HYBRID ENCRYPTION ALGORITHIM

IN WIRELESS

BODY AREA NETWORKS [WBAN]

Dissertation submitted in fulfilment of the requirements for the Degree of

MASTER OF TECHNOLOGY

In

COMPUTER SCIENCE AND ENGINEERING

By

SAMEER FAROOQ

11501907

Supervisor

Mr. DEEPAK PRASHAR

School of Computer Science and Engineering

Lovely Professional University

Phagwara, Punjab (India)

Month: April Year: 2017

TOPIC APPROVAL PERFORMA

School of Computer Science and Engineering

Program : P172::M.Tech. (Computer Science and Engineering) [Full Time]

COURSE CODE : CSE546 **REGULAR/BACKLOG :** Regular **GROUP NUMBER :** CSERGD0012

Supervisor Name : Deepak Prashar **UID :** 13897 **Designation :** Assistant Professor
Qualification : _____ **Research Experience :** _____

SR.NO.	NAME OF STUDENT	REGISTRATION NO	BATCH	SECTION	CONTACT NUMBER
1	Sameer Farooq	11501907	2015	K1519	9501888017

SPECIALIZATION AREA : Networking and Security **Supervisor Signature:** _____

PROPOSED TOPIC : A novel Security approach in Wireless Body Area Networks

Qualitative Assessment of Proposed Topic by PAC		
Sr.No.	**Parameter**	**Rating (out of 10)**
1	Project Novelty: Potential of the project to create new knowledge	7.60
2	Project Feasibility: Project can be timely carried out in-house with low-cost and available resources in the University by the students.	7.20
3	Project Academic Inputs: Project topic is relevant and makes extensive use of academic inputs in UG program and serves as a culminating effort for core study area of the degree program.	7.00
4	Project Supervision: Project supervisor's is technically competent to guide students, resolve any issues, and impart necessary skills.	7.60
5	Social Applicability: Project work intends to solve a practical problem.	7.40
6	Future Scope: Project has potential to become basis of future research work, publication or patent.	7.40

PAC Committee Members		
PAC Member 1 Name: Prateek Agrawal	UID: 13714	Recommended (Y/N): Yes
PAC Member 2 Name: Pushpendra Kumar Pateriya	UID: 14623	Recommended (Y/N): Yes
PAC Member 3 Name: Deepak Prashar	UID: 13897	Recommended (Y/N): Yes
PAC Member 4 Name: Kewal Krishan	UID: 11179	Recommended (Y/N): Yes
PAC Member 5 Name: Anupinder Singh	UID: 19385	Recommended (Y/N): NA
DAA Nominee Name: Kanwar Preet Singh	UID: 15367	Recommended (Y/N): Yes

Final Topic Approved by PAC: **A novel Security approach in Wireless Body Area Networks**

Overall Remarks: Approved

PAC CHAIRPERSON Name: 11011::Dr. Rajeev Sobti **Approval Date:** 26 Oct 2016

ABSTRACT

I The trend of wireless sensor networks is increasing day by day in today‘s world. Nowadays in every field of our life sensors and sensor networks are gaining higher importance such as, health services, defence sectors, civilian services, food industries, manufacturing plants and also in research areas. But due to various limitations of sensor networks such as broadcasting nature, limited power, dynamic topology and lack of central coordination, sensor networks are prone to variety of security attacks and failures. So we need to handle these vulnerabilities very carefully so that its functionality or features will not get affected adversely while in transit of communication. In this work, we proposed "HYBRID ENCRYPTION ALGORITHIM IN WIRELESS BODY AREA NETWORKS [WBAN]”, that consists a complete set of steps that we can use in achieving authentication, generate key and encrypting data to secure the communication between the senor nodes and the base station.

DECLARATION STATEMENT

I hereby declare that the research work reported in the dissertation entitled " HYBRID ENCRYPTION ALGORITHIM IN WIRELESS BODY AREA NETWORKS [WBAN]" in partial fulfilment of the requirement for the award of Degree for Master of Technology in Computer Science and Engineering at Lovely Professional University, Phagwara, Punjab is an authentic work carried out under supervision of my research supervisor Mr. Deepak Prashar. I have not submitted this work elsewhere for any degree or diploma.

I understand that the work presented herewith is in direct compliance with Lovely Professional University's Policy on plagiarism, intellectual property rights, and highest standards of moral and ethical conduct. Therefore, to the best of my knowledge, the content of this dissertation represents authentic and honest research effort conducted, in its entirety, by me. I am fully responsible for the contents of my dissertation work.

Signature of Candidate

Sameer Farooq

11501907

SUPERVISOR'S CERTIFICATE

This is to certify that the work reported in the M.Tech Dissertation entitled "**HYBRID ENCRYPTION ALGORITHIM IN WIRELESS BODY AREA NETWORKS [WBAN]"**, submitted by **Sameer Farooq** at **Lovely Professional University, Phagwara, India** is a bonafide record of his / her original work carried out under my supervision. This work has not been submitted elsewhere for any other degree.

Signature of Supervisor
Mr. Deepak Prashar

Date:

Counter Signed by:

1) **Concerned HOD:**
   HoD's Signature: _____

   HoD Name: _____

   Date: _____

2) **Neutral Examiners:**

   External Examiner

   Signature: _____

   Name: _____

   Affiliation: _____

   Date: _____

   Internal Examiner

   Signature: _____

   Name: _____

   Date: _____

ACKNOWLEDGEMENT

I take this opportunity to express my profound gratitude and my deep regards to my guide Mr. Deepak Prashar for his exemplary guidance, monitoring and constant encouragement throughout the course of this thesis. The blessing, help and guidance given by him time to time shall carry me a long way in the journey of my life on which I am about to embark.

This work of thesis would also not be possible without the valuable teachings of our professors which help me in this course of thesis. The professors were also very helpful.

I would also like to express my gratitude towards our institution Lovely Professional University for providing us with huge amount of literature work not only on presented work but also on different domains.

Lastly, I would like to thank my almighty and my parents for their constant encouragement which also helps me carry out my piece of work with full enthusiasm.

TABLE OF CONTENTS

CONTENTS **PAGE NO.**

TABLE OF CONTENTS

CONTENTS **PAGE NO.**

LIST OF ABBERVIATIONS

ABBERVIATIONS	DESCRIPTION
WSN	Wireless Sensor Networks.
WBAN	Wireless Body Area Networks.
HEA	Hybrid Encryption Algorithm.
RBS	Radio Base Station.
ECC	Elliptic Curve Cryptography.
ECDH	Elliptic Curve Diffie-Hellman Algorithm.
AES	Advanced Encryption Standard.
IPSec.	Internet Protocol Security.
PDA	Pocket Digital Assistant.
GPRS	General Packet Radio Service.
WCDMA	Wideband Code Division Multiple Access.
LTE	Long-Term Evolution.
ECG	Electrocardiography.
EMG	Electromyography.
EEG	Electroencephalography
SSL	Secure Socket Layer.
TLS	Transport Layer Security.
S/MIME	Secure/Multipurpose Internet Mail Extensions.
IKE	Internet Key Exchange.
QCR	Quantum Computing Resistant.
NGE	Next Generation Algorithm.
MAC	Message Authentication Code.

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1

INTRODUCTION

The Wireless Body Area Network is part of Wireless Sensor Network in which both indoor and outdoor patients are monitored using sensors and wireless technology. The critical phase of monitoring is transmission of real time data from remote location to hospital community cloud, when patients outside the hospital at some remote location and is connected hospital cloud using internet connection. So there is need to encrypt the data collected by sensor from patient before transmission. The paper is presenting the new concept, Hybrid Encryption Algorithm [HEA] that is suitable for ad-hoc as well as for wired networks also. The algorithm not only considers security of data but also the various constraints of sensor networks like battery power, bandwidth, limited processing capability, dynamic topology etc.

1.1 Wireless Sensor Networks

Wireless sensor network consists, a group of autonomous sensing devices that are deployed over a particular geographic region or in some hostile environment for sensing physical and environmental conditions (such as temperature, humidity, pressure, etc.) or for monitoring & analysis purposes. It consists of an array of autonomous sensors & each sensor network node is capable to sense phenomena, perform computations on collected data & to communicate this data with rest of network nodes. A sensor node has typically several parts: a radio, transceiver, antenna and microcontroller.

Due to the broadcasting nature of the network & deployment of nodes in hostile areas or hazardous environments. This makes the networks prone to the various kinds of attacks and potential threats. Besides all this the dynamic network topology and limited resources availability, this makes these ad-hoc networks, implementation difficult. So the major challenge in ad-hoc networks implementation is security of data and resource usage. The limited availability of power resource and memory space limitations makes implementation of high level security a daunting task. There are two main problems that arises in wireless ad-hoc networks related to security algorithms. First, the complexity that security algorithms adds should be very low (in messages), because

every bit (of message) that is processed by the sensor node needs power and thus decreases battery level of the sensor node for every second that computation needs. Second, the memory usage by processing activities in the node (encrypted text and cipher key), should be minimized to very less because in sensor nodes we have limited memory spaces and limited bandwidth available. Due to the various constraints of wireless sensor networks such as limited battery power, limited bandwidth, limited processing capability of nodes and dynamic topology the implementation of the complex & powerful algorithms is not possible. So we needs to select the algorithm, which will provides better security, less computations, low power consumption & small sized output.

The main aim of designing the sensor networks is to collect and analyze the real time data in hostile environments or hazardous locations, where human access is not possible. Because of this property of senor networks, they are used in various applications surveillance and monitoring like battlefields, terrains, simulations, nuclear sites, space etc. The combination of sensing technology with the network technology makes it greater for wide variety of application and usages. Popular wireless sensor network applications include remote patients monitoring, wildlife monitoring, environmental monitoring, warzone surveillance, intelligent communications, industrial quality control, smart buildings, traffic monitoring etc. Our topic is related to the application of the wireless sensor networks in healthcare system.

1.2 Wireless Body Area Networks [WBAN]

WSN has wide variety of application and usages everywhere particularly in healthcare system and defense industry. In healthcare system they comes under wireless body area networks [WBAN]. The WBAN consists of a group of small autonomous sensor node of different types that are wore by person or may be implanted on the patient's body in order to measure the various physiological activities (like ECG, EEG, EMG etc.) & record them continuously for medical observation. The sensed data recorded by the sensors is sent to the hospital community cloud for diagnosis purpose where the clinicians (doctors) monitors the patients remotely. The physiological sensor is electrical equipment that is capable of sensing the various physiological condition. The most commonly used physiological sensors are:

ECG sensor:-Monitors heart functioning.

EMG sensor: - Monitors muscle functioning.

EEG sensor: - Monitors brain functioning.

There are also other types of sensors like Blood Pressure, Tilt, Movement, Breathing, Temperature etc.

WBAN suffers from the same constraints as we discussed for wireless sensor networks like bandwidth, performance, dynamic topology, battery power etc., which makes them vulnerable to security attacks. However WBAN has been successfully deployed, in healthcare areas that includes monitoring of patients health remotely and e-health services. On connecting WBANs with the cloud, this increase its robustness, flexibility, availability, thus overall throughput with sharing of data and computations among different devices located in the cloud. Thus we can increase memory storage and computation power by connecting the WBAN network with the cloud to larger extent.

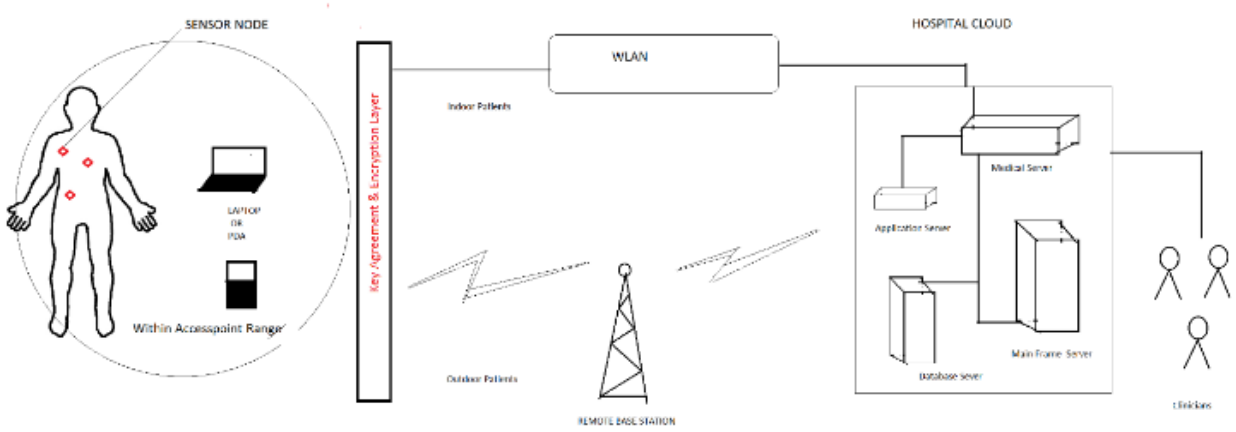


Figure 1: Wireless Sensor Networks in Healthcare systems.

In the proposed framework, we are going to implement the HEA algorithm on every the sensor node who is collecting physiological data form patients body and sending it to the sink (via PDA, Mobile, Laptop) that is hospital cloud, where doctors and other clinicians monitors patients body activities. In the whole scenario are dealing with WBAN, we have heterogeneous network clusters, so each node will act as its own cluster head, sending data to sink (hospital cloud) individually. The connection with sink is established through intermediate devices (viz. Mobile, Laptop, PDA, RBS, GPRS, WDCMA, LTE) using the HEA procedure step by step. We apply HEA at every sensor node interface, which encrypts the data collected, after fixed intervals of time. The encrypted data is then sent to sink via some nearest intermediate device (Mobile, Laptop, PDA, RBS etc.). The Figure: 1 explains the whole scenario. Remember in case of WBAN we have two types of patients, indoor patients and outdoor patients. Indoor patients are connected to hospital cloud through WLAN of hospital which is kept secure using firewalls, IDS etc. The outdoor patients are connected through internet to the hospital cloud. So the risk of attacks and intrusions is more, that is the reason we are using HEA.

CHAPTER 2
REVIEW OF LITERATURE

To date, many cryptography algorithms have been proposed but a most of them are not suitable for WSNs, due to the various constraints of ad-hoc networks. Encryption, the process of encoding information into non readable form in order achieve the confidentiality, is of two major categories. One is symmetric and another is asymmetric. Symmetric uses single key for both encryption as well as for the decryption. The most commonly available symmetric algorithms for encryption includes Advanced encryption standard algorithm (AES) and Data encryption standard algorithm (DES).The another type is asymmetric cryptographic algorithm, commonly known as public-key cryptographic algorithm. It needs two different keys for encryption and decryption data. Elliptic Curve Cryptography (ECC) and RSA are the most known asymmetric algorithms for encryption. Elliptic Curve Digital Signature Algorithm (ECDSA) and Elliptic Curve Diffie-Hellman (ECDH) are based on ECC algorithm.

Both asymmetric and symmetric cryptographic techniques offer both disadvantages and advantages. Symmetric encryption techniques are efficient and cost-effective methods available for securing data however; sharing the secret key is a problem. On the other hand, asymmetric techniques solve key distribution problem but they takes more processing time in contrast to symmetric encryption and consume more resources. Therefore, the best solution is using of both techniques. This combining approach tries to get the advantages of both algorithms and also avoids the disadvantages of both techniques. For integrity check we use hashing technique MD5 that computes the finite sized hash value for a data set or message. MD5 algorithm is the most accepted and widely used hash function for cryptography. It produces 16 byte (128-bit) hash value The MD5 has been used in lot of security areas till date.

In 1980, R.C Merkle [1] was first to develop protocols for public key cryptosystem. The protocol developed by him are still used in all the cryptosystems that are present today and also in new ones that are evolving. There are different types of protocols for different types of digital signatures and public key distribution methods. These protocols varies in size and standards when compared to one another.

In 1996, M. Bellare, H.Krawczyk, and R.canetti [2], proposed hashing method for message authentication "HMAC". They developed Keyed hash function for message authentication. In modern days almost every internet application and protocol uses different types of hashing and message authentication procedures. These mechanisms are simple to implement and are supported by all the types of networks and application. In turn they provides them best security strength. The hash functions are irreversible, that means we can calculate hash value of any message but we can't get back the same message from that hash value. The different type of hashing functions are md5, SHA, NMAC, UMAC, NMAC etc. they all provides different types of security strengths.

In 2000, Xaiodong and Wanger [6], proposed "The practical techniques for search on encrypted data". The main point of their focus was on securing the searching of data that is stored online in various types of trusted and untrusted servers, in the form of emails, files, databases etc. They implemented cryptosystem in order to secure the searching keywords that were used while data retrieval. The system was also meant to prevent untrusted server to know anything about the message stored in encrypted on it. The main aim was to maintain the secrecy of the searching keywords in order to avoid compromise of the stored data on untrusted servers

In 2002, Perrig and Robert [7] proposed security protocol for wireless sensor networks SPINS, as we know the sensor networks are susceptible to numerous vulnerabilities, due to its broadcasting nature. The protocol is using two sub protocols "Secure Network Encryption Protocol" [SNEP] and micro version of "Timed, Efficient, Streaming, and Loss-tolerant Authentication Protocol" [µTESLA]. The first one was providing, Authentication, Confidentiality and Integrity of data sent and received and was also preventing replay attack by providing data freshness auditing. The second one that is micro version of TESLA was providing authentication of data being broadcasted by nodes in resource constrained environment and was also preventing the loss of energy while transmission.

In 2004, P. Golle, J. Staddon, and B.Waters [3], proposed “secure conjunctive keyword search over encrypted data". The system proposed was mainly consisted of “search criterion methodology” for server and “search keyword”. The method was providing the way to store encrypted documents on untrusted servers. In order to store the encrypted document on untrusted server, the user has to provide a set of keywords to the server and also some extra information about that document like its size or format. For retrieval the user was providing the server search criterion capability permit, and also the same keyword and information about that document that was given while storing. This was allowing server to spot that document precisely.

In 2010, Xueying Zhang [22], proposed, “Energy efficiency of symmetric key cryptographic algorithms in Wireless Sensor Networks. In the proposed schema, that includes examination of the energy efficiency of symmetric key algorithms when applied on wireless sensor networks. The proposed system calculates the computational cost in terms of energy, CPU time for data encryption and decryption etc. The system is evaluated with other symmetric key ciphers and by applying all of them to noisy channel in a WSN and their performance and power consumption is calculated.

In 2010 Yang Zhao [24] introduced “A co-commitment based secure data collection scheme for tiered wireless sensor networks”. Wireless sensor networks that are susceptible to various security attacks, mostly to the attacks that are carried on storage nodes that processes the data buffered from sensor readings. To overcome this problem the proposed architecture introduces Secure Data Collection Protocol (SDCP) to support time based queries in tiered WSNs. With small overhead introduced to data communication, Secure Data Collection Protocol (SDCP) maintains both data integrity and data confidentiality. The proposed scheme is co-commitment schema for supporting data queries that are time based. In case while facing of data loss, the protocol easily distinguishes between normal communication signal loss and security override with higher probability without increasing system overhead.

In 2010, Subasree and Sakthivel [36], proposed security algorithm architecture pin which, a given plain text is encrypted using ECC algorithm. The generated cipher text is sent to receiving station by using secured medium. To generate the hash value MD5 is used, which is then encrypted by using DUAL RSA algorithm. The produced cipher text of the hash value is sent to the destination. In this algorithm it is difficult to extract

the hash value and the plain text because due to complex encryption by DUAL RSA and ECC. The new hash value is generated using MD5 compared with the existing one for the integrity checking. It has one disadvantage that it is slow due to ECC and DUAL RSA. Another problem is, if private key got compromised, the entire messages can be read. The third limitation is size of bits generated in the algorithm that is huge. So it is not suitable for wireless ad-hoc networks

In 2011, V Upadhyay and P Kashyap [4], both proposed DES security algorithm architecture for wireless security networks. Their goal was to secure the information produced by the sensor networks with such an algorithm that will not only encrypt the data but also operates on the lower cost for per bit encryption. But due to the various security risks in wireless sensor networks, the algorithm was susceptible to the various vulnerabilities.

In 2011, Jing shi [26], proposed "A Spatiotemporal Approach for Secure Range Queries in tiered Sensor Networks". As we know the cluster head in sensor networks is responsible for transmitting the data of other nodes as well as responsible for answering the incoming queries. . So the cluster head is susceptible to more attacks as compared to other nodes, and in case if it is compromised, it will leak the sensitive data and may also return false or incomplete data in response to query.to overcome this problem the proposed system uses bucketing techniques to ensure only secured range of queries in event driven two tired wireless sensor network. The proposed system was providing confidentiality to the data collected by cluster head, to prevent reading it and was also higher probability check to the query in order to know whether it is complete, incomplete, malicious or false.

In 2011, Ashok Kumar [25], proposed key establishment scheme for WSN using post deployment knowledge. Due to the resource constraints and security concern, the pairwise key establishment in sensor network is tedious job. To overcome this limitation the proposed system introduces novel version of the key prioritization method using post deployment knowledge. The proposed scheme provides better security and network connectivity.

In 2011, Dubal [33], proposed security algorithm in which the given text is enciphered by the key produced ECDH. Dubal used DUAL RSA as an encryption algorithm. The calculated cipher text and digital signature generated are by the ECDSA algorithm for more authentication security are appended wand sent to destination. In parallel, the algorithm calculates the hash value of this cipher text by using MD5 algorithm. After this cipher text and the signature are sent to the destination through secured channel. At the destination the hash value is first calculated after that it is compared with the signature, for the verification of the digital signature received with ciphered message. After that decryption of encrypted cipher text is done by DUAL RSA (Sun et al., 2007) to get the actual plaintext. In this algorithm, the used asymmetric encryption algorithms (DUAL RSA and ECDH) are slow as compared to symmetric encryption. In addition, the attacker can decrypt the messages if he/she can determine the private key. The requirement of secured channel is also a problem.

In 2011, Zhu [30], proposed his algorithm that was using hybrid architecture. The algorithm was using symmetric encryption algorithm to encrypt the plain text. The key and digital signature were encrypted with asymmetric algorithm, that algorithm was using for symmetric encryption. To encrypt the message the sender was using the AES algorithm along with its secret key. The key shared is only used once for encryption and decryption in order to ensure the security. The receiver only accepts the information after signature verification. The problem with the algorithm is that it suffers from the low security, due to encryption of message in single phase, that eventually leads less complexity thus make it more vulnerable to the cryptanalysis attacks.

In 2011, Ren and Miao [18], they proposed hybrid architecture, in which to transmit data the DES. The DES block encryption algorithm with higher efficiency as compared to its counter parts. The key that algorithm uses is encrypted with the RSA algorithm. RSA is best in key management ciphering. The 64-bit DES key is only used once for encryption. The sender gets new keys from key center which manages public keys. The session key is encrypted with RSA. The sender finally sends the combined cipher text generated from DES encryption along with the session key. The algorithm is using DES along with RSA and both of them are weak. So it provides low security.

In 2012, Sadaqat and Bilal [5] proposed comparison on the basis of analysis that they did on different types of encryption techniques and cryptographic algorithms by using MAC ad-hoc networks. The ad-hoc networks are growing day by day and are becoming necessary part of our day to day life. But the most common issues in ad-hoc networks is its restricted resources and dynamic topology. Their analysis work was investigating various cryptographic techniques likes' asymmetric key symmetric key cryptography and cryptography. Not only this but it also compares different techniques for encryption like block cipher (viz, RC2, RC5, RC6), stream cipher (viz, RC4), and hashing methods (viz, SHA, SHA1, MD, MD4, MD2,). Their work resulted in providing the technique for selecting algorithms as per need by selecting different comparison matrices for communication device that includes details of processing time ,energy consumption, , memory expenses that satisfies both the needs as well as security for ad-hoc environment.

In 2012, Kumar [35], proposed hybrid algorithm architecture for message encryption. In this algorithm, the plain text is first encrypted with AES algorithm and then with ECC algorithm. After that the MD5 is used to calculate hash value of this encrypted cipher text. The hash value is appended with the cipher text and the sent to destination. At destination side, the Hash value is first evaluated and integrated. After that, cipher text is decrypted by AES and ECC decryption algorithms. This algorithm is a combination of both symmetric and asymmetric cryptographic techniques. However, the processing time for encryption and decryption is double than normal algorithm because the plaintext is encrypted sequentially by both AES and ECC.

In 2014, Farruk and Aftab [29], proposed cloud-based healthcare framework for security and patients' data privacy using wireless body area networks. The proposed system uses multi-biometric based scheme to get random and secure key. However in the existing system the number of attacks are possible due to poor communication architecture. As well as there are number of problems related to complexity of algorithm, which effects the storage space, device's life & execution time. Though there is no bound on senor nodes like authentication of node, registered nodes of network, known node or friendly nodes, so attacker can also send the malicious message in the network acting as a true node in the network. The attack may be spoofing type or of snooping type either to the disturb communication process or to gain to secret

information in the network. In the existing system there is no bound on message freshness (timestamp checking) so the various attacks like Dos attack, DDos attack, Synchronization Flooding attack are possible. The, another attack that is also possible is man in middle attack. As it clearly visible while sending the message (m1) in first transaction the contents of message are not encrypted, so if someone will capture the m1 and replace id of sender with his own id he will get access to the network easily. Another weakness of proposed algorithm is complexity. The generation & usage of multi-biometric key in the system increases complexity in terms of storage, computations & power consumption & execution time. Since the whole system is dealing with the wireless sensor networks where every resources is limited. So the proposed system fails here.

In 2015, Rawya Rizk and Yasmin Alkady [32], Two-phase hybrid cryptography algorithm for wireless sensor networks. The proposed system uses two-phase hybrid cryptography algorithm (THCA) for data encryption in wireless sensor communication. The framework introduces a new method of cryptography by merging both symmetric and asymmetric techniques in order to produce the new hybrid encryption algorithm. This technique avoids the disadvantages of the existing both symmetric and asymmetric algorithms & achieves high security level without increasing the execution time. However the problem in the existing system is the use of secret key for AES encryption. Although the key is encrypted with ECC algorithm but anyone who will know any of the parameter like trust center public key (TCPK) can easily decrypt the half block of cipher text (ci).

As we know the algorithm is using DUAL RSA & so the algorithm is susceptible to prime factorization attack with which we can easily calculate the key. Thus decrypt the remaining half block of cipher text (Ci). The algorithm uses XOR DUAL RSA the algorithm which is neither QCR (Quantum computer resistant) nor NGE (Next Generation Encryption) algorithm. Another problem of the algorithm is the computational complexity, the given algorithm uses ECC, AES & DUAL RSA in encryption. & in decryption the same algorithms are used ECC, AES & DUAL RSA i.e. total six algorithms are used. This consumes lot of power as well as increases the encryption & decryption time of messages & cipher text. Since we all are aware that in sensor networks we have a lot of constraints like limited battery power, low

performance chips for processing & execution time of algorithms etc. The, another problem is DUAL RSA key size which is mainly 1024 bits in normal. Thus good amount of storage is required to store key & intermediate results, unfortunately which is not available in case of wireless sensor networks.

CHAPTER 3
PRESENT WORK

3.1 Problem Formulation

3.1.1 Introduction

The proposed framework consists of sensors that are implanted or attached on the patient's body. These sensors are of different types viz, ECG, EGG, EMG etc. They collects physiological data from the body of patient, the data collected is sent to nearer base station and then transmits it to the hospital cloud's servers securely via some intermediate devices (Laptop/PDA) and base stations (RBS), here the doctors and other medical staff take the readings of the data and then provides treatment to the patient accordingly. In the proposed system we are dealing with the heterogeneous sensor network where all the nodes are of different types. Thus there is no need of cluster formation or cluster head selection, as we have limited number of sensors attached to the patient's body and all of them are of different types in their working sense and technology.

3.1.2 Details of Proposed System

In this phase the patient who is going to use the wireless sensors for medical observation, the hospital community will provide him the unique registration number (RN) & the number is kept confidential. The different types of sensors are implanted or attached on the patient's body depending on types of illness. These sensors are given unique ID's (NID) under the given registration number. So each sensor on patient's body will be identified with unique registration number (RN) and node ID (NID).

3.1.2.1 Registration Phase

In this phase the patient who is going to use the wireless sensors for medical observation, the hospital community will provide him the unique registration number (RN) & the number is kept confidential. The different types of sensors are implanted or attached on the patient's body depending on types of illness. These sensors are given unique ID's (NID) under the given registration number. So each sensor on patient's body will be identified with unique registration number (RN) and node ID (NID). Attached on the patient's body depending on types of illness. These sensors are given unique ID's (NID) under the given registration number. So each sensor on patient's body will be identified with unique registration number (RN) and node ID (NID).

3.1.2.2 Authentication Phase

Before any actual transmission of data between the base station (hospital cloud) and the sensor nodes both needs to authenticate each other for prevention of any attack viz. malicious node, man in the middle attack or worm hole etc. In order to authenticate the sink nodes with the base station and vice versa, few computation are done on both base station server side as well as the sink node side. Both sides, uses registration number (RN), node id (NID), and the time stamp (TM) for authentication and message freshness.

Table 1: Authentication process

Sensor Node	**Base Station**
Compute m1=H(RN+NID)||RN||TM **(send)**	
	Extract H (RN+NID), RN, TM from received m1.Fetch details of RN from databases and find corresponding NID value. Compute H (RN+NID) and compare it with received one for integrity check and authentication.
	Compute m2=H(NID)||RN||TM **(send)**
Extract H (NID), RN, TM from received m2. Compute H (NID) and compare it with received one for integrity check and authentication.	

NID: Node ID.

TM: Time-stamp value.

RN: Registration number of patient.

H: MD5 Hash Function.

m1: Message sent by sensor node to base station server.

m2: Message sent by base station server to sensor node.

After the successful integrity checks on the both side the authentication will be achieved. Now the sink & base station can communicate with each other & can send sensitive data to one another as both are authentic.

3.1.2.3 ECHD Key Exchange Phase

This phase includes they exchange of key between sink node & base station that will be used for data encryption & decryption on sink node & base station side respectively. The algorithm is used to exchange the key between sender and receiver is ECDH (Elliptic curve Diffie-Hellman (ECDH)).

The domain parameters for ECDH are:

Table 2: ECDH domain Parameters

P	Field (modulo p)
a, b	Curve Parameters
G	Generator (Base Point)
N	Order(G)
H	Co-factor

All of these domain parameters are public.

Elliptic curve equation:

$$y^2=x^3+ax+b$$

The steps of ECDH-key generation on both sides are given below:

I. First the sink node will pick up a random key **β**, such that **1< β < n-1**. This will be his private key.

II. Similarly the base station will also pick up a random key **α**, such that **1< α < n-1**. This will be his private key.

III. Sink node will compute **S=β G**, and base node will compute **B=α G**.

IV. Now both will exchange the **S** and **B** though an ordinary channel. "*There is no need of secure channel"*.

V. Now sink node will have **B= (xB, yB)** & base station **S= (xS, yS)**. So they both will multiply the received **B**, **S** with their private keys to get final keys:

Key of sink node **P=α.β.G.**

Key of base node **Q=α.β.G.**

VI. After computations, the final key **K** will be on both sink node side as well as base station side:

K=α.β.G.

VII. The final key **K** of ECDH will consist x, y coordinates like **K(x, y)**.

The steps of ECDH-AES key generation on both sides are given below:

After generating ECDH key successfully on the both sides of sink and base station, the generated key is going to be used for ECC-128 bit encryption-decryption process. For AES-128 bit encryption-decryption process, another key of 16-bytes will be generated by using existing ECDH key. The generated ECDH key **[K(x, y)]** that consists of x and y coordinates will be used to generate 16-byte AES key. In order to generate that key on both sides of sink node and base station, the steps given below are going to be followed:

I. First the values of **x, y** will be rounded to the nearest integers, so as to convert these values into integer form if they are in real form.

II. The second step will be, if the numbers are less than 1 then add prime number 3 if it is **x** otherwise add prime number 5 if it is **y.**

If **[x** < = 1] then

x=x+3

If **[y** < = 1] then,

y=y+5

III. The third step will include squaring of both **x, y**.

$$\mathbf{X = x^2 \quad \& \quad Y = y^2}$$

IV. Now the 16-byte key will be calculated by squaring and cubing values of x and y alternatively along with calculating mode of each value.

V. The next values will be the alternative squares and cubes of previous values.

$$\mathbf{K1 = X^2 \bmod 99.}$$

$$\mathbf{K2 = Y^2 \bmod 99.}$$

$$\mathbf{K3 = (X*X^{2)} \bmod 99.}$$

$$\mathbf{K4 = (Y*Y^{3)} \bmod 99.}$$

…….

$$\mathbf{K15 = (X'*X^{2)} \bmod 99.}$$

$$\mathbf{K16 = (Y'*Y^{3)} \bmod 99.}$$

VI. These values from **K1 - K16** will be converted into the hexadecimal equivalents and the act as 16-byte AES-128 Key.

Table 3: Generated ECDH-AES key

K1	K2	K3	K4
K5	K6	K7	K8
K9	K10	K11	K12
K13	K14	K15	K16

3.1.2.4 Encryption Phase

The proposed framework uses Hybrid encryption algorithm (HEA). For encryption this algorithm divides the plaintext of message into **'n'** number of smaller units or blocks **'Ni'** each of 128-bit in size. These units are further divided into two parts **Mi (1: n/2)** blocks, and **mi (n/2+1: n) blocks**. In case if the nth part is not equal to 128-bit size the algorithm pads the block with null bits in order to make it equal to 128.

In step 1, the first n/2 blocks **'Mi (1: n/2)'** are encoded by with **ECC-128**-bit algorithm. The algorithm uses key **'K'** produced from ECDH algorithm. The first part is enciphered in the following way:

$$\mathbf{Mi} = \sum_{\mathbf{i=1}}^{\mathbf{i=\frac{n}{2}}} (\mathbf{Ni}) \qquad \mathbf{1 \leq i \leq \frac{n}{2}}$$

Elliptic Curve encryption function **ECC_enc()** enciphers the **Mi (1: n/2)** with key **K** generated by ECDH algorithm. The cipher text produced will be

$$\mathbf{Ci = ECC\_enc\ (\ Ni,\ K)}$$

In step 2 that will be performed in parallel of step 1 the remaining n/2 blocks '**mi (n/2+1: n)'** are encrypted using **AES-128** encryption algorithm. In this algorithm the key '$\mathbf{K_{1\text{-}16}}$' generated by ECDH-AES algorithm is used for encryption. The cipher text produced will be:

$$\mathbf{mi} = \sum_{\mathbf{i}=(\frac{\mathbf{n}}{\mathbf{2}}+\mathbf{1})}^{\mathbf{i}=\mathbf{n}} (\mathbf{Ni}) \qquad \frac{\mathbf{n}}{\mathbf{2}} + \mathbf{1} \leq \mathbf{i} \leq \mathbf{n}$$

Advanced encryption standard function **AES_enc()** enciphers the **mi (n/2+1: n)** with key $\mathbf{K_{1\text{-}16}}$. The cipher text produced will be

$$\mathbf{ci = AES\_enc\ (Ni,\ K_{1\text{-}16})}$$

MD5 hashing algorithm is used to generate hash values of the cipher texts **Ci** and **ci**.

$$\mathbf{Hi = MD5\ (Ci).}$$

$$\mathbf{hi = MD5\ (ci).}$$

And, finally, cipher text **C** which is generated by padding **Ci** and **ci** is sent to the base station node. The hash values **Hi** and **hi** of the corresponding cipher texts **Ci** and **ci** are integrated **(H =Hi +hi)** and are sent along with message to the destination.

$$\mathbf{C = Ci + ci}$$

$$\mathbf{H = Hi + hi}$$

3.1.2.5 Decryption Phase

In decryption, the received cipher message **C** which is in encrypted form is divided into **'n**' number of blocks **'Ni'** each unit is of 128-bit size. The blocks are then grouped into two separate parts. The first half consists **'Ci' (1: n/2)** blocks and second half consists **'ci' (n/2+1: n)** blocks. For integrity check of received cipher text either to accept or reject the hashing is done by using same hashing algorithm are used by sender.

In order to get the first half block of plain text, the first half of received message **'Ci' (1: n/2)** is decrypted by using **ECC 128-bit** algorithm decryption phase.

$$\mathbf{Ci} = \sum_{\mathbf{i=1}}^{\mathbf{i=(n/2)/}} (\mathbf{Ni}) \qquad \mathbf{1 \leq i \leq \frac{n}{2}}$$

$$\mathbf{Mi = ECC\_dec\ (Ci,\ K)}$$

'Mi' is the first part of decrypted text. The remaining n/2 blocks **ci (n/2+1: n)** are decrypted with AES-128 bit algorithms decryption phase as follows:

$$\mathbf{ci} = \sum_{\mathbf{i=(\frac{n}{2}+1)}}^{\mathbf{i=n}} (\mathbf{Ni}) \qquad \mathbf{\frac{n}{2} + 1 \leq i \leq n}$$

$$\mathbf{mi = AES\_dec(\ ci\ ,\ K)}$$

'mi' is the other part of the decrypted text.

The process of decryption of **'Ci'** and **'ci'** goes in parallel like as in encryption. Finally after the complete decryption of whole cipher message the blocks are combined in same order as divided to get the complete message.

$$\mathbf{M = Mi + mi}$$

3.1.3 Algorithms

3.1.3.1 Encryption Algorithms

The hybrid encryption Algorithm proposed for encryption is as follows:

Input:

P=Plain text

K =Key generated using ECDH

S= (Block size 128-bit)

Output:

C= Cipher text

C i= Cipher text produced with ECC

ci = Cipher text produced with AES

H= Hash value of Cipher text

Hi= Hash value of first part of cipher text

hi= Hash value of second part of cipher text

1. n = P/S;
2. set i = 1;
3. do
4. {
5. Mi =$\sum_{i=1}^{\frac{n}{2}}(\mathbf{NI})\ 1 \leq i \leq n/2$
6. Ci = ECC_enc (**Ni, K**);
7. Hi = MD5 (Ci);
8. i++;
9. }
10. while (i<n/2+1);
11. i = (n/2+1)
12. do
13. {

14. mi=$\sum_{i=\frac{n}{2}+1}^{n}$ (**NI**) $\frac{n}{2}+1 \leq i \leq n$

15. c i = AES_enc (**NI, K**);

16. hi = MD5 (c i);

17. i++;

18. }

19. while (i < n+1);

20. C = Ci + ci;

21. H = Hi + hi ;

3.1.3.2 Decryption Algorithms

The hybrid encryption Algorithm proposed for deryption is as follows:

Input:

Hi'= Hash value of first part of received cipher text

hi'= Hash value of second part of received cipher text

C= Cipher text

Ci= Cipher text produced with ECC

ci = Cipher text produced with AES

H = Hash value of Cipher text

K = Key generated using ECDH

S= (Block size 128-bit)

Output:

P=Plain text

1. n = C/S;

2. set i = 0;

3. do

4. {

5. Ci = $\sum_{i=1}^{n/2}$ (Ni) $1 \leq i \leq n/2$

6. Hi' = MD5 (Ci);

7. hi' = MD5 (C i);

8. If (Hi = Hi') & (hi = hi')

9. {

10. M i = ECC_dec (**Ni, K**);

11. i++;

12. }

13. }

14. while (i < n/2+1);

15. i = n/2;

16. do

17. {

18. ci = $\sum_{i=\frac{n}{2}+1}^{n}$ (Ni) $1 \leq i \leq n/2$

23. mi = AES_dec (**Ni, K**);

21. i++;

24. }

25. }

26. while (i < n+1);

27. P= Mi + mi ;

3.2 Objectives of the Study

As we know wireless sensor networks inherent various limitations such as low energy capacity, less computational power and limited storage facility etc. So the principal objective of this study is to design an appropriate encryption system for wireless sensor networks and to figure out an analysis of various parameters and factors of the proposed system.

The main objectives of the proposed system are as under:

1. To achieve Mutual authentication in data transmission between base station and sensor nodes.

2. To propose how to generate secured key for AES and ECC algorithm using ECDH algorithm.

3. To propose new encryption algorithm “Hybrid Encryption Algorithm” in order to secure the transmission of data.

4. Comparing the proposed system with the existing system in terms of its various factors such as Mutual authentication, Key generation, Cipher text size (memory usage), Encryption & Decryption time and Complexity.

3.3 Research Methodology

3.3.1 Assumptions and parameters of interest

1. The sensor nodes that are implanted or wore by the patient who is at remote location.

2. All the sensor nodes are heterogeneous, so there is no need of choosing cluster head while data transmission.

3. The data collected by the sensors is in numerical form.

4. The reading collected by the senor is not transmitted frequently rather it is stored in buffer of sensor, so that the fair amount of data is collected then it is sent after regular intervals.

5. The data collected by sensor node is encrypted at the sensor node before it is being sent further.

6. The data collected by sensor node is sent to nearer intermediate device (Laptop/PDA), which transmits it further to hospital cloud's servers via RBS.

7. The hospital categorizes the data received from sensors into different types on the basis of provided sensor node Id's.

8. The data of different patients is categorized on the basis of provided registration numbers.

9. In our system we are considering that there are two separate processing units where ECC and AES-128 algorithms are executed in parallel.

10. Another assumption is that the data collected by sensors is encrypted simultaneously and are sent after fixed intervals of time.

3.3.2 Factors for consideration and comparison

1. Mutual authentication: It includes authentication of the base station (hospital community cloud server) by the sink node and vice versa. This study assumes that the nodes that all node who are collecting data from patients body are authenticating base station separately and base station also authenticates them separately on the basis of provided node Id's and registration numbers.

2. ECDH & ECDH-AES key generation: it includes generation of secured key by using ECDH a1gorithm. The key generated is more secured and does not require any secured separate channel for sending it to other end.

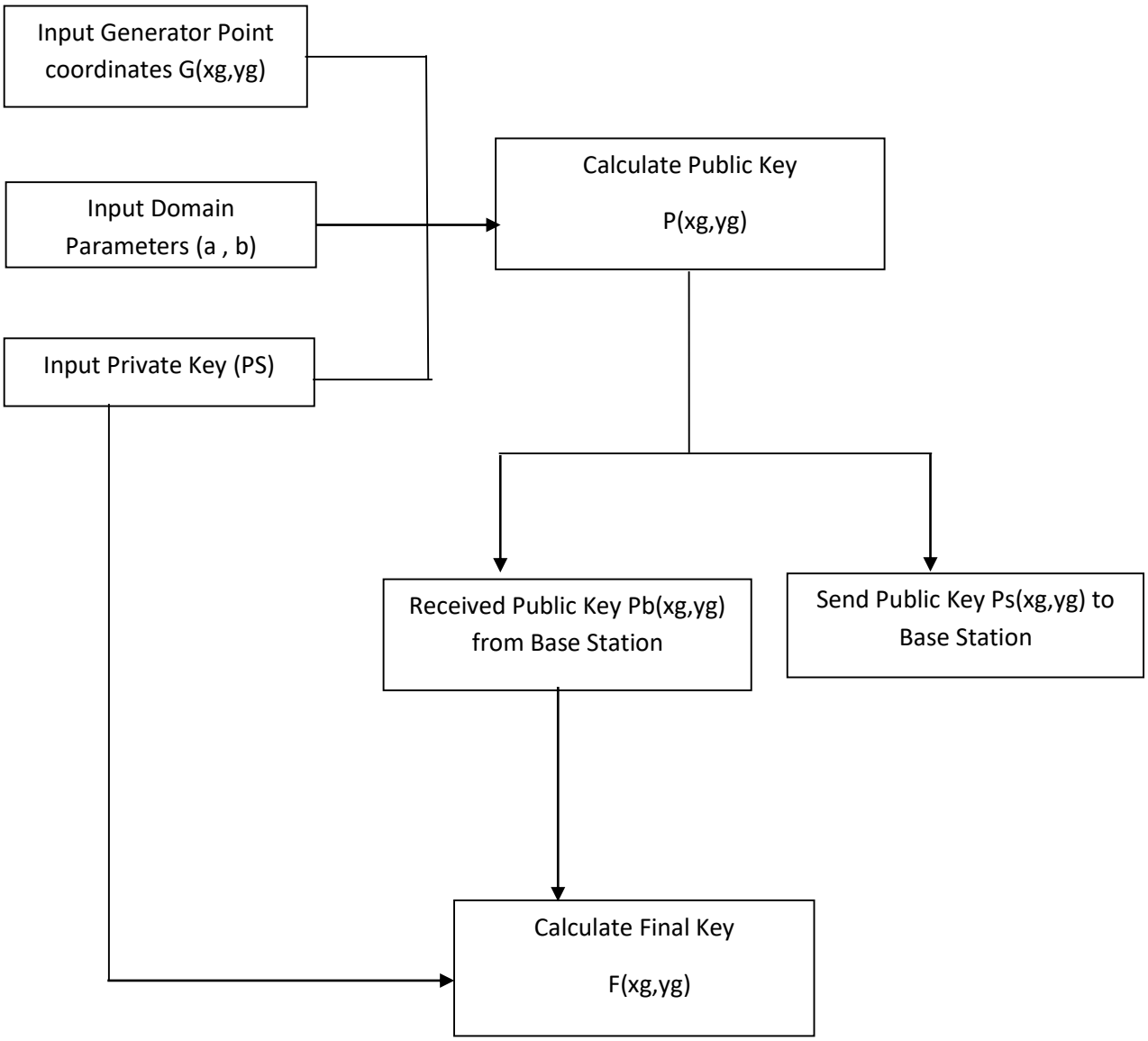
3. Cost trade off: The new proposed algorithm uses less number of steps to generate cipher text. More the number of steps, means more the cost burden, in terms of processing time, battery consumption and memory usage.

4. Execution time: The new proposed algorithm generates small sized cipher text as compared to the existing system. And for each bit of cipher text generated the more processing power, more battery power and more memory space is required. The new system has shorter execution time as compared to the previous systems.

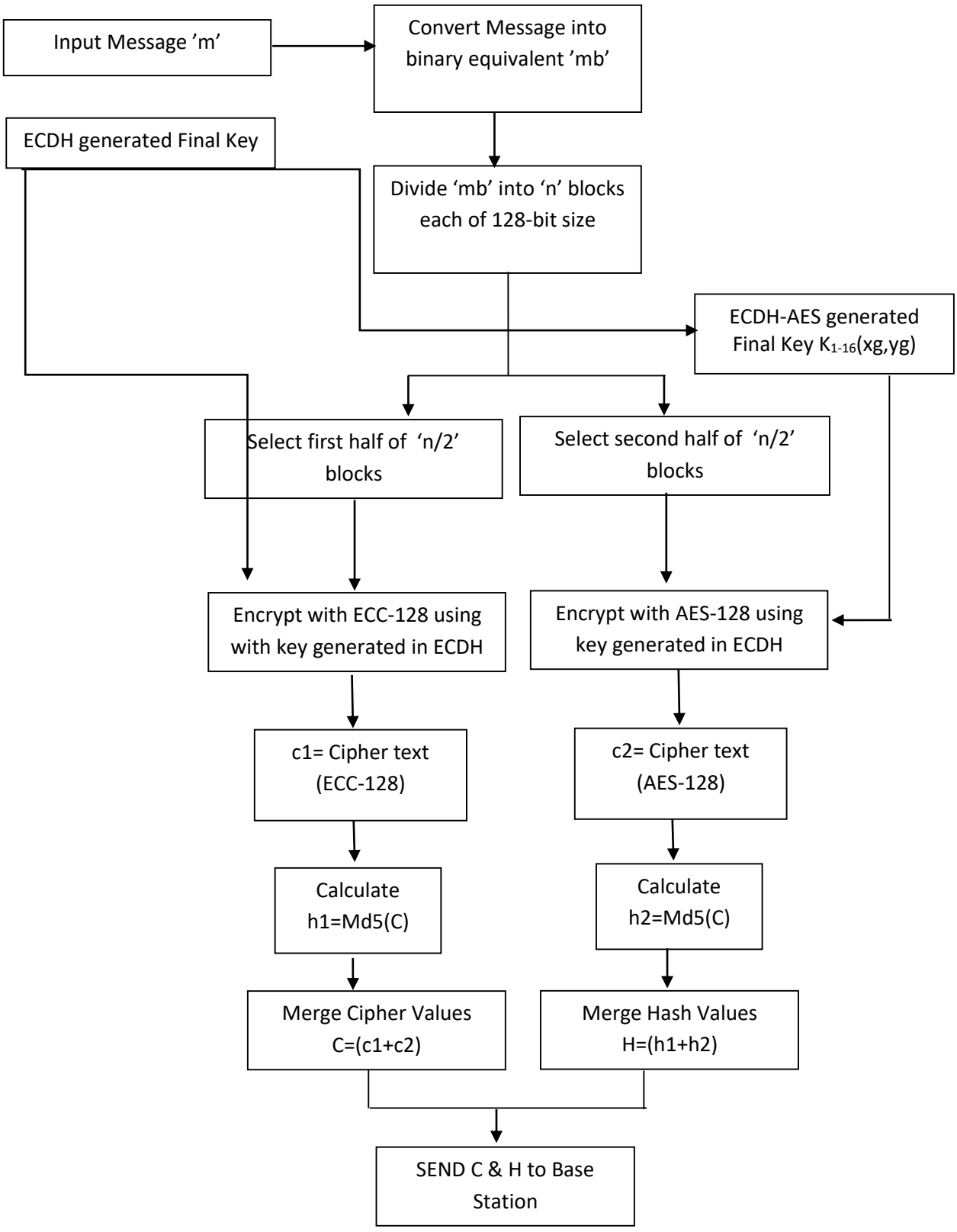
5. Algorithmic complexity: The space and time complexity of proposed algorithm is less than existing algorithm and the proposed algorithms also provides more secured cryptographic method for encryption than existing one due to use of discrete properties of elliptical curves in key generation and well as in encryption.

3.3.3 Flow chart of the Proposed Methodology:

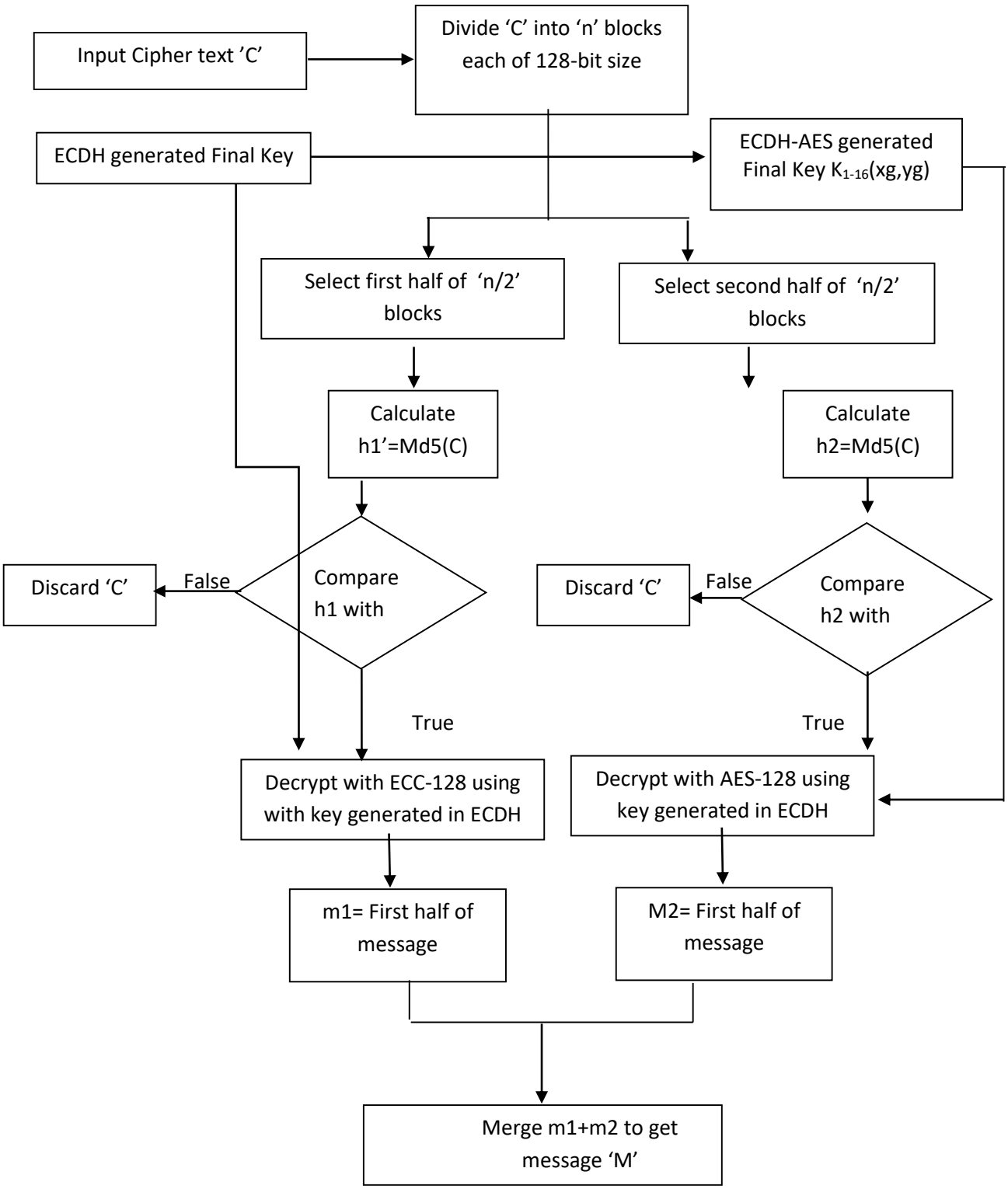
Flow chart for ECDH Key generation:



Flow chart for HEA [Encryption Phase]:



Flow chart for HEA [Decryption Phase]:



CHAPTER 4
RESULTS AND DISCUSSION

4.1 Experimental results

The proposed framework was implemented in MATLAB 2012a and Visual Studio 2013. The novel proposed algorithm namely Hybrid Encryption Algorithm [HEA] along with its various components like ECDH key generation, AES key generation , ECC-128 bit encryption-decryption and AES-128 bit encryption- decryption all were implemented by using MATLAB 2012a. The mutual authentication process between sink node and base station was demonstrated using Visual Studio 2013.

The result calculation includes encryption and decryption time taken by algorithm to encipher and decipher message. It also include the time taken for ECDH key generation and ECDH-AES key generation. The following section will contain screen shorts along with their explanation.

Figure 2, shows the mutual authentication process between sink node and base station. In order to authenticate each other both sink nodes and base station will do some computations. Both sides, uses Registration number **(RN)** and Node id **(N_ID)** for authentication computations. Sink node computes hash value **H (NID+RN)** of given registration number and then it sends it to the base station along with appended given registration number. The base station extract registration number from message, then using the same registration number it fetches corresponding details from databases that includes NID value. After this base station compute **H (RN+NID)** and compare it with received one for integrity check and authentication. If received hash value is same as calculated hash value then the node is allowed to connect for further processing otherwise node is blocked. If node is verified genuine then the base station will calculate hash value of Node id **H (NID)** and it will send it along with the appended registration number to the sink node. At sink node in order to verify whether the base station is genuine the hash value of Node id **H (NID)** will be calculated and compared with received one. If verification is successful then then connection for data transmission will be established between sink node and base station.

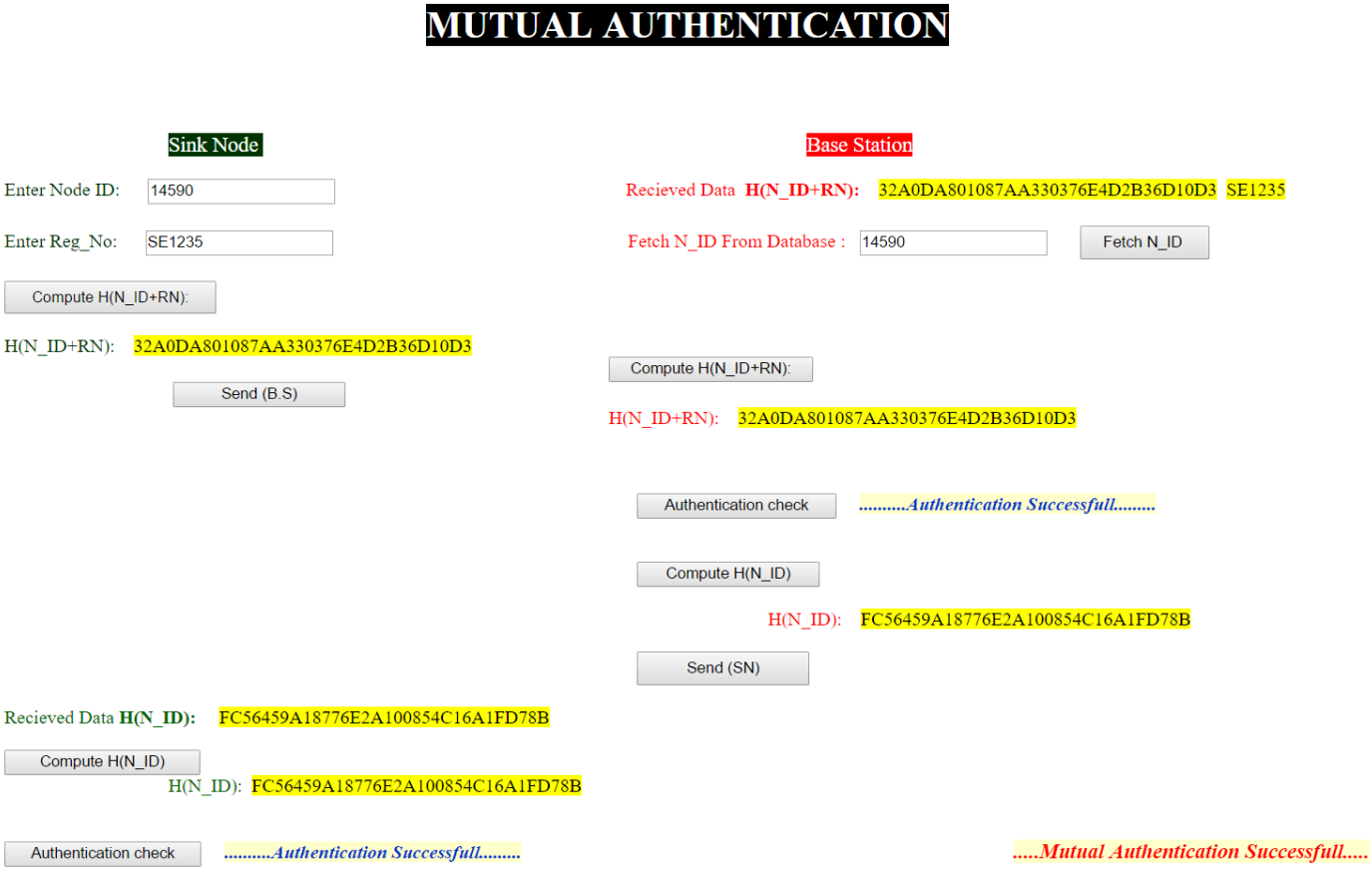


Figure 2: Mutual Authentication

Figure 3, shows the ECDH key generation process between sink node and base station. Here the common domain parameters are selected first on the both ends. After that the sink node selects his private key to generate intermediate key by using elliptic-curve point doubling methodology. Similarly, the base station selects his private key to generate intermediate key using same point doubling methodology. Both ends exchanges their intermediate key results with one another in order to generate final key. The final key is generated by geometrically multiplying their private key with the intermediate key received from other end. **Figure 4**, depicts the MATLAB implementation of ECDH algorithm, and shows how keys are generated practically using MATLAB.

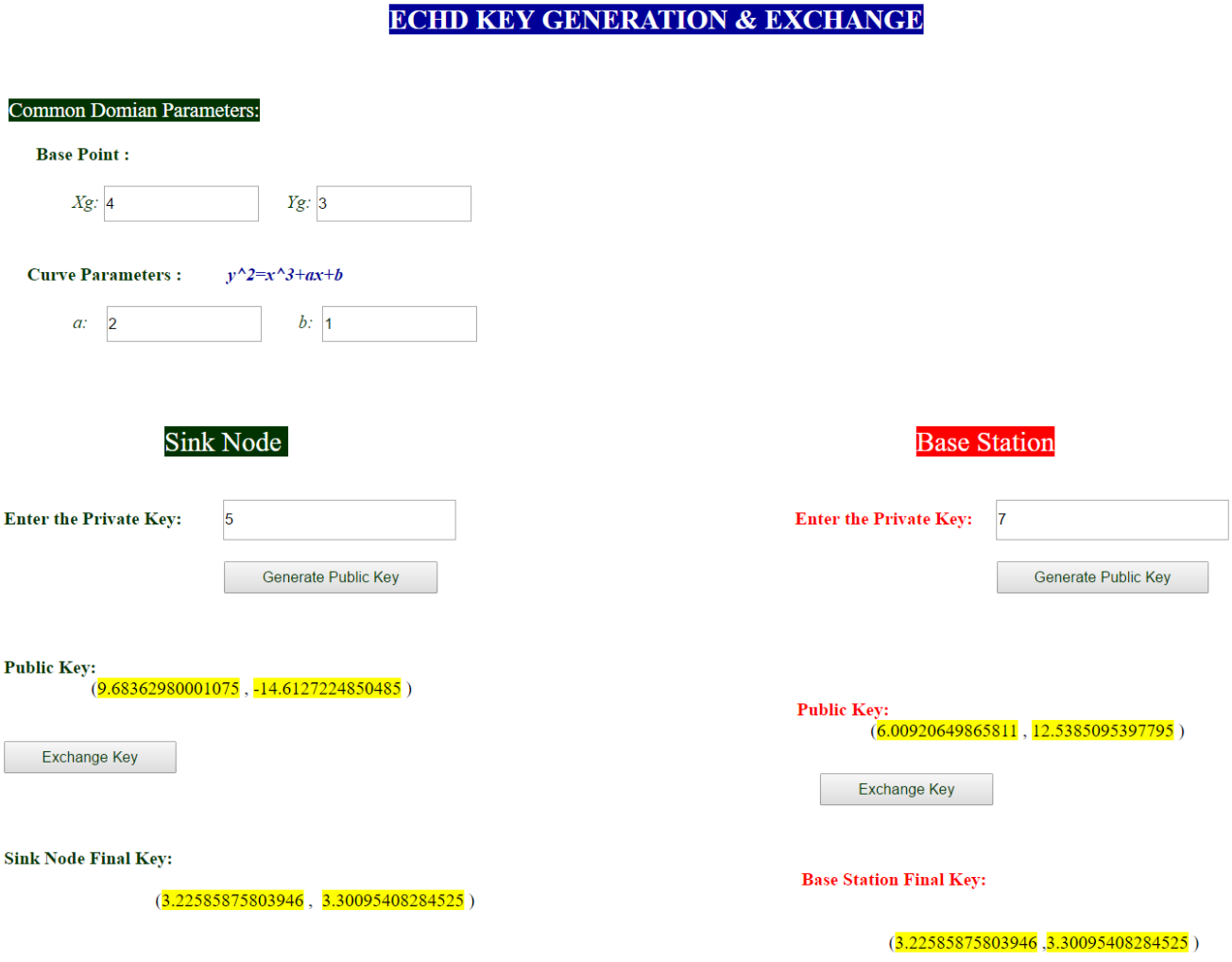


Figure 3: ECDH key generation

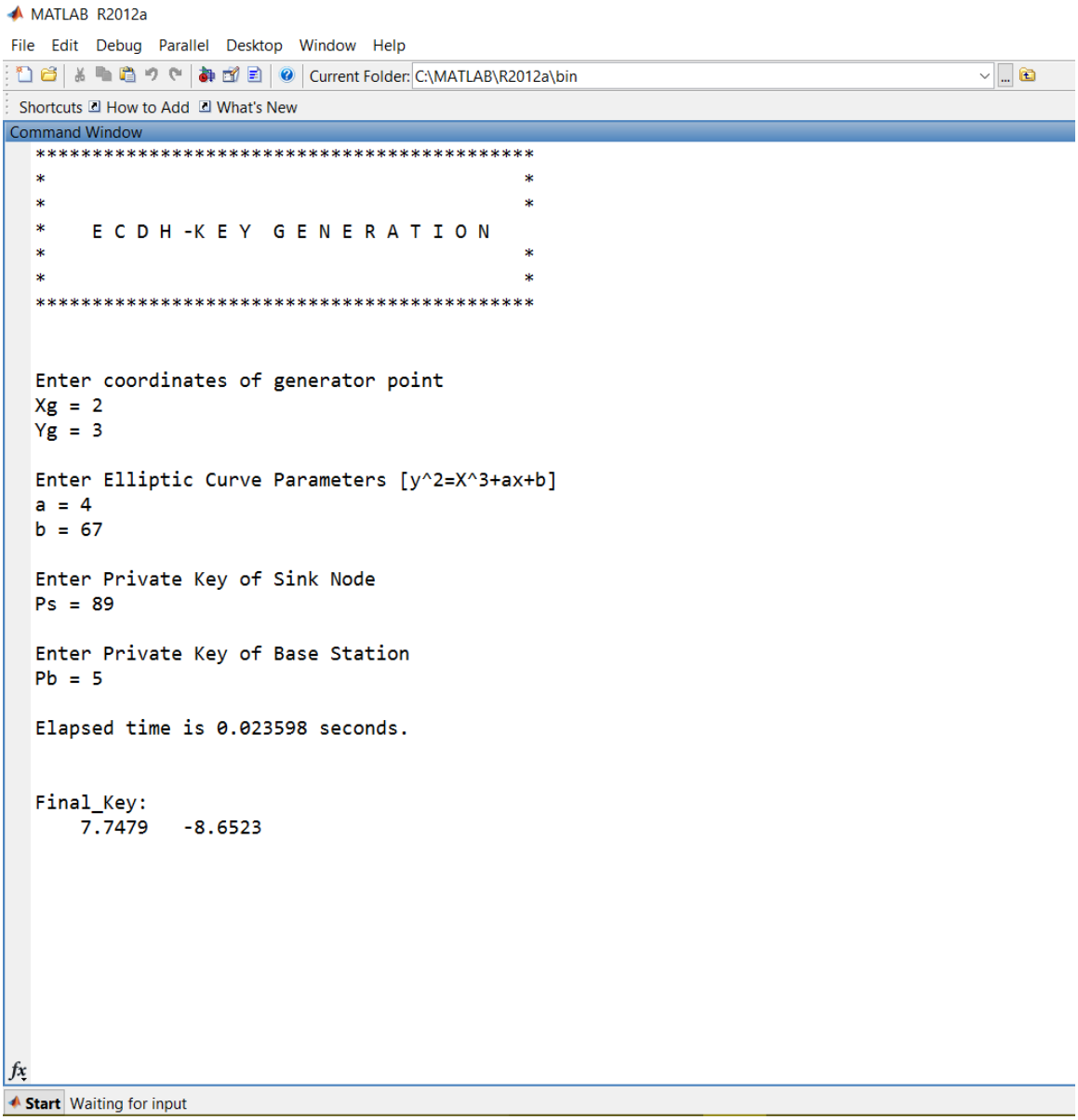


Figure 4: MATLAB ECDH key generation

Figure 5, shows the ECDH-AES key generation process between sink node and base station. AES-128 16-bytes key is generated from existing ECDH key. The ECDH key's **[K(x, y)]** coordinates x and y coordinates will be used to generate 16-byte AES key. The process how this key is generated is explained in ECDH key generation phase of proposed system. **Figure 6**, depicts the MATLAB implementation of ECDH-AES algorithm, and shows how 16-byte keys AES-128 algorithm is generated practically using MATLAB. **Figure 7**, shows the 16-byte hexadecimal equivalents of the previously generated key using MATLAB implementation.

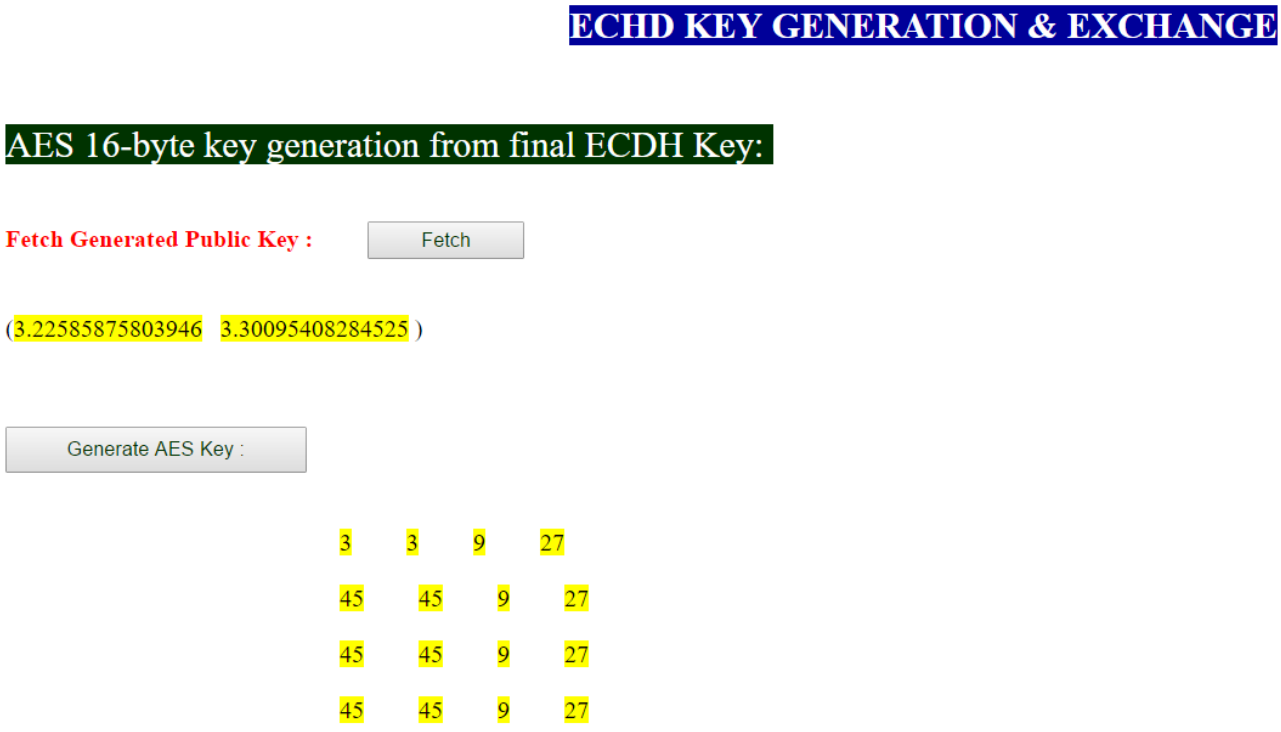


Figure 5: ECDH-AES key generation

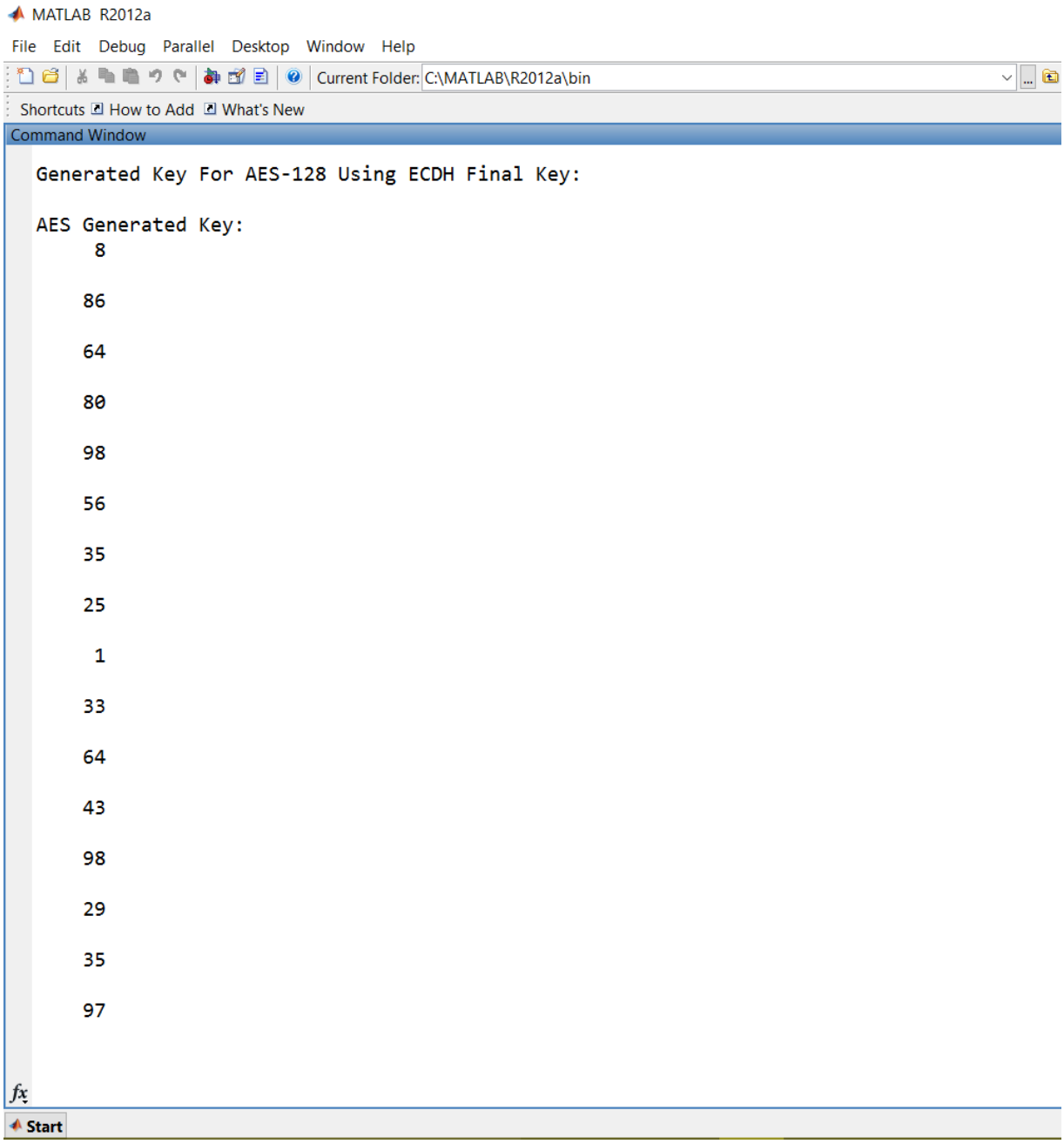


Figure 6: MATLAB ECDH-AES key generation

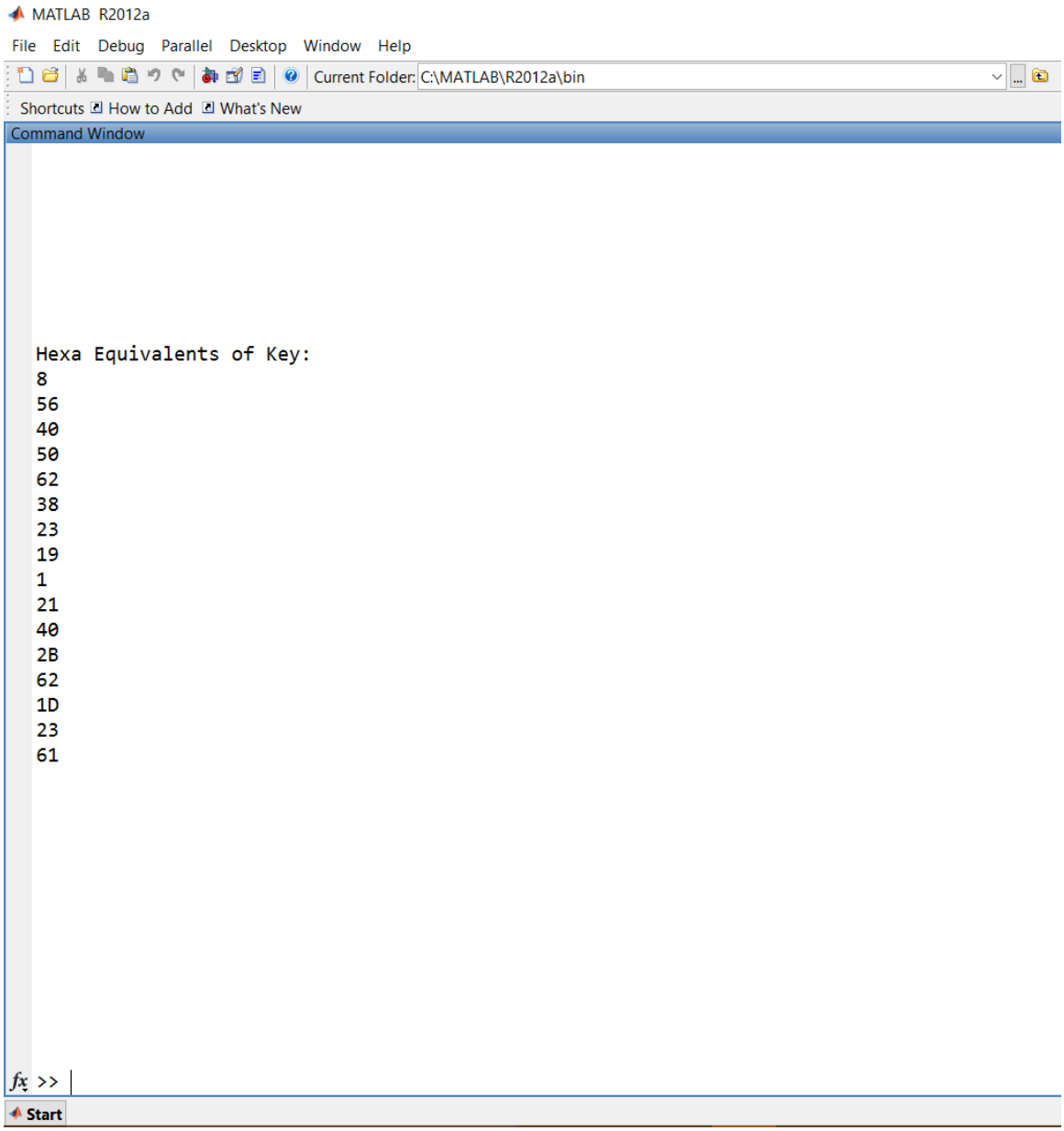


Figure 7: MATLAB 16-byte ECDH-AES key

Figure 8, shows the ECC and ECDH-AES key generation time, using MATLAB. The figure shows the different durations of time taken by these two key for generation while the plain text was of different sizes. In the graph it is clear the time taken by ECC-AES key generation is relatively higher as compared to the simple ECDH key generation algorithm. Since we need both for our algorithm so both have equal priority.

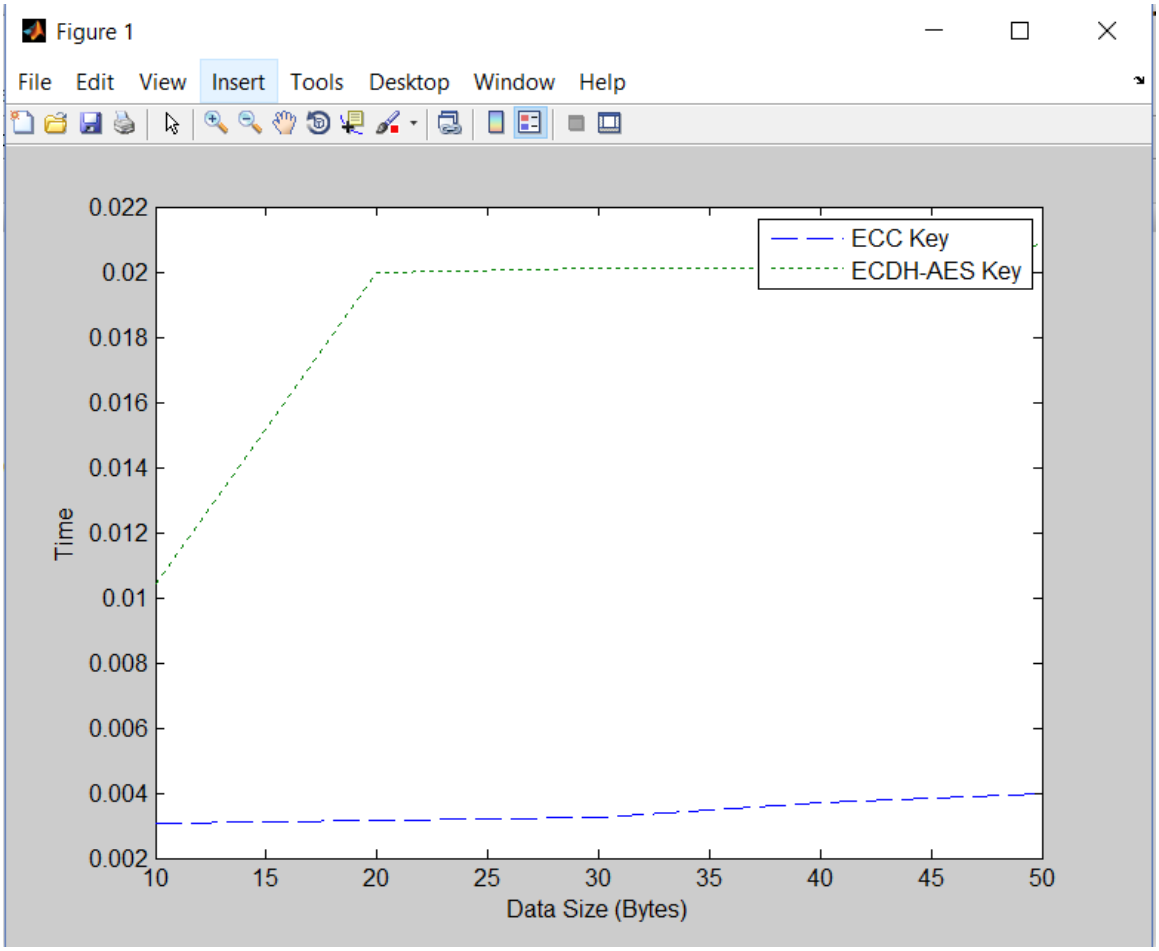


Figure 8: ECC & AES key generation time

Figure 9, shows encryption and decryption time taken by ECC algorithms with different sizes plain text. It is clear from the figure that there is gradual increase in encryption and decryption time, with increase in plain text size. But in our case as we are dealing with the sensor node which sends data regularly after frequent intervals of the time, so we don't needs to worry about all this. Because the nodes on which we are working, they encrypt data in from of small chunks, due to limited size of memory, data processing facilities and need of real time data transmission to hospital community cloud.

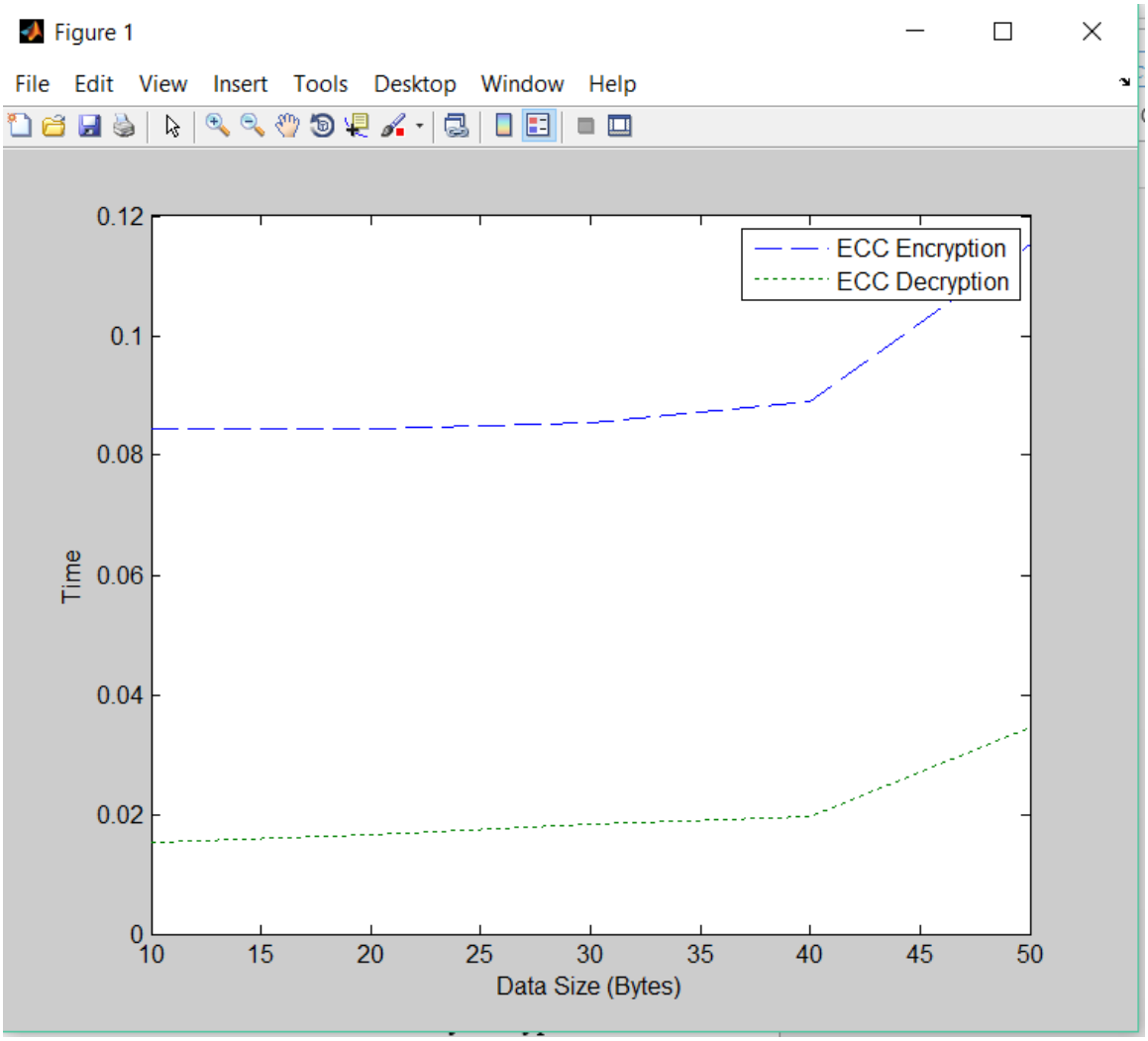


Figure 9: ECC encryption & decryption time

Figure 10, shows encryption and decryption time taken by AES algorithms with different sizes plain text. It is clear from the figure that there is gradual increase in encryption and decryption time, with increase in plain text size. It is also clear the time taken by decryption process of AES is more as compared to its encryption time. In our case as we are dealing with the sensor node which sends encrypted data frequently in from of small chunks, and thus avoids the aggregation of huge data that may take large amount of time.

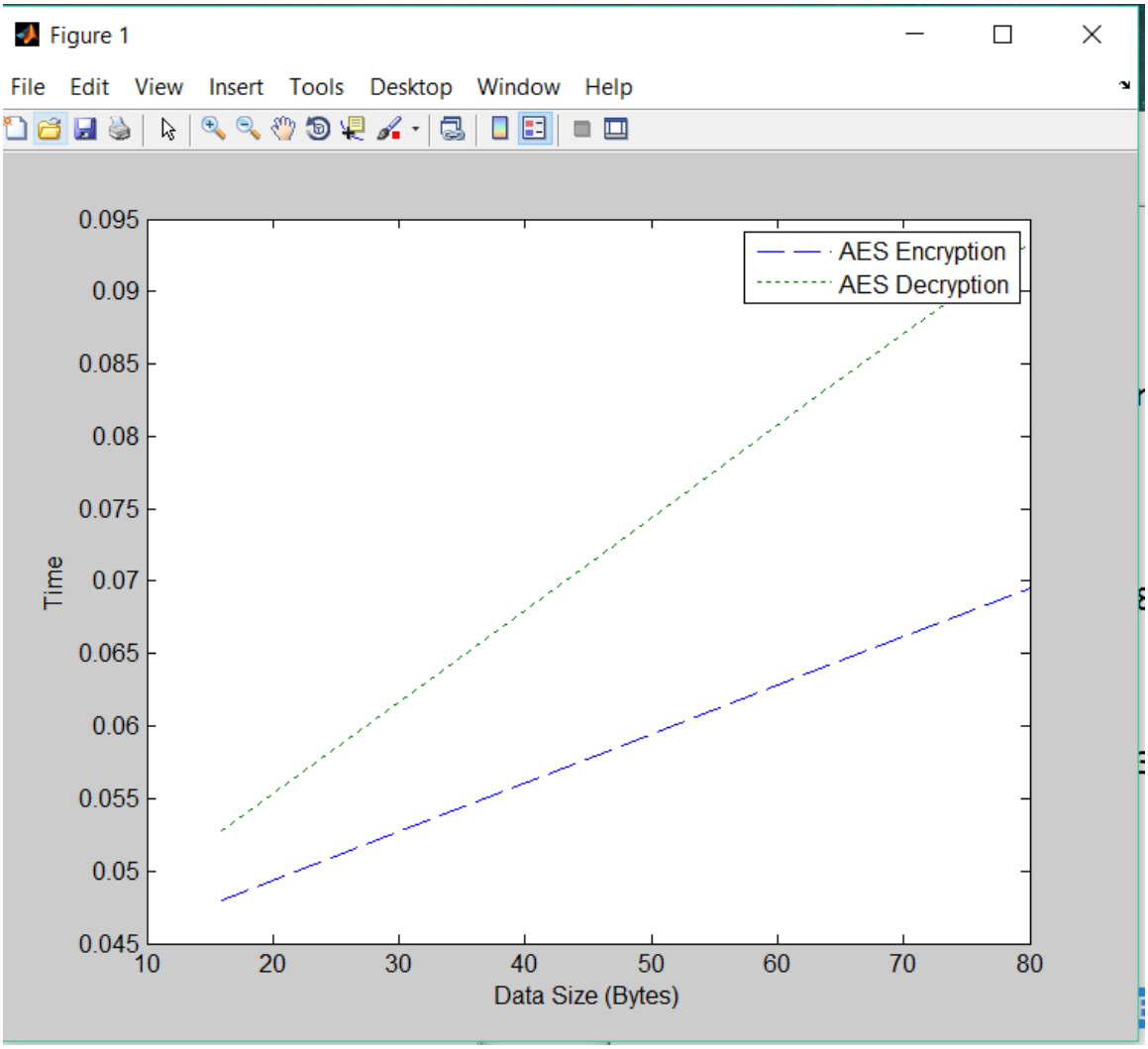


Figure 10: AES encryption & decryption time

From **Figure 9 and Figure 10** it is clear that the time taken by ECC algorithm is more for both encryption and decryption because it is asymmetric as compared to AES which is asymmetric, thus takes less time. ECC consumes more time so we will consider the execution time of ECC as the total execution of whole system. Because algorithms are running in parallel, so the on which takes more time will be considered as the execution time of the system.

Figure 11, shows the amount of cipher text generated by the various algorithms, in directly it shows the amount of memory that algorithm needs for cipher text generation. From the figure it is clear that the cipher text produced by the ECC algorithm varies linearly with the size of the plain text. But the cipher text of generated by AES algorithm

shows gradual change in the certain points, this is because AES is producing cipher text in form of 16-bytes, that is the reason the combined cipher text is also forming the same shaped curve like AES.

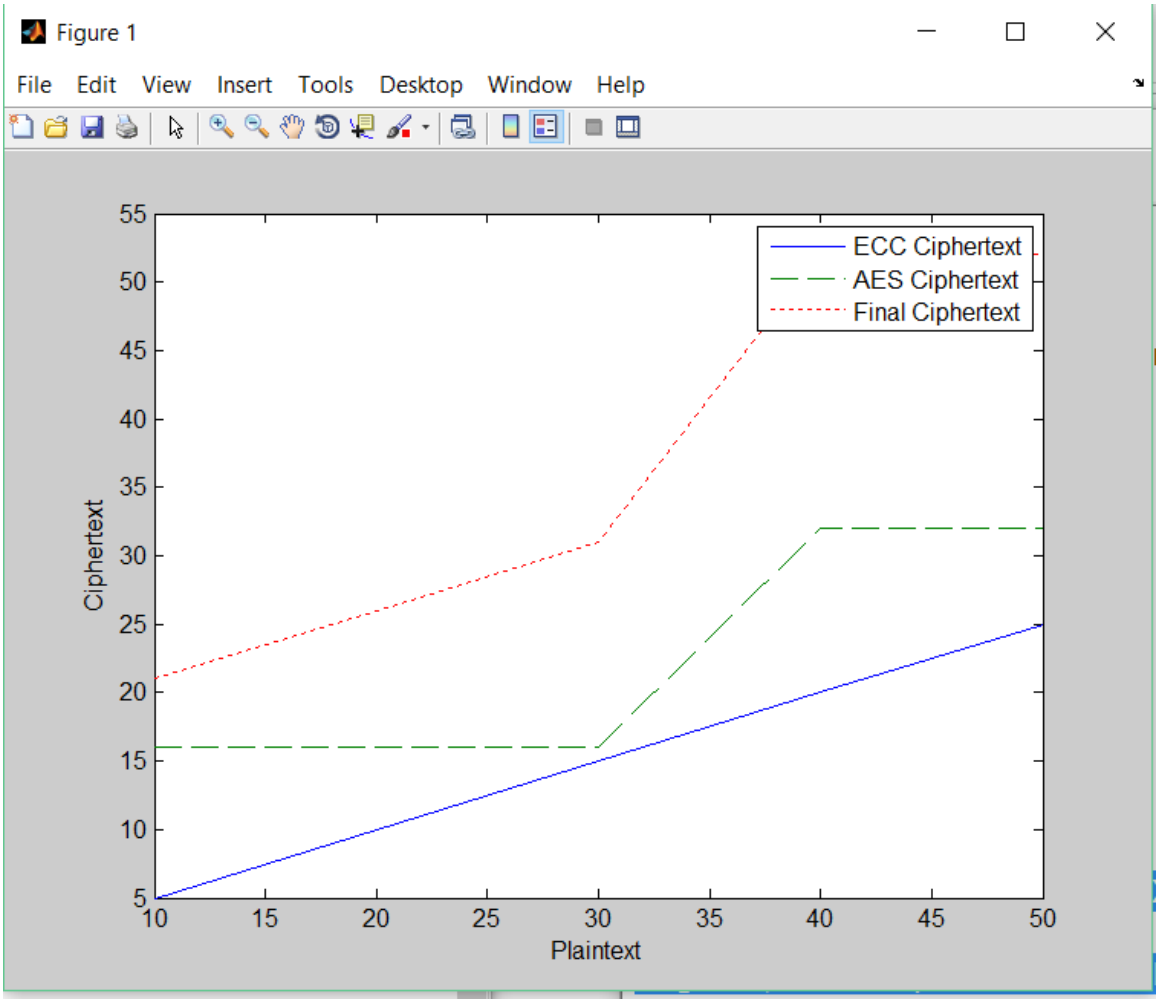


Figure 11: ECC & AES Cipher text

4.2 Comparison with existing technique

The proposed system is compared to the existing systems in terms of various factors that includes mutual authentication, ECDH and ECDH-AES key generation, encryption and decryption time, cipher text size (memory usage) and complexity.

1. Mutual Authentication:

In the existing systems there is no bound on data transmission and receiving of sensor nodes. None of the existing systems concerned about this security factor. They only explained about the algorithm, but they didn't explained how sensor after encrypting the data is going to send it to the exact destination. There is also no bound on transmission freshness to prevent replay attack. But in the proposed system there is bound on sensor communication, only after successful authentication of both source and destination they are able to communicate with one another. The proposed system also uses the timestamp value to check the freshness of communication during authentication, in order to avoid replay attack .this is one advantage of proposed system over existing systems.

2. Key Generation:

The existing systems uses secret key their algorithms like TCHA. So they requires secured channel for key sharing, which is almost impossible in the wireless communication. Another problem with the key sharing is that, if there is always the weakness of man in the middle attack, who can get key easily and thus intercept the ongoing transmission. But in our proposed system the keys for ECC and AES algorithms are generated using ECDH method. Thus we don't need any secure channel for key sharing. Another advantage is that ECDH keys are difficult for guessing and cryptanalysis because they use discrete properties of elliptical curves. This is another advantage of proposed system over existing systems.

3. Cipher text size (memory usage):

Table 4, shows the different sizes of the cipher texts produced by the various algorithms from the different inputs of the plane text, indirectly it shows the amount of the memory that we requires for the cipher text generation. In the table the highest size of cipher text is produced by the '*Kumar',* while the smallest size is produced by the *'Zhu'* and is very close to our proposed system. But when we look at the algorithm proposed by the *'Zhu'* it encrypts the message in the single phase that makes message less secure while our proposed system is more secure as compared to *'Zhu'* algorithm.

Table 4: Cipher text produced from plain text

Plain-text size (bytes)	***Dubal***	***Ren***	***Kumar***	***Zhu***	***Subasree***	***TCHA***	***HEA***
609	673	602	846	609	609	641	609
25615	25645	25610	35142	25615	25615	25647	25623
35080	35192	35070	48226	35080	35080	35112	35092
61386	61486	61369	84340	61386	61386	61418	61397
184162	184262	184143	253008	184162	184162	184194	184177

4. Encryption and Decryption Time:

Figure 9 and Figure 10 it is clear that the time taken by ECC algorithm is more for both encryption and decryption for smaller messages, but when size of plain text increases the encryption and decryption time increases slowly. Reverse is in case of AES algorithm, since it is symmetric so it takes smaller time as compared to the ECC algorithm which is asymmetric. Since both algorithms are running in parallel on two different parts of messages. Thus we needs to consider that algorithms execution time as the execution time of system in total which consumes more time. ECC consumes more time so we will consider the execution time of ECC as the total execution of whole system.

Table 5: Encryption time

Plain-text size (bytes)	***Dubal***	***Ren***	***Kumar***	***Zhu***	***Subasree***	***TCHA***	***HEA***
609	2032	1432	1500	998	2063	998	241
25615	6305	1490	1518	1022	3683	1022	327
35080	15,643	1468	1526	1059	5651	1059	363
61386	120,608	3019	4219	3143	15,351	3143	548
184162	198,700	4970	5752	3814	105,889	3814	881

Table 5, shows the encryption time (in milliseconds) taken by the existing systems as well as by our newly proposed system. In our system we are considering that there are two separate processing units where these two algorithms are executed in parallel. Another thing is that the data collected by sensors is encrypted simultaneously and are

sent after fixed intervals of time. The total time for encryption will also include the time of key generation.

Table 6, shows the decryption time (in milliseconds) taken by the existing systems as well as by our newly proposed system. In our system we are considering that there are two separate processing units where these two algorithms are executed in parallel. Another thing is that the data collected by sensors is encrypted simultaneously and are sent after fixed intervals of time. The total time for decryption will also include the time of key generation.

Table 6: Decryption time

Plain-text size (bytes)	***Dubal***	***Ren***	***Kumar***	***Zhu***	***Subasree***	***TCHA***	***HEA***
609	1016	756	996	562	1078	562	205
25615	4053	821	972	713	1085	713	245
35080	13227	953	980	824	1082	824	258
61386	13227	864	991	891	1197	891	297
184162	18578	1075	1099	907	2087	907	538

5. Algorithm Complexity:

In HEA, the algorithm complexity of encryption process is calculated as combined complexity of AES algorithm and ECC algorithm .The complexity of AES and ECC algorithm is: $O(log\ 2(n+1)+\sqrt{n}+4n)$ (*Kumar et al. 2012*).

Similarly the algorithm complexity of decryption process is calculated as combined decryption complexity of AES and ECC. The complexity of the proposed system for decryption is $O(log\ 2(n+1)+\sqrt{n}+5n)$ (*Kumar et al. 2012*).

Since we are executing algorithms in parallel so the calculated complexity is not going to effect on the complexity of whole algorithm.

The **Table 7** shows the encryption and decryption complexities of various algorithms.

Table 7: Algorithm Complexity

Algorithm	Encryption process	Decryption Process
Dubal	$O(log(\mathrm{n}^2)+\log 2(n)+\sqrt{n}+4n)$	$O(log\left(2\mathrm{n}^3\right)+\log 2(n)+\sqrt{n}+4n)$
Ren	$O(log(\mathrm{n}^2)+\sqrt{n}+4n)$	$O(log(\mathrm{n}^3)+\sqrt{n}+4n)$
Kumar	$O(log\ 2(n+1)+\sqrt{n}+4n)$	$O(log\ 2(n+1)+\sqrt{n}+5n)$
Zhu	$O(log\ 2(2n+1)+\sqrt{n}+4n)$	$O(log\ 2(2n+1)+\sqrt{n}+4n)$
Subasree	$O(log(\mathrm{n}^2)+4n)$	$O(log(2\mathrm{n}^3)+4n)$
TCHA	$O(log(\mathrm{n}^2)+\log(n)+3n)$	$O(log(\mathrm{n})+\log(2\mathrm{n}^3)+2n)$
HEA	$O(log\ 2(n+1)+\sqrt{n}+4n)$	$O(log\ 2(n+1)+\sqrt{n}+5n)$

CHAPTER 5
CONCLUSION AND FUTURE SCOPE

5.1 Conclusion

The proposed system presents the robust hybrid encryption algorithm for wireless body area networks. The main aim behind the design is to solve the several problems as practical implementation, secured key generation with ECHD, mutual authentication, short response time, efficient power consumption and strength of cryptosystem.

The proposed framework combines both methods of encryption that are symmetric as well as asymmetric. It combines the best features of both of them and also avoids the drawbacks of both systems. The HEA splits the plain text into two parts and then applies two different algorithms' on them so as confuse the attacker and also avoid the trap of cryptanalysis attack. The system does not require secured channel for key sharing and has also bound on communicate of participating sensors, that is only registered nodes can participate in communication. The proposed framework uses ECDH algorithm to generate a secured key for communication between the sink node and base station server. The framework uses hybrid algorithms: ECC-128 and AES-128 for data encryption. The proposed framework will be unique as it will provides a secure data movements in Wireless Body Area Networks (WBAN) with minimum costs and complexity without compromising the security.

Though the system is meant for wireless body area networks, using cloud and mainly focuses on remote patients for secure data transfer from sensor nodes to hospital cloud. The proposed algorithm can also be used other type of sensor networks e.g. in military areas. Consider a scenario where a fleet of fighter jets 'F16' is flying towards the enemy territory, all the fighter plane are connected with SAAB AEW&C for frequents updates about enemy positions and friendlies. Here everything relies upon sensors and their communication. Here is need for secure data moments between base station (SAAB) and sink (F16) radar.

5.2 Future Scope

The proposed framework can be used in every area of networking where encryption is required. We can use the proposed algorithm in future for ad-hoc as well for non-ad-hoc networks, whenever encryption is required. The algorithm can also overcome the problem of, requirement of secured channel for key sharing. The algorithm's working is not only bound to the WBAN rather it can be used anywhere, where there is sensor network like in battlefields, remote sensing or in research.

REFERENCES

[1] R. Merkle “protocol for public key cryptosystem,” in proc, IEEE S&P, 1980 ,pp. 133-134.

[2] M. Bellare, H.Krawczyk, and R.canetti, “HMAC: Keyed–hashing for message authentication,” RFC 2104, 1996.

[3] P. Golle, J. Staddon, and B.Waters, “secure conjunctive keyword search over encrypted data, “ in proc. ACNS,2004,pp. 31-45.

[4] Vimal Upadhyay, Pintu Kashyap, Inder Kumar, Jai Balwan , Lalit Choudhary “ secure data in wireless sensor network via des” International Journal of Enterprise Computing and Business Systems ISSN (Online) : 2230-8849

[5] Sadaqat Ur Rehman, Muhammad Bilal, Basharat Ahmad, Khawaja Muhammad Yahya, Anees Ullah, Obaid Ur Rehman “Comparison Based Analysis of Different Cryptographic and Encryption Techniques Using Message Authentication Code (MAC) in Wireless Sensor Networks (WSN)” IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 1, No 2, January 2012

[6] Dawn Xiaodong Song David Wagner Adrian Perrig “Practical Techniques for Searches on Encrypted Data” Security and Privacy, 2000. S&P 2000. Proceedings. 2000 IEEE Symposium on 2002.

[7] Adrian Perrig, Robert Szewczyk, J. D. Tygar, Victor Wen David E. Culler “ SPINS: security protocols for sensor networks” Wireless Networks 8, 521.534, 2002 Kluwer Academic Publishers. Manufactured in the Netherlands.

[8] Hakan Hacıgumus¸ Bala Iyer Chen Li Sharad Mehrotra, “Executing SQL over Encrypted Data in the Database Service Provider Model” in 2002.

[9] Michael Gertz, April Kwong, Charles U. Marte, Glen Nuckolls, “Databases that tell the Truth: Authentic Data Publication”, Copyright 2004 IEEE (Volume:16 , Issue: 10)

[10] Lingxuan Hu, David Evans “Secure Aggregation for Wireless Networks ” NationalScience Foundation (CCR-0092945 and EIA0205327) , in 2004

[11] Bijit Hore, Sharad Mehrotra, Gene Tsudik “A Privacy-Preserving Index for Range Queries” Proceedings of the 30th VLDB Conference, Toronto, Canada, 2004 .

[12] Wenliang Du, Jing Deng, Yunghsiang S. Han, “A Key Management Scheme for Wireless Sensor Networks Using Deployment Knowledge” in 2004

[13] Ronald Watro, Derrick Kong, Sue-fen Cuti, Charles Gardiner “TinyPK: Securing Sensor Networks with Public Key Technology’ Copyright 2004 ACM 1-58113-972-1/04/0010

[14] Michael Gertz , April Kwong , Charles U. Martel, “Databases that tell the Truth: Authentic

Data Publication ” in 2004.

[15] Gunnar Gaubatz, Jens-Peter Kaps, Berk Sunar, “Public Key Cryptography in Sensor Networks Revisited ” Grants No. ANI-0133297 (NSF CAREER Award) and No. ANI-0112889.in 2004

[16] Gaubatz,G., Kaps, J.-P., Ozturk, E. Sunar, B “State of the art in ultra-low power public key cryptography for wireless sensor networks” NSF Grants No. ANI-0133297 (NSF CAREER Award) and No. ANI-0112889. In 2005

[17] Donggang Liu, Peng Ning, Rongfang Li “ Establishing pairwise keys in distributed sensor networks” CCS’03, October 27–31, 2005, Washington, DC, USA

[18] Ren, W., Miao, Z., 2010. A hybrid encryption algorithm based on DES and RSA in bluetooth communication. In: Proceedings of the 2nd International

Conference on Modeling, Simulation and Visualization Methods, China, pp. 221–225..

[19] Luk, M, Mezzour, G. ; Perrig, A. ; Gligor, V. “MiniSec: A Secure Sensor Network Communication Architecture ”, Information Processing in Sensor Networks, 2007. IPSN 2007. 6th International Symposium.

[20] de Meulenaer, G, Gosset, F. ; Standaert, O.-X. ; Pereira, o “On the Energy Cost of Communication and Cryptography in Wireless Sensor Networks”, Networking and Communications, 2008. WIMOB '08. IEEE International Conference on Wireless and Mobile Computing,

[21] Roberto Di Pietroa, Alexandre Viejob“Location privacy and resilience in wireless sensor networks querying” Computer Communications Volume 34, Issue 3, 15 March 2011, Pages 515–523

[22] Xueying Zhang, Heys, H.M. ; Cheng Li ,“ Energy efficiency of symmetric key cryptographic algorithms in wireless sensor networks”, Communications (QBSC), 2010 25th Biennial Symposium.

[23] Subhankar Chattopadhyay et.al, “A Scheme for Key Revocation in Wireless Sensor Networks”, International Journal on Advanced Computer Engineering and Communication Technology (IJACECT) in 2010.

[24] Yang Zhao a, et.al ,“A co-commitment based secure data collection scheme for tiered wireless sensor networks” in 2010, Published by Elsevier B.V.doi:10.1016/j.sysarc.2010.05.010.

[25] Ashok Kumar Das,” a key establishment scheme for mobile wireless sensor networks using post-deployment knowledge”, Published in International Journal of Computer Networks & Communications (IJCNC) Vol.3, No.4, July 2011

[26] Jing Shi, “A Spatiotemporal Approach for Secure Range Queries in Tiered Sensor

Networks", Wireless Communications, IEEE Transactions on (Volume:10 , Issue: 1) 2011.

[27] Anderson Santana de Oliveira, Hoon Wei Lim, Su-Yang Yu " Privacy-Preserving Techniques and System for Streaming Databases" in 2012.

[28] Fei Chen and Alex X. Liu , "Privacy and Integrity Preserving Range Queries in Sensor Networks" in Dec. 2012. Networking, IEEE/ACM Transactions on (Volume:20 , Issue: 6)

[29] F. Aslam, A. Ali, H. Abbas, N. Al, and H. Haldar, "A cloud-based healthcare framework for security and patients ' data privacy using wireless body area networks," Procedia - Procedia Comput. Sci., vol. 34, pp. 511–517, 2014.

[30] Zhu, S., 2011. Research of hybrid cipher algorithm application to hydraulic information transmission. In: Proceedings of International Conference on Electronics, Communications and Control (ICECC), China.

[31] S. K. Shankar, A. S. Tomar, and G. K. Tak, "Secure Medical Data Transmission by using ECC with Mutual Authentication in WSNs," Procedia - Procedia Comput. Sci., vol. 70, pp. 455–461, 2015.

[32] R. Rizk and Y. Alkady, "Two-phase hybrid cryptography algorithm for wireless sensor networks," J. Electr. Syst. Inf. Technol., vol. 2, no. 3, pp. 296–313, 2015.

[33] Dubal, M.J., Mahesh, T.R., Ghosh, P.A., 2011. Design of a new security protocol using hybrid cryptography architecture. In: Proceedings of 3rd International Conference on Electronics Computer Technology (ICECT), vol. 5, India.

[34] Hossain, Md.A., Islam, Md.K., Das, S.K., Nashiry, Md.A., 2012. Cryptanalyzing of message digest algorithms MD4 and MD5. Int. J. Cryptogr. Inf. Secur. (IJCIS) 2 (1).

[35] Kumar, N., 2012. A Secure Communication Wireless Sensor Networks Through Hybrid (AES+ECC) Algorithm, vol. 386. von LAP LAMBERT Academic Publishing.

[36] Subasree, S., Sakthivel, N.K., 2010. Design of a new security protocol using hybrid cryptography algorithms. IJRRAS 2 (2), 95–103.