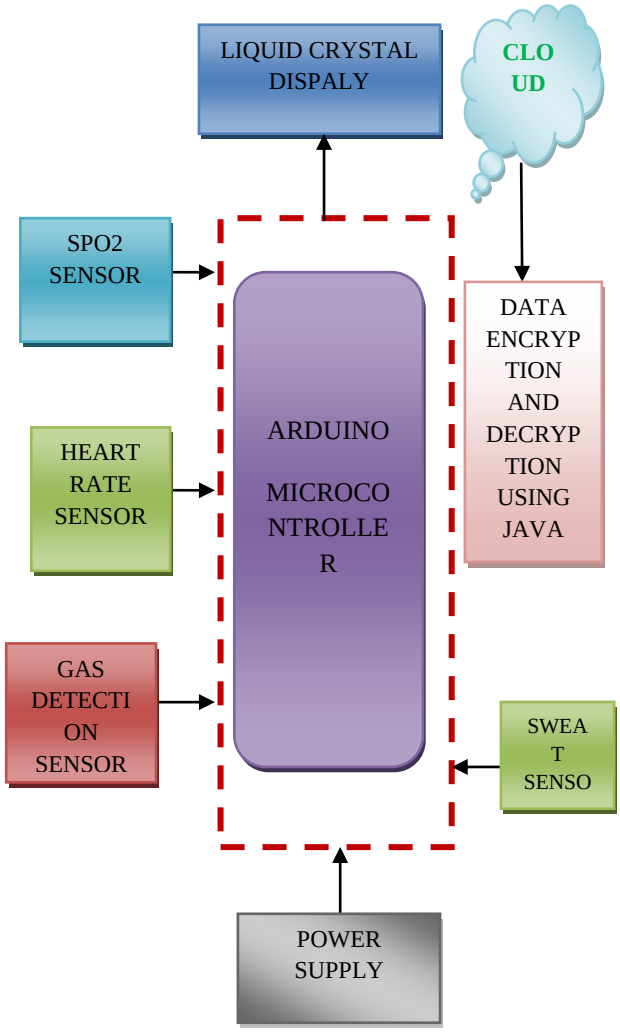


Fig3: Block Diagram

6. COMPONENTS USED

ARDUINO UNO:
Arduino uno is microcontroller dependent on ATMega 328.Simulation is done on Arduino IDE programming. The ATmega 16U2 gives sequential information to the fundamental processor and has a worked in USB fringe. Arduino Uno control link Standard A-B USB cable. It has 14 computerized I/O pins.

PULSE SENSOR:
Heartbeat sensor is intended to give simple yield of heart beat when a finger is set on sensor. It begins working; Driven on top side will begins squinting with every heart beat. To see the sensor yield, yield stick of sensor is associated with controller .The working guideline of sensor depends on light regulation by blood move through nerves at every heart beat.

GAS SENSOR:
Semiconductor sensors are ordinarily used to recognize hydrogen, oxygen, liquor vapor, and unsafe gases, for example, carbon monoxide. Since the sensor must interact with the gas to identify it, semiconductor sensors work over a littler separation than infrared point or ultrasonic indicators. Working with MQ2 Gas Sensor is as follows. The MQ-2 Gas Sensor module distinguishes gas leakage in home and industry. The MQ arrangement of gas sensors utilizes a little warmer inside with an electrochemical sensor. They are delicate to a scope of gasses and are utilized inside at room temperature. The MQ-6 can recognize gas focuses somewhere in the range of 200 to 10000ppm. This sensor has a high affectability and quick reaction time. The sensor's yield is a simple obstruction. The drive circuit is extremely basic; you should simply control the radiator curl with 5V, include a heap obstruction, and interface the yield to an ADC.

SPO2 SENSOR:
At the point when the heart siphons blood, there is an expansion in oxygenated blood because of having more blood. As the heart unwinds, the volume of oxygenated blood likewise diminishes. By knowing the time between the expansion and reduction of oxygenated blood, the beat rate is resolved. It turns out, oxygenated blood ingests progressively infrared light and passes increasingly red light while deoxygenated blood retains red light and passes progressively infrared light. This is the primary capacity of the MAX30100: it peruses the assimilation levels for both light sources and put away them in a cushion that can be perused by means of I2C.

SWEAT SENSOR:
Sweat liquor levels associate with blood liquor levels, new research affirms. The discoveries originate from an examination by US scientists who have made a wearable gadget that animates sweat creation and measures its ethanol fixation at regular intervals. The framework could be

created to follow significant analytics like hormones, or pharmaceuticals, to tell clients how sedates are utilizing in their body continuously. Sensor examines the perspiration. It gauges hydrogen peroxide, which is created when liquor oxidize on the sensor's anode utilizes ethanol.

WIFI-MODEM:
The ESP8266 wifi module is an independent SOC with consolidated TCP/IP convention stack that can offer any controller access to wifi arrange. It utilizes 802.11 b/g/n conventions. Backup control utilization is under 0.1mW. The Fig.4 shows the System Architecture

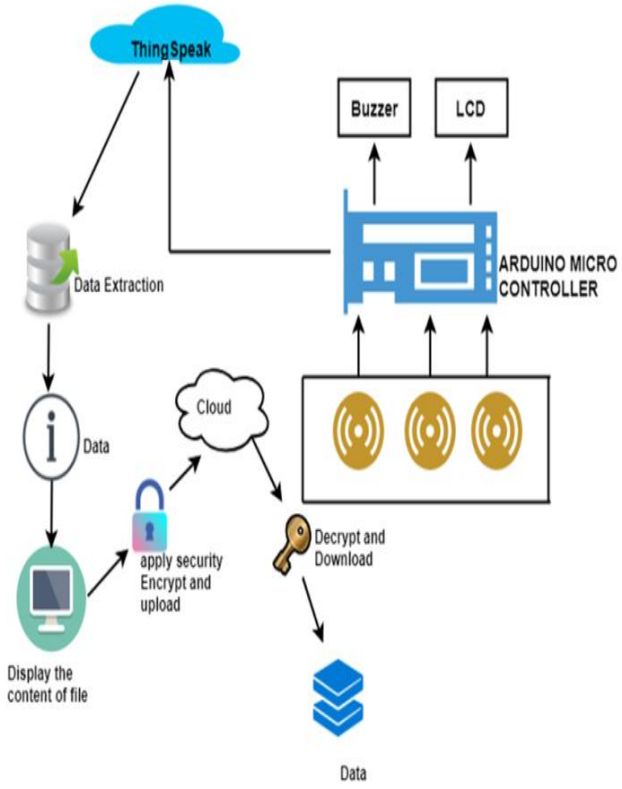


Fig4: System Architecture

IoT CLOUD PLATFORM:
a) Use the Thingspeak stage to send information to the cloud from any Internet-empowered gadget.
b) You would then be able to design activities and alarms dependent on your continuous information and open the estimation of your information through visual instruments.
c) Use the Think talk offers a stage for engineers that empower them to effortlessly catch sensors information furthermore, transform it into helpful data.

7. SOFTWARE SPECIFICATIONS

To be utilized proficiently, all PC programming needs certain equipment parts or other programming assets to be available on a PC. These essentials are known as (PC) framework prerequisites and are frequently utilized as a rule instead of a flat out standard. Most programming characterizes two arrangements of framework necessities: least and suggested. With expanding interest for higher preparing force and assets in more current forms of programming, framework necessities will in general increment after some time. Industry examiners recommend that this pattern has a greater influence in driving moves up to existing PC frameworks than mechanical progressions. Programming necessities manage characterizing programming asset necessities and essentials that should be introduced on a PC to give ideal working of an application. These necessities or requirements are commonly excluded in the product establishment bundle and should be introduced independently before the product is introduced.

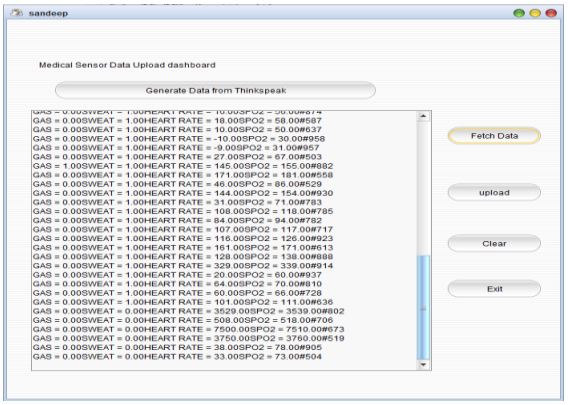
- Java1.4 or higher
- Java Swing – front end
- JDBC –Database connectivity
- UDP-User Datagram Protocol
- TCP-Transmission Control Protocol
- Networking-Socket programming
- ORACLE –Back end
- Windows 98 or higher-Operating System

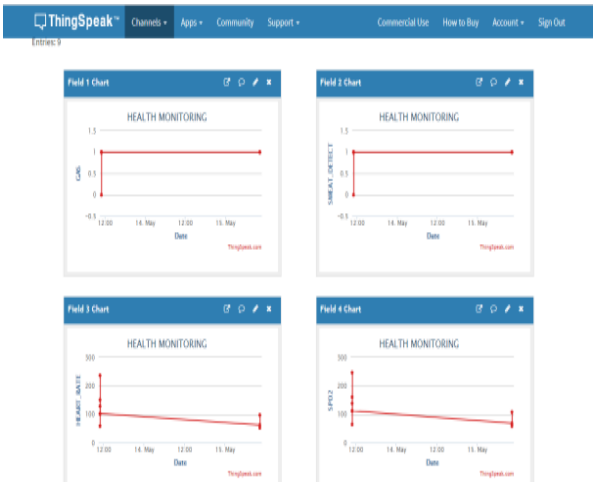
8. RESULTS

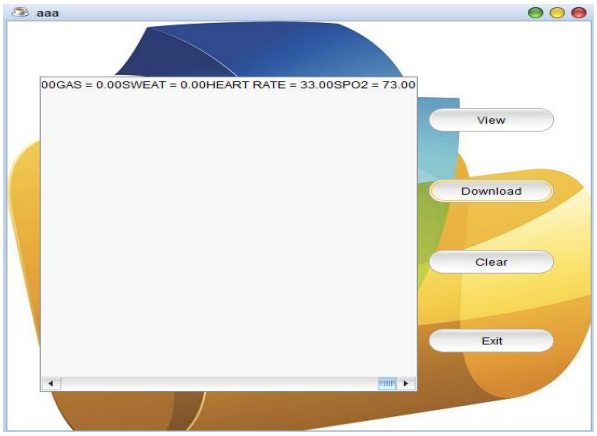
HARDWARE RESULT:

HARDWARE THINGSPEAK RESULT:

SOFTWARE RESULTS:







9. CONCLUSIONS

Conclusion of our work is that it is very much essential to measure the human body parameter which is in critical situation and to analyze the date, without analyzing we can't identify the exact problem and if we analyze the data then we can treat patient more accurately more efficiently and as soon as possible. With the help of IoT we can transmit that analyzed data wirelessly to doctor. In this work, we gave another customer support space in which a genuine customer enrolled at the BRC will most likely ordinarily check with an open wearable sensor center point with the assistance of the CoTC. Around the satisfaction of beneficial normal underwriting among customer and wearable sensor center, both develop a mystery session key that is also used for future secure trades. The formal security using ROR model, which applies signature to file after file will be encrypted & decrypted to doctors.

FUTURE SCOPE

Sound can be added to the contraption with the target that the gadget makes a sound each time a heartbeat is kicked and caution is off for sporadic accomplishment condition. More parameters (like circulatory strain) can be added to the device. In decision instead of the structure can in like way give more than one numbers so past what one client can get crisis message. According to straightforwardness of sensors or progression in biomedical model more parameter can be sense and screen which will improve the sufficiency of the remote watching structure in biomedical field.

The future work includes evaluating the proposed scheme in a real-world wearable devices deployment that will permit us to fine-tune the scheme, if necessary, to offer better performance as well as security. Innovative Designs for Network and Transmission Security, it is observed that network and transmission security is also ignored for S-CI. There must be improved techniques and methods for patient data privacy and security to give efficient, reliable, and continuous transmission

REFERENCES

[1] J. Zhou, Z. Cao, X. Dong, and X. Lin, "Security and privacy in cloud-assisted wireless wearable communications: Challenges, solutions, and future directions," IEEE Wireless Communications, vol. 22, no. 2, pp.136–144, April 2015.

[2] A. K. Das, M. Wazid, N. Kumar, M. K. Khan, K. K. R. Choo, and Y. Park, "Design of Secure and Lightweight Authentication Protocol for Wearable Devices Environment," IEEE Journal of Biomedical and Health Informatics, 2017, DOI: 10.1109/JBHI.2017.2753464.

[3] J. C. S. dos Anjos, M. D. Assuno, J. Bez, C. Geyer, E. P. de Freitas,A. Carissimi, J. P. C. L. Costa, G. Fedak, F. Freitag, V. Markl, P. Fergus,and R. Pereira, "SMART: An Application Framework for Real Time Big Data Analysis on Heterogeneous Cloud Environments," in IEEE International Conference on Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing, Liverpool, UK, Oct2015, pp. 199–206.

[4] J. Wu, H. Li, S. Cheng, and Z. Lin, "The promising future of healthcare services: When big data analytics meets wearable technology, "Information& Management, vol. 53, no. 8, pp. 1020–1033, 2016.

[5] D. Johnson and A. Menezes, "The Elliptic Curve Digital Signature Algorithm (ECDSA)," Technical Report CORR 99-34, Dept. of C &O, University of Waterloo, Canada, August 23, 1999.

[6] M. Wazid, A. K. Das, V. Odelu, N. Kumar, and W. Susilo, "Secure Remote User Authenticated Key Establishment Protocol for Smart Home Environment," IEEE Transactions on Dependable and Secure Computing,2017, DOI: 10.1109/TDSC.2017.2764083.

[7] "Secure Hash Standard," FIPS PUB 180-1, National Institute of Standards and Technology (NIST), U.S. Department of Commerce, April 1995. http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf.Accessed on April 2017.

[8] P. Sarkar, "A Simple and Generic Construction of Authenticated Encryption with Associated Data," ACM Transactions on Information and System Security, vol. 13, no. 4, pp. 1–16, 2010.