International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 06 Issue: 09 | Sep 2019 www.irjet.net p-ISSN: 2395-0072

SECURED MIND UPLOADING METHOD IN WIRELESS BODY AREA NETWORK

N. Sinthuja

Research Scholar, School of Computer Science, Engineering and Application, Bharathidhasan University

---

Abstract - *In recent technologies, mind uploading is the popular technology which is used to transfer the original brain to the artificial computer substrate. Mind uploading is an ongoing active research bringing together ideas from neuroscience, computer science and philosophy. Implementation of wireless Body Area Network (WBAN) monitors the human body environment and their health conditions. The main deprivation of recent survey delivers the problem of data upload from the dead user. Thus the significant data which are in need to others on the data may not be known. In proposed system, a mind uploading whole brain emulation (WBE) system is designed to upload the essential data to the cloud with a secured process of Elliptical Curve Cryptography (ECC). This lends the retrieval of the extreme critical or significant data from the dead user. The WBAN is used to get the sensitive data from the user like memory loss or heartbeats etc. Where, the secured data is uploaded from the user with the cryptographic. Key on the secured data is generated from the Key Generation Center (KGC) and the secret key can ensure the data safety from the data owner side. An end-to-end security implementation is given and the mind uploaded technology used to make human brain on an artificial aspect and saves the lost data or documents.*

Key Words: – **Mind upload, Wireless Body Area Network (WBAN), Whole Brain Emulation (WBE), Elliptical Curve Cryptography (ECC), Artificial Brain, Key Generation Centre (KGC).**

1. INTRODUCTION

Over the last few years, cloud computing has witnessed an enormous technologies towards user to shift their adoptions and promises a significant cost reduction in business environment. Cloud computing infrastructure has a resource oriented premises where the user can be provided with a remote access over the cloud resources. Several prototype applications and industries such as IBM, Google, Amazon and the Elastic computing Platform are used as a cloud environment for the user. According to US National Institute of Standards and Technology (NIST) "Cloud computing is a enabling convenient, on demand network access to shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or cloud provided interaction". But the resources are lively updated by the user to the cloud which acts as a live resource cloud service provider. Sometimes, data loss occurs if the user of the data seems to be unused or dead. The advancement of Information Communication and Technology (ICT) has brought an enormous change in human's life. Wireless Body Area Network is an emerging technology which collects the biological data and it monitor's the health condition of the human. Some data can be critical and sensitive information which needs to be protected, secured in the cloud service. Identification of the user status implemented through the WBAN and the mind upload technology enhances the sensitive data upload to the cloud.

The paper is organized as followed by related works in the chapter III and the proposed system and the architecture is employed in the chapter IV with its specified calculations added through the system. ECC and the KGC steps are defined in the chapter IV. Chapter V makes the analysed result of the security process provided. The future enhancements and the conclusion is discussed in the chapter VI and the references are provided in the last chapter VII.

II. RELATED WORKS

Light weight encryption algorithms for wireless body area network

CH. Radhika Rani1, Lakku Sai Jagan , Ch. Lakshmi Harika 3, V.V. Durga Ravali Amara 4, International Journal of Engineering & Technology, 7 (2.20) page no: 64-66, year 2018.

The WBAN comprise of body sensors during which the energy resources ar restricted and since consumption of energy are additional it's essential to travel for lightweight weight algorithms to produce security and reduce energy consumption.

Lightweight Encryption Algorithm in Wireless Body Area Network for e-Health Monitoring.

Azza Zayed Alshamsi, Ezedin Salem Barka, Mohamed Adel Serhani, 12th International Conference on Innovations in Information Technology (IIT), IEEE,144-150, 2016.

The patient are going to be sporting sensors to sense his/her important signs, like vital sign, pressure, sugar level, temperature, etc. Since patient's information is non-public, the readings are encrypted, victimization. AN energy economical light-weight cryptography formula, to make sure the confidentiality, privacy, and integrity of the patient's information. once the cryptography, the info are going to be transmitted to movable, or the other mobile device.

Security In Wireless Body Area Networks From In-body To Off-body Communications

Muhammad Usman, Muhammad Rizwan Asghar, Imran Shafique Ansari And Marwa Qaraqu.Ieee Access, VolNo: doi 10.1109/Access .2873825, 2016.

Wireless Body body Networks (WBANs) play a significant role in shaping today's health care systems. Given the essential nature of a WBAN in one's health to mechanically monitor and diagnose health problems, security and privacy of those health care systems want a special attention. during this work, initial propose a completely unique four-tier design of remote health observation system so determine the safety needs and challenges at every tier.

Data Security and Privacy in Wireless Body Area Networks

Ming Li and Wenjing Lou. Journal Name(IEEE), Vol No:1536-1284/10, Page No:51-58, 2010.

They two vital knowledge security problems, 1. Dependable distributed data storage and a pair of fine-grained distributed data access management for the sensitive and personal patient medical knowledge are mentioned.

Securing Data Communication in Wireless Body Area Networks Using Digital Signatures.

M. Anwar, A.H. Abdullah, R.A. Butt, M.W.Ashraf, K.N. Qureshi And Fullah, IEEE Access, Vol No: 23, Page No: 50-56, 2018.

This paper, highlight the key problems and challenges associated with knowledge security and privacy in WBANs. The planned knowledge hybrid technique named D-Sign for encrypting and decrypting victimisation digital signatures.

An Efficient Biometric-based Algorithm Using Heart Rate Variability for Securing Body Sensor Networks.

Sandeep Pirbhul, Heye Zhang, Subhas Chandra Mukhopadhyay, Chunyue Li,yumei Wang, Guanglin Li, Wanqing Wu And Yuan Ting Zhang, IEEE, Vol No:15, Page No:15067-15089, 2015.

A device node in BSN delivers major information so, it's terribly important and security. A BSN space supported advanced cryptologic key generation procedures, that not solely demands high resource utilization and computation time, however additionally consumes great amount of energy, power and memory throughout information transmission.

Wireless Body Area Network Security and Privacy Issue In E-healthcare

Muhammad Sherz Asha Malik, Muhammad Ahamed, Tahir Abdullah, Naila Kousarmehak Nigar Shumaila, International Journal Of Advanced Computer Science And Applications,Vol No:9, Page No:209-215, 2018.

In this paper, a primary gift an outline of WBAN, however they utilized for health care watching, its design then highlight major security and privacy necessities and assaults at totally different network layer during a WBAN and a finally bring up numerous cytological algorithms and laws for providing resolution of security and privacy in WBAN.

An Enhanced AES Algorithm Using Cascading Method On 400 Bits Key Size Used In Enhancing The Safety Of Next Generation Internet Of Things

Ritambhara, Alka Gupta, Manjit Jaiswal, International Conference on Computing, Communication and Automation (ICCCA),

IEEE, page no: 422-427, 2017.

Body Node Coordinator Placement Algorithms For Wireless Body Area Networks

Md Tanvir Ishtaique ul Huque, Student Member, IEEE, Kumudu S. Munasinghe, Member, IEEE and Abbas Jamalipour, Fellow, IEEE, DOI 10.1109/JIOT.2366110, IEEE Internet of Things Journal, 2016.

Three totally different completely different BNC(Bayonet Neill - Concelman) placement algorithms considering different options of accessible energy economical routing protocols in a very WBAN. A simulation results show that these algorithms at the side of associate degree acceptable routing protocol will more prolong the network time period.

III. PROPOSED WORK

Our work is related to the process of secured mind uploading of critical or sensitive data, WBAN technology to know the status of the human and Elliptical Curve Cryptography to secure the data uploaded from the artificial brain.

Mind Uploading: Current model of consciousness and neural processing in brain is generally a decentralized adaptive process. If the model of consciousness is true then they could be transferred to a computer incrementally via adaptation. If the question raises that whether it is possible to upload the human brain to computer? The research reveals that "it's extremely difficult but it is possible" says neuroscientist Randal Koene. Human brain cannot able to live forever but because of brain cell may able to live indefinitely do mean humans could live forever. Mind upload has important existential and ethical implications, yet little is known how the ordinary people feel from the artificial brain data upload. The current paper aims to provide the evaluation system of the cognitive factors that explain the people's feeling and reaction for the use of mind upload technology.

Consciousness is currently understood as an epiphenomenon of the brain activity specifically of the cerebral cortex. Unlike an identity, this is a composition of information stored in brain. It is reasonable to understand

the intrinsic property of the human brain. The technology can be made using the Whole Brain Emulation (WBE) technology where it will scan the hypothetical futuristic process of the mental state (including long term memory and self). Computational neuroscience attempts to understand the brain by mathematical and software models of neural systems.

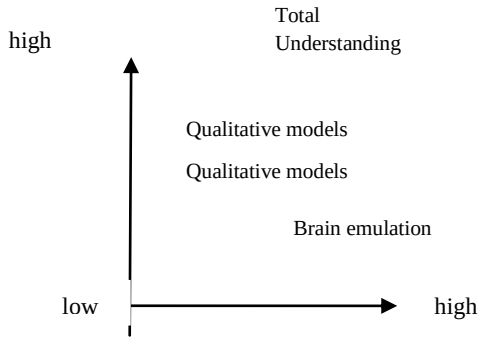


Fig 1 Understanding the function vs Understanding the models

Currently, the models are far simpler than the simpler than the studied system, with the exception of small neural system. Often these models require the simplified parts and the neural networks.

Wireless Body Area Network: A fast developing technology, which provides the patient medical data from the human body vital parameters. This emerged as a promising technology that will revolutionarily seek the way of healthcare of the human called as E-healthcare. Thus the WBAN can be implemented in the process of knowing the user consciousness whether in a state of dead or coma. If the user seems to be in a brain idle state this technology guides to recover the critical or the sensitive data from that user. Such, that it enables the WBAN monitoring system of the human body. The WBAN sensors monitor the user heartbeat and locomotive activity which it delivers the user state. Wireless Body Area Network generally has two types of nodes (i.e) wearable nodes and implantable nodes which work at some certain frequencies. The implantable node works at 400MHz, utilizing the Medical Implantable Communication Systems (MICS) band. WBAN can communicate with the net and other technologies like Zig-Bee, Wi-Fi, Bluetooth, cell system and other Personnel Area Network (PAN) technologies. So this makes a good advantage for WBAN to get communicated with other technologies and upload the critical data in a secured manner.

Microcontroller:

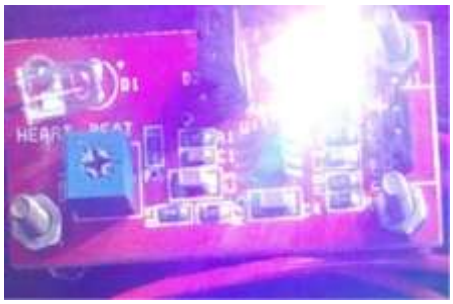
In this system the patient is monitored using the WBAN where the sensors will collect the data from the patient whether he/she is dead or alive. Such that 3 main microcontrollers are implemented they are: fig 2 the diagram represents the overall processing.

Fig 2 the diagram represents the overall processing

- Heartbeat sensor
- PIC16F877

Heart Bear Sensor:

Heartbeat sensor is used to sense the heartbeat of the patient to know that they have high heart rate, low heart rate and dead. This helps the user to know he is dead for mind upload this process is used to know the patient status. Fig 3 Architecture of the heart beat sensor.



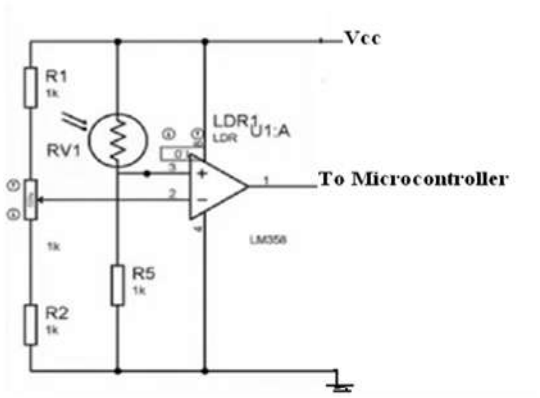
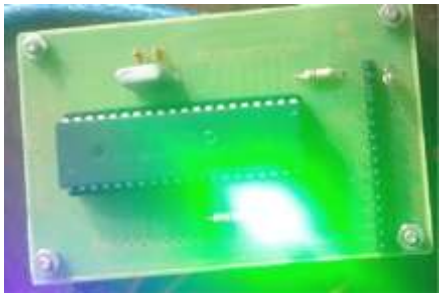


Fig 3 Architecture of the heart beat sensor

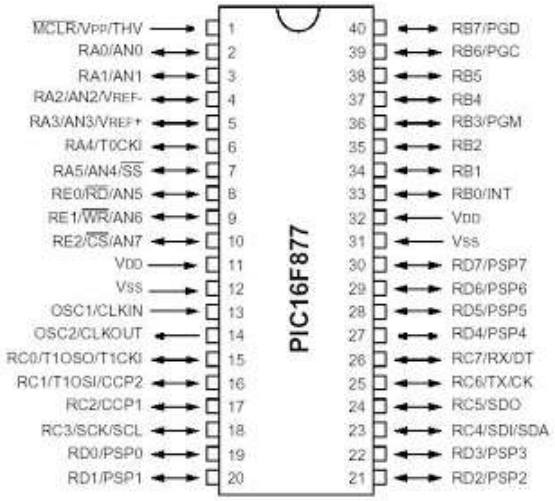
The sensor contains the transmitter and the receiver so that the receiver will receive the patient heart beat and the transmitter will transmits to the user through the PIC microcontroller.

PIC16F877:



These microcontrollers are known as Programmable Interface Controller programmed to carry a vast range of tasks. Thus PIC microcontroller helps to sets the control with a timer limit so that they can collude with the heartbeat sensor to predict the heartbeat within a given time. Fig 4 the diagram represents the pin diagram of the PIC16F877.

Fig 4 the diagram represents the pin diagram of the PIC16F877



Bluetooth

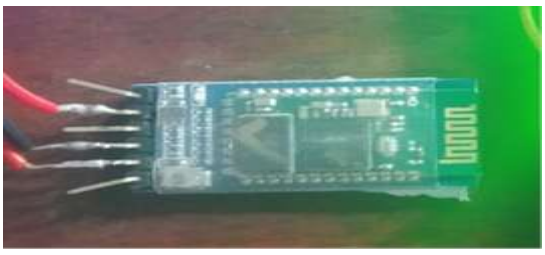


Fig 5 the diagram represents Bluetooth

Bluetooth is a type of microcontroller which is used to connect the device and get the heart beat of the patient. Thus the Bluetooth can connect at 2.4GHz at a baseband. Fig 5 the diagram represents Bluetooth.

Elliptical Curve Cryptography: Elliptical curve cryptography (ECC) may be a public key encoding technique that evolved from elliptical theory that may be wont to produce quicker and smaller scientific discipline keys. Here, the Encryption key is made public and the decryption key is made private where as it is known as asymmetric key cryptographic methods. The particular strategy uses the elliptical curve to secure the encrypted products. Logarithmic process helps us to create the more complex cryptographic technique, where a category called discrete logarithmic value protocols has been modified to get elliptic curve calculations. ECC requires smaller keys compare to the non EC Cryptographic techniques. Short encryption key is the value which is fed into the encryption algorithm to decode an encrypted message. The short key is faster and requires less computing power than the first generation encryption algorithms. An elliptical curve is an algebraic function (y2=x3+ax+b) which looks like a symmetric curve parallel to the x axis when plotted.

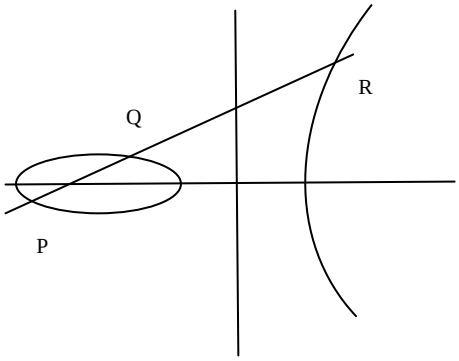


Fig 4 this figure denotes the Elliptical Curve of the x axis which are plotted using the algebraic functions

ECC uses different mathematical properties to achieve the property over RSA algorithm. The easiest way to explain the curve using the mathematical function using three points along the curve (P, Q and R) by knowing two of the points P and Q the other point can be calculated easily. But using the R value the P and Q value cannot be derived.

IV. PROPOSED SYSTEM ARCHITECTURE

System overview

We assume a system which is designed in the way that it can upload the sensitive information to the cloud after the loss of consciousness of the user in a secured manner. The mind loader technology is proposed to upload the critical information in the cloud using the Whole Brain Emulation (WBE). The brain can be simulated, by creating an intelligence machine. Thus the data can be uploaded after the user seems to be idle or the data seems to be in a cold storage. The system is changes with a calculative purpose of hot storage and cloud storage of the cloud data.

However, the system is implemented in a secured way using the Elliptical Curve Cryptography (ECC) which enhances the small key encryption process which overcomes the property. The data can be accessed only by the authorized person and

it will be defined by the user. This architecture implements the process of secure mind upload over cloud using wireless Body Area Network. Here the critical data of an unconscious user will be used in an efficient manner. The user health will be monitored using the sensor where it monitors their heartbeat, motion of the user, pulse, etc. the process can be monitored and accessed through an access point. If the user seems to be unconscious or seems to be brain dead then the critical document can be transferred from the human brain to the Cloud Service Provider (CSP). The main proposed system which has been enhanced here is that the document which are uploaded from the artificial intelligent system will be in a secured manner because to maintain the document in a protected manner from the unauthorized user. ECC algorithm is derived to get the document in an encrypted process with a public key. If the user is known as an authorized user then the Key Generation Center (KGC) where it generates the key to the user who can access the data after it is uploaded.

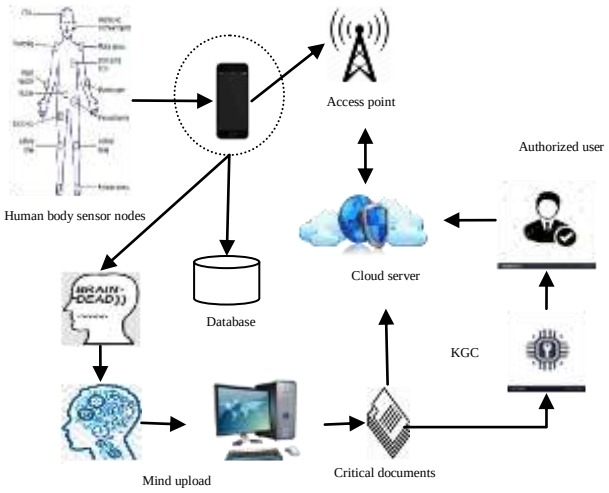


Fig 6 secured mind upload architecture

Brain Models

Over dozen of brain models human brains are modeled using the pathological process from the anatomical chart. Current neuroscientists make research on many organisms to develop a brain model over an artificial intelligent process. Thus it provides a human brain model emulator which is a primitive among the wide range of organisms

a. Primate Brain (human brain)

The explorations on the human brain are one of the relevant models which are used for the WBE technology. The functional models proposed the primate brain enhanced with magnetic resonance and the electric fields of the brain. The artificial emulator is connected through neurons called a node which creates a biological process of the human brain.

Key Generation Center (KGC)

The proposed KGC generates a secret key to encrypt and decrypted resources which are uploaded to the cloud. Most, of the time KGC gets a session key where it acts as a session key shared with each entity. The key information is send to the authorized user so that they can decrypt data and utilize the resources which are shared. The unauthorized user cannot get the shared session key and anyhow it enhances the security issues inside and outside the CSP.

a. Advantages

The main security advantages over the secured key generation is that,

- Key freshness
- Key confidentiality and
- Key authentication

Key Freshness: Key freshness enhances a new key which will be generated to the authorized user so that they can get a key which will be changed when it is newly uploaded. The key can be generated in a random process so that the security implementation is high.

Key Confidentiality: Key confidentiality is that the authorized can only recover the key from the KGC but not by an unauthorized user

Key authentication: Key authentication ensures that the key generated only from the KGC, not by the attacker. Sometimes attacker can generate the key to the user and the data get attacked by the one who generates the attacked key.

b. Key Generation and Distribution

Upon receiving a request from the user, KGC has to generate a secret key and share to the user. KGC needs to send the secret session key in an authenticated manner. Assume that the key requester as {U} and the secret key which added as (xi, yi) for i=1,…….t

The Key Generation process contains five steps

Step 1: The data access user sends a request to the KGC as {u}

Step 2: KGC verifies the user whether they are authorized user or a non authorized user at the secret key generated only to the authorized user xi

Step 3: The user send a random challenge to the KGC as R

Step 4: KGC selects a random secret key with an interpolated polynomial function f(x) with degree t to i=1 which passes through the (t+1) points. It compares the additional points P (0,k) with the functional degree of points which are added for i=0…….t on f(x) the Auth=h(k:u;Rt…. p1) where h is one way hash function. All computations are performed in Zn.

Step 5: For the user the hash function f(0) which are calculated on it polynomial values (xi, yi, XOR Ri) and checks the authentication value is true. The identical values authenticate the Ui the key sent from the KGC process.

c. Discrete Logarithms

The computation of the logarithmic fields added to the ECC to enhance a valuable calculation and efficiency compared to the security of the data resources used.

Sender = gx mod P

Receiver=gy mod P

K= (gy)x mod P

An elliptical curve denotes the field K in a non singular cubic curve in two variables, f(x,y)=0 with a rational point (which the point may be infinity). The field K is usually taken in finite complex numbers, reals, and algebraic extensions of rationales, p addict numbers or infinite fields.

Elliptic Curve Cryptography is a plane curve defined by the sequence of the equation form

Y3=x2+ax+b

The point which is sitting on the top plot of x implants the point of infinity which passes through the vertical curve and both the y axis which is added in the process execution. The scalar point of addition and multiplication is proposed to the curve finite field analysis.

Design implementation:

The mind upload WBAN process is implemented by using the microcontroller connected with a system, an android application to gather the sensed data and to predict the user status.

Fig 6 the diagram presents the implementation work for the WBAN with mind upload security technology

V. RESULTS

A comparative summary of the ECC evaluation makes a comparison of the security analysis among the other cryptographic algorithm. ECC implementation in terms of code bytes and clock timing are given in the table I. The fastest implantation is achieved while encrypting and decrypting the resources using the secret key generated from the KGC.

Table -1: Result Analysis

Symmetric key size (bits)	Diffie Hellman and RSA key size (bits)	Elliptical Curve Cryptography (bits)
80	1024	160
112	2048	224
128	3072	256
192	7860	384
256	15360	521

Table I the comparison table for the key size of each algorithms where ECC acts at a mediator level of bits the fastest encryption process is achieved

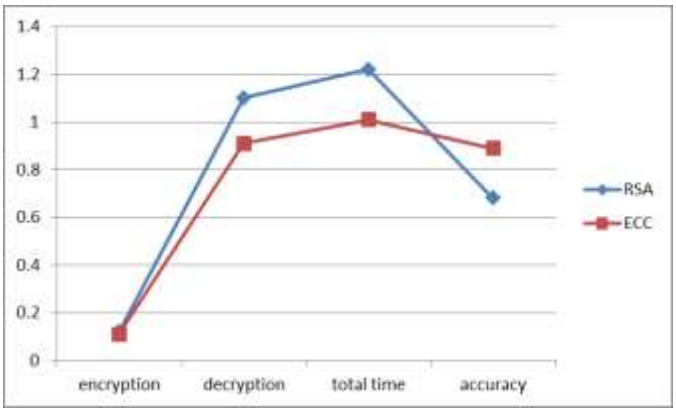


Chart -1: Fig 4 gives a comparison line chart for the security process of the enhanced functionality

VI. CONCLUSIONS

The work which had been presented with a WBAN technology is utilized in an efficient manner. The user resources can be efficiently used even after the user unconsciousness or the user death. The extended research can be analyzed in a way of two technologies (1) monitoring the health condition of the human using the health monitoring nano sensors with the wireless communication technology and (2) the cloud storage providing hot storage or cold storage. If the user data seems to be cold storage over a period of time then the data can be automatically copied or transferred to the authorized person who is the next owner of the critical or sensitive documents utilized. Thus these enhances the utilization of the critical data instead it been loosed without getting authorization from the particular user. The security implications are provided using ECC cryptographic algorithm and the process is analyzed using the algorithmic verification of the finite fields. An obvious area of future research may be usage of the time complexity which is made to analyze the user health and to identify the

cold storage resource in the cloud service provider. Moreover, our current architecture creates an efficient way of time complexity precedence over the security enhancement. Finally from the usability point of view the authorized user can access the mind uploaded data from the user. User can securely handle the resources using Key Generation Center.

REFERENCES

[1] Md. Rownak Hossain and Md. Selim Hossain, "Efficient FPGA Implementation of Modular Arithmetic for Elliptic Curve Cryptography", International Conference on Electrical, Computer and Communication Engineering (ECCE), 7-9 February, 2019

[2] Shubhankar Chaudhary, Ashish Singh, and Kakali Chatterjee," Wireless Body Sensor Network (WBSN) Security and Privacy Issues: A Survey", International Conference on Computational Intelligence & IoT, 2018

[3] Heye Zhang, Subhas Chandra Mukhopadhyay, Sandeep Pirbhulal ,Chunyue Li, Yumei Wang, Guanglin LiShantha A, Renita J and Edna Elizabeth N, Wanqing Wu and Yuan-Ting Zhang, "An Efficient Biometric-Based Algorithm Using Heart Rate Variability for Securing Body Sensor Networks", Sensors 2015

[4] CH. Radhika Rani1 , Lakku Sai Jagan2 , Ch. Lakshmi Harika 3 , V.V. Durga Ravali Amara 4, "Light weight encryption algorithms for wireless body area networks", International Journal of Engineering & Technology, 7 (2.20) (2018)

[5] Shantha A, Renita J and Edna Elizabeth N," Analysis and Implementation of ECC Algorithm in Lightweight Device", International Conference on Communication and Signal Processing, April 4-6, 2019

[6] Amal HAFSA1 , Anissa SGHAIER1 , Mohsen MACHHOUT1 , Jihene MALEK, "A New security Approach to Support the operations of ECC and AES Algorithms on FPGA", 2019 19th international conference on Sciences and Techniques of Automatic control & computer engineering (STA), March 24-26, 2019

[7] M. Anwar , A. H. Abdullah , R. A. Butt , M. W. Ashraf , K. N. Qureshi , F. Ullah," Securing Data Communication in Wireless Body Area Networks Using Digital Signatures", Technical Journal, University of Engineering and Technology (UET), 2018

[8] Muhammad Sheraz Arshad Malik, Muhammad Ahmed, Tahir Abdullah, Naila Kousar, Mehak Nigar Shumaila, "Wireless Body Area Network Security and Privacy Issue in E-Healthcare", International Journal of Advanced Computer Science and Applications, Vol. 9, No. 4, 2018

[9] Muhammad Usman∗ , Muhammad Rizwan Asghar† , Imran Shafique Ansari‡ , and Marwa Qaraqe", "Security in Wireless Body Area Networks: From In-Body to Off-Body Communications", Division of Information and Computing Technology, 2018

[10] Wonjun Ko, Eunjin Jeon, Jiyeon Lee, and Heung-Il Suk," Semi-Supervised Deep Adversarial Learning for Brain-Computer Interface", Department of Brain and Cognitive Engineering,2019