Developing a Low-Cost Security Model for Small Scale Healthcare Organizations using the Internet of Things

Project report submitted in partial fulfillment of the requirement for thedegree of Bachelor of Technology
In

Computer Science and Engineering

By

ShilpiKumari(141379)

Arushi Dogra(141222)

Under the supervisionof

(Dr. Ravindara Bhatt)

To

Department of Computer Science & Engineering and Information Technology

Jaypee University of Information Technology Waknaghat, Solan-173234, Himachal Pradesh

CERTIFICATE

Candidate's Declaration

This is to certify that the work which is being presented in the report entitled **"Developing a Low-Cost Security Model for Small Scale Healthcare Organizations using the Internet of Things"** in partial fulfillment of the requirements for the award of the degree of **Bachelor of Technology** in **Computer Science and Engineering/Information Technology** submitted in the department of Computer Science & Engineering and Information Technology**,** Jaypee University of Information Technology Waknaghat is an authentic record of our own work carried out over a period from August 2017 to May 2018 under the supervision of **Dr. Ravindara Bhatt** (Assistant Professor, Senior Grade, Computer Science &EngineeringDepartment).

The matter embodied in the report has not been submitted for the award of any other degree or diploma.

ShilpiKumari, 141379 **Arushi Dogra, 141222**

This is to certify that the above statement made by the candidates is true to the best of my knowledge.

Dr. Ravindara Bhatt
Assistant Professor (Senior Grade)
Computer Science & Engineering Department
Dated:

ACKNOWLEDGEMENT

We owe our profound gratitude to our project supervisor **Dr. Ravindara Bhatt**, who took keen interest and guided us all along in my project work titled **—Developing a Low-Cost Security Model for Small Scale Healthcare Organizations using the Internet of Things**, till the completion of our project by providing all the necessary information for developing the project. The project development helped us in research and we got to know a lot of new things in our domain. We are really thankful to him.

TABLE OF CONTENTS

List of Abbreviations

S.NO.	ABBREVIATIONS	DESCRIPTION
1	IOT	Internet of Things
2	TEA	Tiny Encryption Algorithm

LIST OF FIGURES

List of Graphs

LIST OF TABLES

ABSTRACT

The Internet of Things (IoT) makes smart objects the ultimate building blocks in the development of cyber-physical smart pervasive frameworks. The IoT has a variety of application domains, including health care. The IoT revolution is redesigning modern health care with promising technological, economic, and social prospects. It finds enormous applications in the field of healthcare monitoring , information management system , agriculture, predicting the natural disaster etc. In all those applications of IoT, security plays a vital role . This project is indented to give an Implementation of developing a low-cost security model for small scale healthcare organizations using the Internet of Things .

There are many emerging areas in which highly constrained devices are interconnected and communicated to accomplish some tasks. Nowadays, Internet of Things (IoT) enables many low resources and constrained devices to communicate, compute process and make decision in the communication network. In the heterogeneous environments for IoT, there are many challenges and issues like power consumption of devices, limited battery, memory space, performance cost , and security in the Information Communication Technology (ICT) network. We will use light weight algorithm. The light weight Encryption Algorithm is a cryptographic algorithm designed to minimize memory footprint and maximize speed.

1. Chapter-1INTRODUCTION

1.1Introduction

The Internet of Things (IoT) is a concept reflecting a connected set of anyone, anything, anytime , anyplace, any service, and any network . The IoT is a megatrend in next generation technologies that can impact the whole business spectrum and can be thought of as the interconnection of uniquely identifiable smart objects and devices within today's internet infrastructure with extended benefits. Benefits typically include the advanced connectivity of these devices, systems, and services that goes beyond machine-to-machine (M2M) scenarios. Therefore, introducing automation is conceivable in nearly every field. The IoT provides appropriate solutions for a wide range of applications such as smart cities, traffic congestion, waste management, structural health, security , emergency services , logistics, retails, industrial control, and health care. Medical care and health care represent one of the most attractive application areas for the IoT. The IoT has the potential to give rise to many medical applications such as remote health monitoring, chronic diseases, and elderly care. Compliance with treatment and medication at home and by healthcare providers is another important potential application. Therefore, various medical devices, sensors, and diagnostic and imaging devices can be viewed as smart devices or objects constituting a core part of the IoT. IoT-based healthcare services are expected to reduce costs, increase the quality of life, and enrich the user's experience .

The proposed project is an aim at providing better security solutions to the healthcare system and thus make it a more reliable source. Any application or any communication between a hospital and a patient can be made more secure by the use of powerful cryptographic algorithms such as Light weight and Tiny Encryption algorithm.

The project aims at choosing the best alternative among the various cryptographic techniques available. The given document discusses the uses, advantages and disadvantages of various cryptographic algorithms and provides a comparative analysis for the same .

1.2 Problem Statement

With the increasing need andi dependence on Internet of Things and a similar increase in the advancement of healthcare, the earlier measures and methods of ensuring secure and reliable transfer of data have found to be insufficient and unreliable. The numbers of cryptanalytic attacks have increased manifolds because of the faster technology available which poses a serious threat on the integrity of user and user information addressed. Also there is an increasing need for the development of reliable methods for hiding of information so that everything is not visible to everyone.

In particular , this healthcare application explicitly addresses the issue of security and strives to find better and more dependable ways of providing data security by means of using Light weight and Tiny encryption algorithms.

1.3Objectives

The main objective of this project is to study IoT based healthcare system as a part and necessity in today's world, its importance and why it has become such a big topic for discussion. And therefore the project aims at understanding the potential risks and threats present along with it and why ensuring security of data is of primary concern. The objective of this project is to study the various used and encryption algorithms available for security provision and finally finding the most suitable and effective combination for the same.

The emphasis is on finding the practical implications of the results proposed and not only focusing on the theoretical concepts.

The motive is to become completely aware and familiar with the technology used for the implementation of the project and make the best use of it for our project completion. Thus we aim at drawing out results which could be used in future in real-time projects by means of collective learning, problem solving and collaborative research work through proper coordination and cooperation.

1.4 Methodology

- **Light weight Algorithm:** This step involves the development of a suitable combination of cryptographic algorithms that best serves our purpose. The combination can be then tested on various parameters such as encryption speed, throughput etc.

- **Application Design:** We then create a client-server user application which can be used as a framework for testing the Light weightalgorithm.

- **Integration of security in healthcare system:** In this step we add the various security features in our application such as Light weight and Tiny encryption algorithms for user authentication and encryption of data that would be stored in a database .

- **Deployment on healthcare system:** In this step we finally deploy our test application on healthcare system.

2. Chapter-2 LITERATURESURVEY

S.No	Title	Approach	Conclusion
1	**"The Internet of Things for Health Care: A Comprehensive Survey"**	The Internet of Things (IoT) is a concept reacting aconnected set of anyone, anything, anytime, anyplace, any service, and any network. The IoT is megatrend in next-generation technologies that can impact the whole business spectrum and can be thought of as the interconnection of uniquely identiable smart objects and deviceswithin today's internet infrastructure with extended benefits. Benefits typically include the advanced connectivity of these devices, systems, and services that goes beyond machineto-machine (M2M) scenarios [1]. Therefore, introducing automation is conceivable in nearly every field. The IoT provides appropriat solutions for a wide range of applications suchias smart cities, traffic congestion, waste management, structural health, security, emergency services, logistics, retails, industrial control, and	This paper proposes a Researchers across the world have started to explore various technological solutions to enhance healthcare provision in a manner that complements existing services by mobilizing the potential of the IoT. This paper surveys diverse aspects of IoT-based healthcare technologies and presents various healthcare network architectures and platforms that support access to the IoT backbone and facilitate medical data transmission and reception. Substantial R&D efforts have been made in IoT-driven healthcare services and applications. In addition, the paper provides detailed research activities concerning how the IoT can address pediatric and elderly care, chronic disease supervision, private health. For deeper insights into industry trends and enabling technologies, the paper offers a broad view on how recent and

		health care. The interested reader is referred to [1]_[5] for a deeper understanding of the IoT. Medical care and health care represent one of the most attractive application areas for the IoT [6].	ongoing advances in sensors, devices, internet applications, and otheritechnologiesihave motivated affordable healthcare gadgets and connected health services to limitlessly expand the potential of IoT-based healthcare services for further developments. To better understand IoT healthcare security, the paper considers various security requirements and challenges and unveils different research problems in this area to propose a model tha t can mitigate associated security risks. The discussion on several important issues such as standardization, network type, business models, the quality of service, and health data protection is expected to facilitate the provide a basis for further research on IoT-based healthcare services. This paper presents eHealth and IoT policies and regulations for the benefit of various stakeholders interested in assessing IoT-based healthcare technologies.
2	**Advancedlightweig**	There are many emerging	In this paper, we have

	ht Encryption algorithms for IoTdevices: survey, challenges and solutions”	areas in which highly constrained devices are interconnected and communicated to accomplish some tasks. Nowadays, IoT enables many low resources and constrained devices to communicate, compute process and make decision in the communication network. In the heterogeneous environments for IoT, there are many challenges and issues like power consumption of devices, limited battery, memory space, performance cost, and security in the Information Communication Technology (ICT) network. In this paper, we discuss a state-of-art of lightweight cryptographic primitive which include lightweight block ciphers, hash function, stream ciphers, high performance system, and low resource device for IoT environment in details. We analyze many lightweight cryptographic algorithms based on their key size, block size, number of rounds, and structures. In addition, we discuss the security architecture	gone over lightweight cryptographic algorithm in detail. Many low-resource device perform computation in an IoT environment. These devices are limit in regards to memory, battery life, power consumption, and computations. IoT devices also face the challenges of security and privacy as well as the issue of how to maintain trust between IoT users. Furthermore, we summarized different kinds of lightweight cryptographic algorithm that are easy to use for hardware and software implementations. Cryptographic algorithm is vulnerable to some kinds of attacks, which we also described in the paper. It is important to develop more secure and lightweight encryption algorithms that have a smaller key size, fast processing,and require less computation power. In this paper, we proposed a scheme that can be applied in the smart home environment. We also discussed open issues in terms of cipher structure,

		in IoT for constrained device environment and focus on research challenges, issue and solutions.	implementation, block size, key size, new attacks, and security metrics. In the future, we will examine how expensive these solutions are and if it is possible to implement them in a constrained environment. In addition, an algorithm for calculating the threshold value of each device parameter, which has already been laid out in our proposed scheme, should be developed.
3	**A CRYPTANALYSIS OF THE TINY ENCRYPTIONAL GORITHM**	The author of this paper give us a brief idea about what tiny algorithm is and its characteristic and also provides the various advantage of tiny encryption algorithm [8] **Tiny Encryption Algorithm:** The Tiny Encryption Algorithm (TEA) is a cryptographic algorithm designed to minimize memory footprint and maximize speed. It a Feistel type cipher that uses operations from mixed (orthogonal) algebraic groups. The research presents the cryptanalysis of the Tiny	In research found encryption of cipher texts with few round to be weak. Encryption of cipher text with more than six rounds produced a very good mixture of intermediate values and showed high resistance to cryptanalytic attacks. TEA as a best fit cryptographic algorithm for small device where memory and power are primary concern.

		Encryption Algorithm. In this research we inspected the most common methods in the cryptanalysis of a block cipher algorithm. TEA seems to be highly resistant to differential cryptanalysis, and achieves complete diffusion (where a one- bit difference in the plaintext will cause approximately 32 bit differences in the cipher text) after only six rounds. Time performance on a modern desktop computer or workstation is impressive.	
4	**Light Weight Cryptographic Algorithms for Medical Internet of Things (IoT) - A Review**	Amer Abbas et.al (2014) implemented the VHDL design of PRINCE algorithm on Field programmable gate array (FPGA). The input size of 64 bit and key size of 128 bit followed for the 12 rounds. The steps involved in the algorithm are Round function, Round dependent constant, S- box Layer, Linear diffusion Layer and Middle Involution. The author implemented the proposed PRINCE algorithm in vertex 4 and vertex 6 FPGA kit and they proved vertex 6	Due to the advancements in the technology, Internet ofThings becomes part in our day to day life. Even though it finds enormous applications it is lack in security. In this paper, a detailed review on various security algorithms isdone. Comparison between the various algorithms is also made in terms of its key size, block size and its performance. This gives an overview on the limitations of the existing security techniques and lays a platform to propose a

		gives high throughput, high efficiency and low power consumption. They also proved PRINCE algorithm gives better performance compared to the already proposed ICEBERG and SEA algorithm [9]. The author simulated HEIGHT algorithm using Altera Quartus IIversion 11 and version 13. They proved version 13 gives low latency and high speed. They also proved that Hardware showed better efficiency then software [10]. Sridevi et.al (2015) efficiently implemented the advanced Encryption system (AES) on FPGA. AES performs in four modes. The modes are listed as follows, Electronic code block (ECB), Cipher block chaining, Cipher feedback mode (CFB) and output feedback mode. The input size of 128 bit and variable key size are 128, 192, 256 bits Depends on the size of the key, no of rounds (10, 12, 14) are varied. The steps involved in the algorithm are sub bytes, shift rows, mix column, Add round key.	novel light weight technique with minimum number of block size and key size.

		They analyzed the AES algorithm in four ways to increase the throughput as follows: AES was implemented in silicon platform, The structure is modified to pipelined and implemented on FPGA kit, S-box of AES algorithm is replaced by T-box , T-box AES is modified to pipelined architecture. They proved pipelined structure of T-box AES on ECB mode showing higher throughput on FPGA kit [11].	
5	**Advanced Internet of Things for Personalized Healthcare System: A Survey**	As a new revolution of the Internet, Internet of Things (IoT) is rapidly gaining ground as a new research topic in many academic and industrial disciplines, especially in healthcare.Remarkably, due to the rapid proliferation of wearable devicesand smartphone, the Internet of Things enabled technology is evolving healthcare from conventional hub based system to morepersonalized healthcare system (PHS)[12]. However, empowering theutility of advanced IoT technology in PHS is still significantly	Internet of Things paradigm represents the vision of the nextwave of ICT revolution. IoT enabled technology in PHS willenable faster and safer preventive care, lower overall cost, improved patient-centered practice and enhanced un stainability.IoT enabled PHS have the potential to enhance our everyday life in many different aspects and, in particular. In this survey, we explored the application of IoT in healthcare from various perspectives. We reviewed the existing state-of-the-art technologies for IoT enabled

		challenging in the area considering many issues, likeshortage of cost-effective and accurate smart medicalsensors,unstandardizedIoT system architectures, heterogeneity of connected wearabledevices, multi-dimensionality of data generated and high demand for interoperability[13]. In an effect to understand advance of IoT technologies in PHS, this paper will give a systematic review on advanced IoT enabled PHS. It will review the current research ofIoT enabled PHS, and key enabling technologies, major IoT enabled applications and successful case studies in healthcare, andfinally point out future research trends and challenges[14-15].	healthcare applications. From a different perspective, we discussed current technology and infrastructure, such as sensing, networking and data processingtechnologies. More importantly, we provided a high leveldescription of various IoT enabled healthcare applications. But,we are aware that the goals set up for IoT in healthcare are noteasily reachable, and there are still many challenges to be facedand, consequently, this research field is getting more and moreimpetus. Researchers with different backgrounds are enhancingthe current state of the art of IoT in healthcare by addressing fundamental problems related to human factors, intelligence design and implementation, and security, social, and ethical issues. As a result, we are confident that this synergic approach will materialize the complete vision of IoT and its full application in healthcare and human wellbeing.
6	**Internet of Things for Smart**	In this work, we have proposed a unique model for future IoT-	Research in related fields has shown that remote health

	Healthcare: Technologies, Challenges, and Opportunities	based healthcare systems, which can be applied to both general systems and systems that monitor specific conditions. We then presented a thorough and systematic overview of thestate-of-the-art work relating to each component of the proposed model. Several wearable, non-intrusive sensors were presented and analyzed, with particular focus on those monitoring vital signs, blood pressure, and blood oxygen levels. Short-range and long-range communications standard were then compared in terms of suitability for healthcare applications. BLE and NB-IoT emerged as the most suitable standards for short-range and long-range communications in healthcare respectively	monitoring is plausible, but perhaps more important are the benefits it could provide in difference contexts.
7	**Security for the Internet of Things: A Survey of Existing Protocols and Open Research Issues**	The Internet of Things (IoT) introduces a vision of a future Internet where users, computing systems, and everyday objects possessing sensing and actuating capabilities cooperate with unprecedented convenience and economical benefits. As with the current Internet architecture, IP-based	A glimpse of the IoT may be already visible in current deployment where networks of sensing devices are being interconnected with the Internet, and IP-based standard technologies will be fundamental in providing a common and

		communication protocols will play a key role in enabling the ubiquitous connectivity of devices in the context of IoT applications. Such communication technologies are being develope in line with the constraints of the sensing platforms likely to be employed by IoT applications, forming a communications stack able to provide there required power efficiency, reliability, and Internet connectivity.As security will be a fundamental enabling factor of most IoT applications, mechanisms must also be designed to protect communications enabledlby such technologies. This survey analyzes existing protocols and mechanisms to secure communications inthe IoT, as well as open research issues. We analyze how existing approaches ensure fundamental security requirements and protect communications on the IoT, together with the open challenges and strategies for future research work in the area.	well accepted ground for the development and deployment of new IoT applications. Considering that security may be an enabling factor of many of such applications, mechanisms to secure communication using communication technologies for the IoT will be fundamental. With such aspects in mind, in the survey we perform an exhaustive analysis on the security protocol and mechanisms available to protect communications on the IoT.We also address existing research proposals and challenges provid ing opportunities for future research work in the area. we summarize the main characteristics of the mechanisms and proposals analyzed throughout the survey, together with its operational layer and the security properties and functionalities supported. In conclusion, we believe this survey may provide an important contribution to the research community, by documenting the current status of important

		This is, as far asour knowledge goes, the first survey with such goals**.**	and very dynamic area of research, helping readers interested indeveloping new solutions to address security in the context of communication protocol for the IoT.

Advantages

Many researchers have worked on designing and implementing various IoT-based healthcare services and onisolving various technological and architectural problems associated with those services. In addition to research concerns in the literature, there are several other challenges and open issues that need to be carefully addressed. This section briefly presents bot explored and unexplored issues surrounding IoT healthcare services.

A. Standardization

In the healthcare context, there are many vendors that manufacture a diverse range of products and devices, and new vendors continue to join this promisingtechnological race. However, they have not followed standard rules and regulations for compatible interfaces and protocols across devices. This raises interoperability issues. To address device diversity, immediate efforts are required. For example, a dedicated group can standardize IoT-based healthcare technologies. This standardization should consider a wide range of topics such as communications layers and protocol stacks, including physical (PHY) and media access control (MAC) layers, device interfaces, data aggregation interfaces, and gateway interfaces. The management of various value-added services such as electronic health records is another standardization issue. This management comes in various forms, includ access management and healthcare professional registration. Various Health and eHealth organizations and IoT researchers can work together, and existing standardization bodiesisuch as the Information Technology and Innovation Foundation (IETF), the Internet Protocol for Smart Objects (IPSO) alliance, and the European Telecommunications Standards Institute (ETSI) can form IoT technology working groups for the standardization of IoT-based healthcare services.

IoT HealthcarePlatforms

The architecture of IoT-based healthcare hardware is more sophisticated than that of usual IoT devices and requires a real-time operating system with more stringent requirements, there is a need for a customized computing platform with run-time libraries. To build a suitable platform, a service-oriented approach (SOA) can be taken such that services can be exploited by using different application packageinterfaces(APIs). Iniaddition to a specialized platform, libraries and appropriateframeworks should be built so that healthcare software developers and designers can make efficient use of given documents, codes, classes, message templates, and other useful data. Further, a particular class of disease-oriented libraries can be useful.

B. CostAnalysis

Researchers may perceive IoT-based healthcare services as a low-cost technology, but to the authors knowledge, no comparative study has offered any evidence of this. In this regard, a cost analysis of a typical IoThNet may be useful.

C. The App Development Process

There are four basic steps in developing an appiont the android platform: the setup, development, debugging and testing, and publishing. Similar approaches are generally taken on other platforms. In the process of health care app development, the participation of an authorized body or association of medical experts is typically required to ensure an app of acceptable quality. In addition, regular updates on healthcare apps based on the due consideration of recent advances in medical science are vital.

D. Technology Transition

Healthcare organizations can modernize their existing devices and sensors across the healthcare field for smart resources by incorporating IoT approaches into the existing network configuration. Therefore, a seamless transition from the legacy system and setup to an IoT-based configuration is a major challenge. In other words, there is a need to ensure backward compatibility and flexibility in the integration of existing devices.

E. The Low-Power Protocol

There are manyidevices in IoT healthcare scenarios, and such devices tend to be heterogeneous in terms of their sleep, deep-sleep, receive, transmit, and composite states, among others. In terms of service availability,each communications layer faces an additional challenge in terms of power requirements.

F. Network Type

In terms of the design approach, an IoT healthcare network can be of one of three fundamentally different types: data-, service-, and patient-centric architectures. In the data-centric scheme, the healthcare structure can generally be separated into objects based on captured health data. In a service-centric scheme, the healthcare structure is allocated by the assembly of characteristics that they must provide. In the patient-centric scheme, healthcare systems are divided according to the involvement of patients andtheir family members they consider for treatment. In this regard, answering the question of what network type is appropriate for IoT-based healthcare solutions becomes an open issue.

G. Scalability

IoT healthcare networks, applications, services, and back-end database should be scalable because related operations become more complex with the addition of diverse applications as a result of the exponential growth of demands from both individuals and health organizations.

H. Continuous Monitoring

There are many situations in which patients require long-term monitoring (e.g., a patient with a chronic disease). In this regard, the provision of constant monitoring and logging is vital.

I. New Diseases and Disorders

Smart phones are being considered as a frontier IoT healthcare device. Although there are many healthcare apps and new apps are being added to the list every day, the trend has been limited to a few categories of diseases.

J. Identification

Healthcare organization deal with multi-patient environments in which multiple caregivers discharge their duties. From this perspective, the proper identification of patients and caregivers is necessary.

K. The Business Model

The IoT healthcare business strategy is not yet robust because it involves a set of elements with new requirements such as new operational processes and policies, new infrastructure systems, distributed target customers, and transformed organizational structures. In addition, doctors and nurses generally avoid learning and using new technologies. Therefore, there is an urgent need for a new business model.

L. The Quality of Service (QoS)

Healthcare services are highly time sensitive and require QoS guarantees initerms of important parameters such as reliability, maintainability, and the service level. In this regard, the quantitative measurement of each such parameter within the IoThNet framework may be useful.

M. Data Protection

The protection of captured health data from various sensors and devices from illicit access is crucial. Therefore, stringent policies and technical security measures should be introduced to share health data with authorized users, organizations, and applications.

1) Resource-Efficient Security

Because of resource (power, computation, and memory) constraints, IoT healthcare security schemes should be designed to maximize security performance while minimizing resource consumption.

2) Physical Security

An attacker may tamper with and capture physical health devices and extract cryptographic secrets, the attacker may modify programs or replace captured devices with malicious ones. Therefore, devices should include tamper-resistant packaging.

3) SecureRouting

Routing protocols for the IoT health network are particularly susceptible to device-capture attacks. Therefore, proper routing and forwarding methods are vital for real-time or semi-real-time communication in the desired network.

4) DataTransparency

IoT medical devices deal with personal heath data that may be used in IoT cloud services. Therefore, data-transparent services should be designed and developed such that the life cycle of personal data can be traced and data use can be controlled.

The Security of Handling IoT

Biomedical sensors and devices generate huge amounts of health data, and there is a need to securely store captured data. Providing security measures for handling such data, including date transfer and maintenance, without compromising integrity, privacy, and confidentiality requires close attention and much effort.

N. Mobility

The IoT healthcare network must have the ability to support the mobility of patients such that they can be connected anywhere, anytime. This mobility feature is ultimately responsible for connecting dissimilar patient environments.

O. EcologicalImpact

The full-scale deployment of IoT-based healthcare services requires many biomedical sensors embedded in semiconductor-rich devices. These sensors and devices also include rare earth metals and severely toxic chemicals. This has substantially unfavorable impacts on the environment, users, and human health, and for this reason, guidelines are needed for device manufacturing, the use of devices, and their proper disposal.

3. Chapter-3 SYSTEMDEVELOPMENT

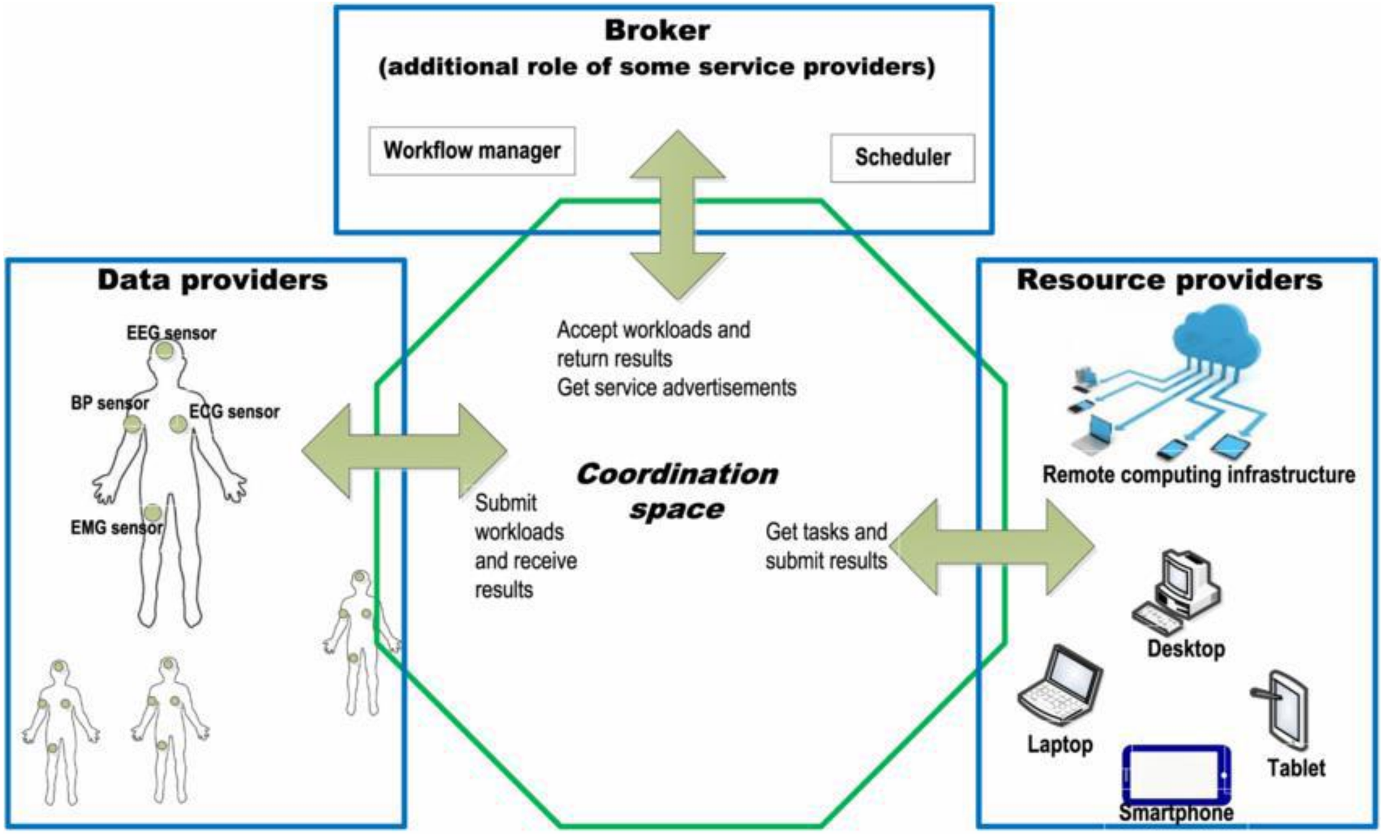
SOFTWARE REQUIREMENTS:

- Netbeans IDE 8 or above
- JDK(Java Development Kit) 1.7 orabove
- matlab

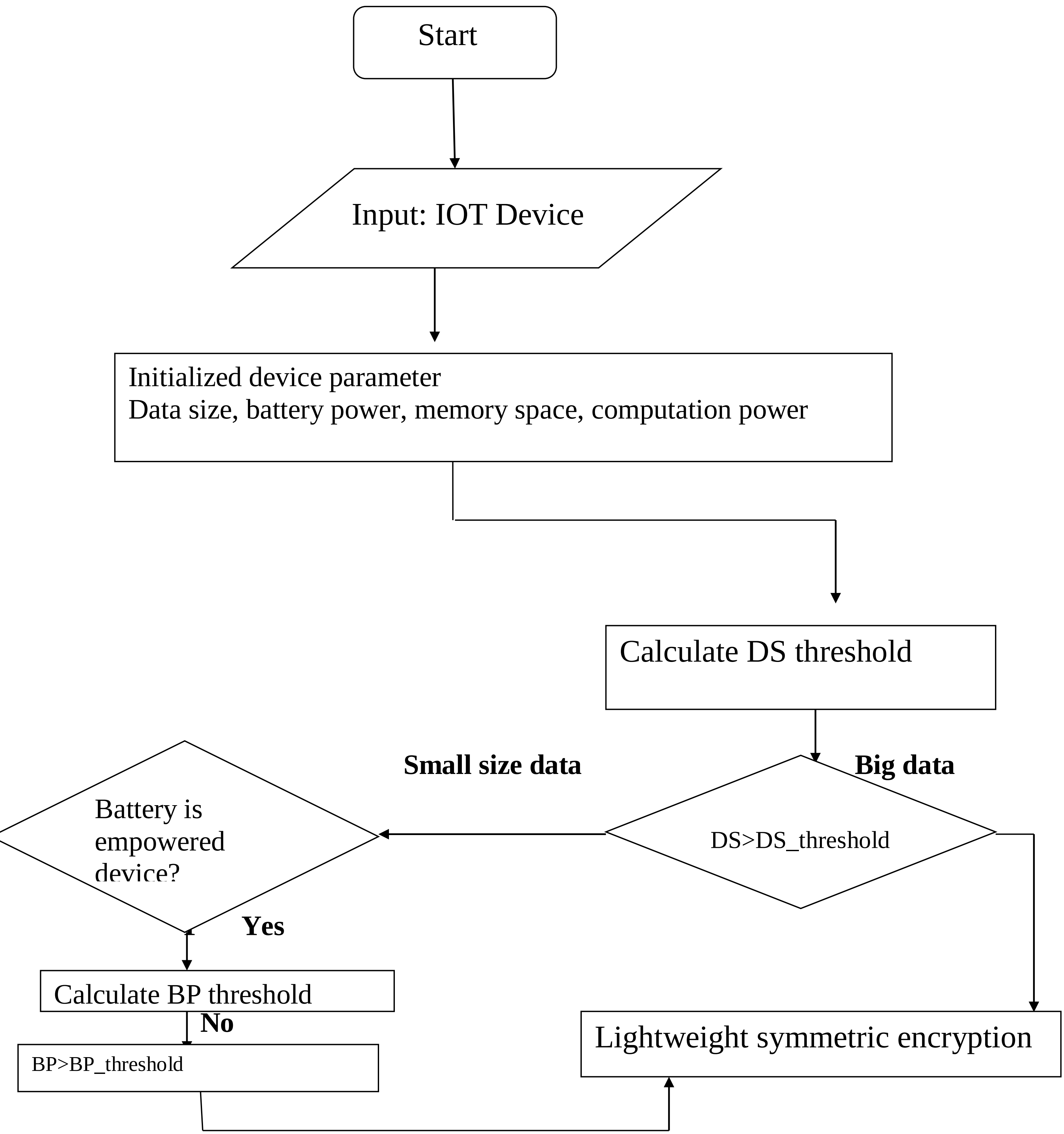
HARDWAREREQUIREMENTS:

- **SystemRequirements:**
  - ✓ CPU: 2.2 GHz Processor and above
  - ✓ RAM: 2 GB orabove
  - ✓ OS: Windows 7 orabove

PROPOSED DESIGN:



SYSTEMDESIGN:



Algorithm

```
void code(long* v, long* k) {

unsigned long y = v[0], z = v[1], sum = 0

delta = 0x9e3779b9, n = 32 ;

while (n-->0) {

sum += delta ;

y += (z<<4)+k[0] ^ z+sum ^ (z>>5)+k[1] ;

z += (y<<4)+k[2] ^ y+sum ^ (y>>5)+k[3] ;

}
                v[0] = y ; v[1] = z ; }
```

4. Chapter-4 PERFORMANCE ANALYSIS

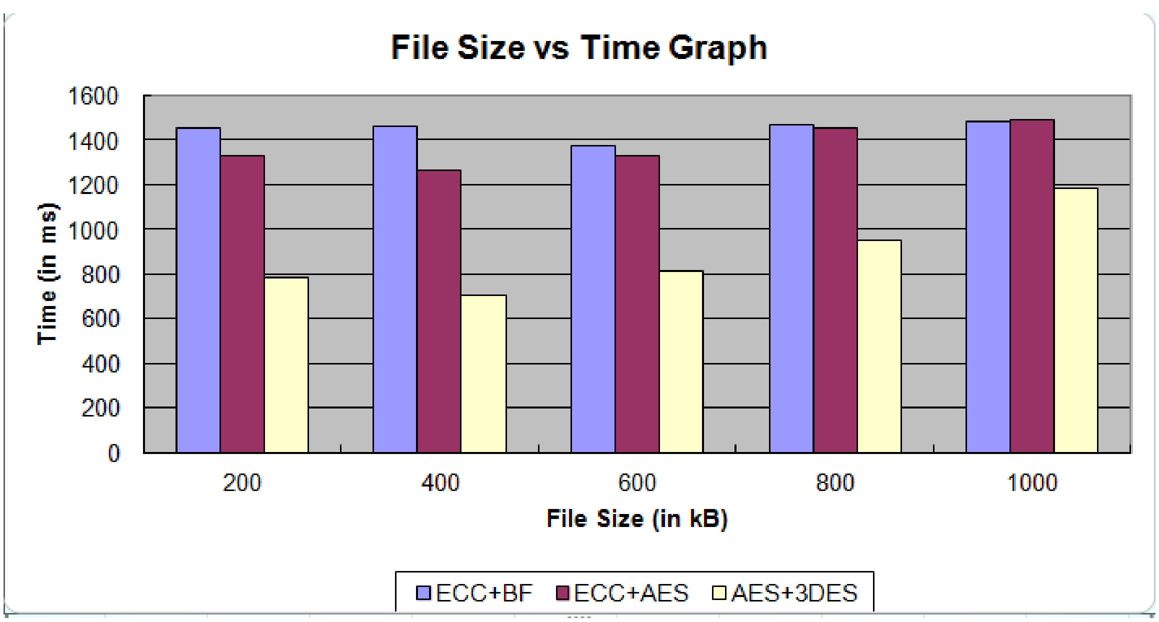
4.1 Comparison table between different type of algorithm

Algorithm	Key size	Block size	Structure	No. of rounds
AES	128/192/256	128	SPN	10/12/14
HEIGHT	128	64	GFS	32
PRESENT	80/128	64	SPN	31
RC5	0-2040	64	Feistel	1-255
TEA	128	64	Feistel	64
XTEA	128	64	Feistel	64
LEA	128,192,256	128	Feistel	24/28/32
DES	54	64	Feistel	16
Seed	128	128	Feistel	16
Twine	80/128	64	Feistel	32
DESL	54	64	Feistel	16
3DES	56/112/168	64	Feistel	48
Hummingbird	256	16	SPN	4
Hummingbird2	256	16	SPN	4
Iceberg	128	64	SPN	16
Pride	128	64	SPN	20

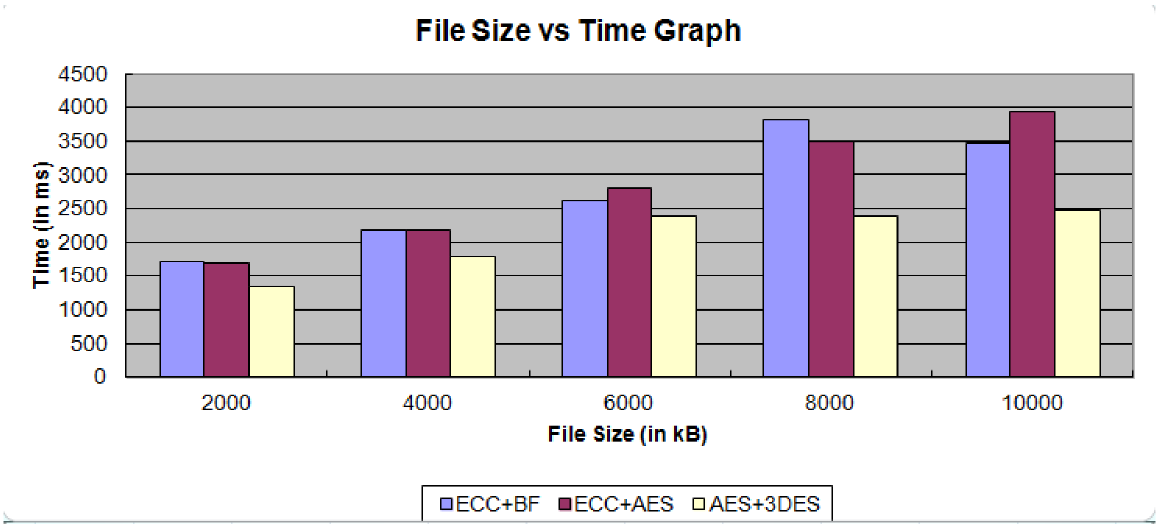
4.1 MULTI LEVEL ALGORITHM TESTING

This testing seeks to run an algorithm combination on files of different sizes in order to record the performance of the combination in relation to increasing file size. On the basis of the feasibility of the algorithms, it was concluded that we could have the combinations of the algorithms AES-3DES, ECC-BLOWFISH, ECC-AES. The files used in the testing were text files of sizes varying from 200 Kilo bytes to 50,000 Kilo bytes. Graphs plotted for various algorithms have been depicted.

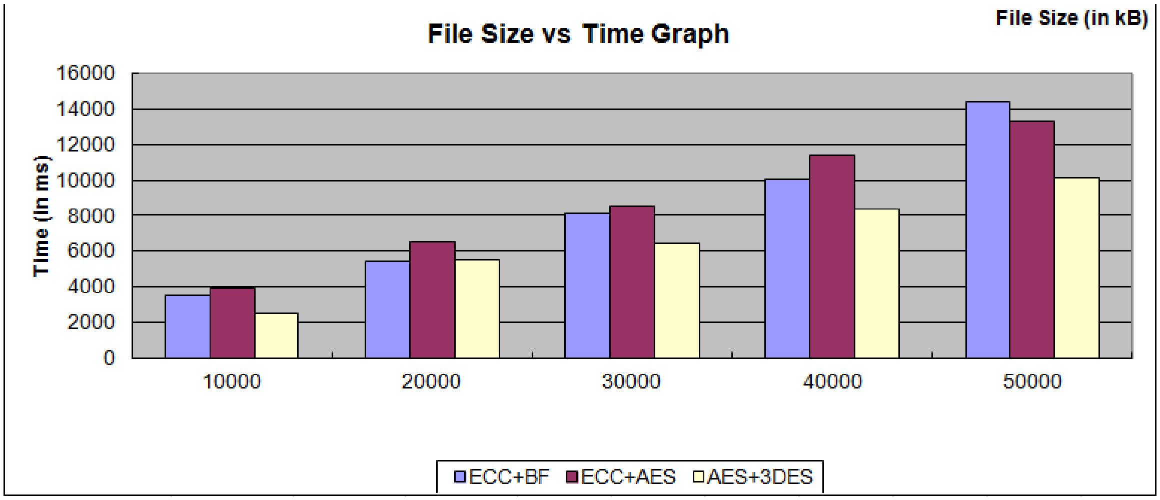
File Size in KB	ECC+BF	ECC+AES	AES+3DES
200	1453	1328	782
400	1464	1265	704
600	1375	1328	812
800	1469	1453	953
1000	1484	1490	1187



File Size in KB	ECC+BF	ECC+AES	AES+3DES
2000	1718	1703	1343
4000	2170	2187	1782
6000	2625	2799	2375
8000	3813	3489	2390
10000	3474	3937	2482



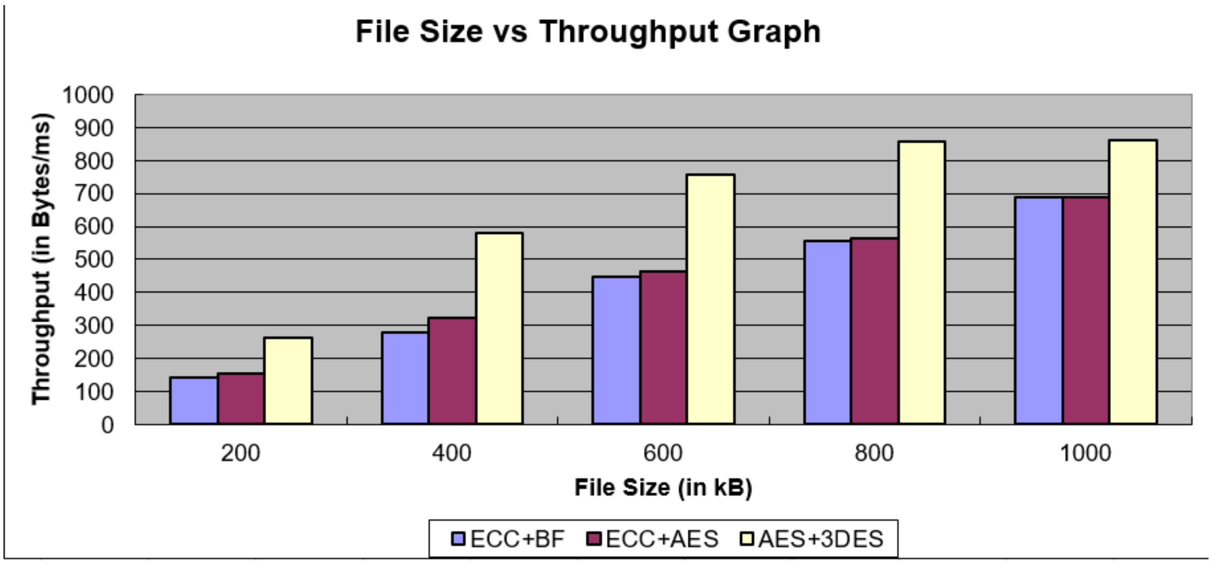
File Size in KB	ECC+BF	ECC+AES	AES+3DES
10000	3474	3937	2482
20000	5450	6524	5541
30000	8086	8570	6400
40000	10066	11400	8394
50000	14423	13293	10121



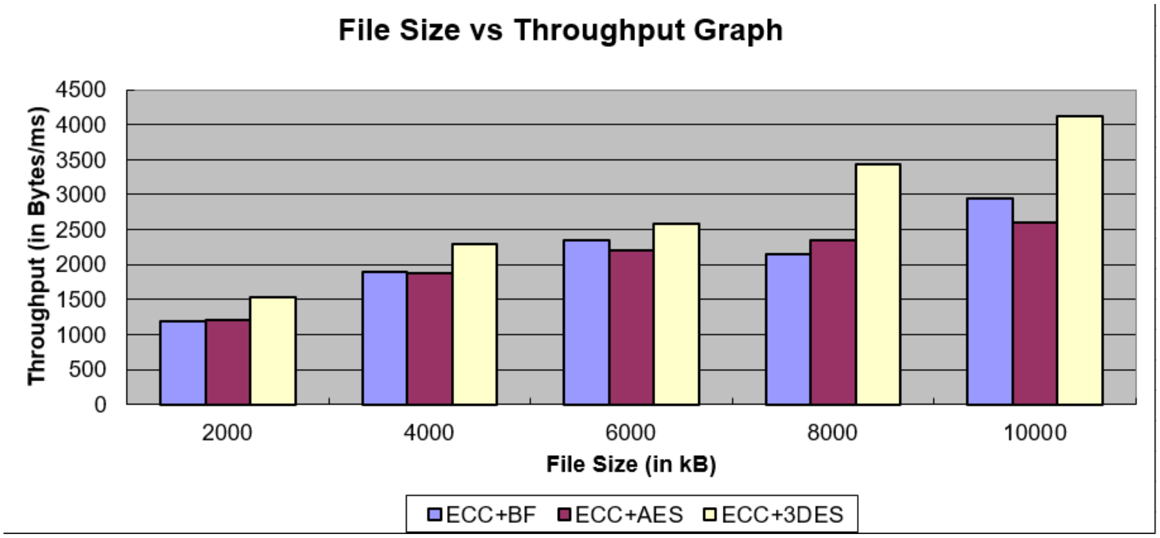
4.2 THROUGHPUT TESTING

This testing seeks to find throughput of the combinations of algorithm. Throughput here is in Bytes per millisecond.

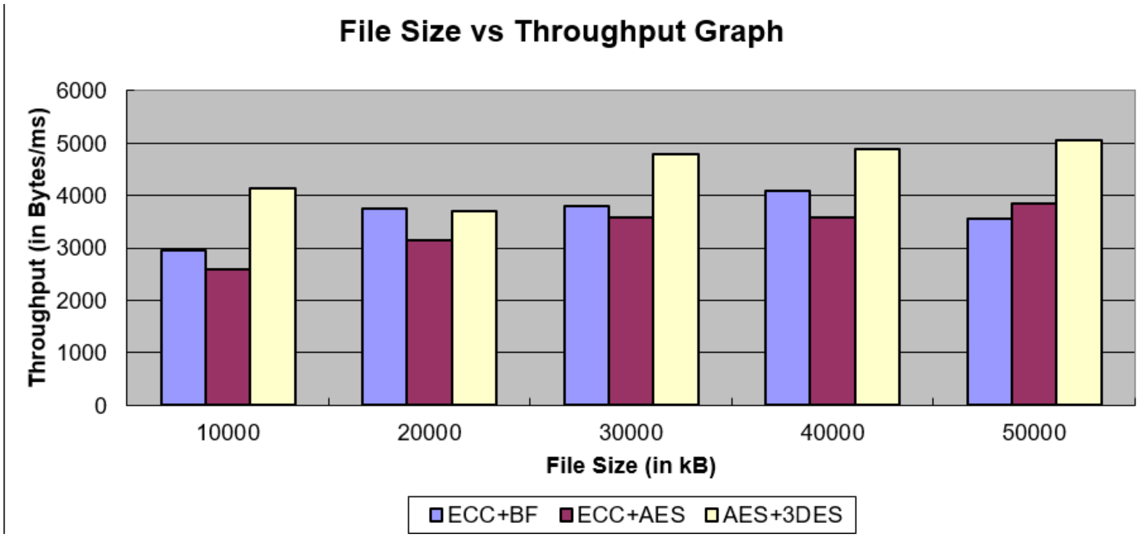
File Size in KB	ECC+BF	ECC+AES	AES+3DES
200	140.9497	154.2168	261.8925
400	279.7814	323.7944	581.8181
600	446.8363	462.6506	756.6502
800	557.6582	563.799	859.6012
1000	690.0269	687.2483	862.679



File Size in KB	ECC+BF	ECC+AES	AES+3DES
2000	1192.0838	1202.5836	1524.9441
4000	1887.5576	1872.8852	2298.5409
6000	2340.5714	2195.0696	2586.9473
8000	2148.4395	2347.9507	3427.615
10000	2947.6108	2600.9652	4125.705



File Size in KB	ECC+BF	ECC+AES	AES+3DES
10000	2947.6108	2600.9652	4125.705
20000	3757.7981	3139.1784	3696.0837
30000	3799.15904	3584.5974	4800
40000	4096.1436	3592.9824	4879.6759
50000	3549.8855	3851.6512	5058.7886


File Size vs Throughput Graph
Throughput (in Bytes/ms)
6000
5000
4000
3000
2000
1000
0
10000
20000
30000
40000
50000
File Size (in kB)
ECC+BF
ECC+AES
AES+3DES

Conclusion

A Light weight algorithm is suggested for IoT devices. The Proposed method suitable for IoT based healthcare scenario.

Implementation of the proposed low-level security model for small scale healthcare organizations will achieve computational efficiency, memory efficiency, energy efficiency, encryption.

By the analysis, we were able to conclude that the hybrid algorithm of ECC+BLOWFISH provided better execution time in comparison to that of ECC+AES. We observed that for relatively small file sizes AES-3DES provided better running time and throughput in Kilo bytes per millisecond as compared to that of ECC+AESand ECC+BLOWFISH. Taking into consideration, the large amount of data that business applications tend to store on the database, file sizes can vary to very large numbers, hence the use of ECC+BLOWFISH hybrid algorithm is suggested to implement multilevel security on system data storage.

5.2 Future scope

- **Optimal Utilization of Assets and Operations** – Healthcare institutions need to ensure optimum utilization of resources to maximise patient care to the fullest of their abilities. Internet of Things aids in efficient timely scheduling by leveraging utilization to serve a greater number of patients. Cloud based scheduling applications can ensure that machines, hospital staff and infrastructure is being utilized to its fullest capacity. Microcontrollers that process and wirelessly communicate data can schedule maintenance activities, patient calls and perform inventory management functions. An IoT medical device can provide daily machine utilization statistics that can be employed for well-organized patient scheduling.

- **Maintaining a Warehouse of Patient Related Data** – It is essential for healthcare institutions to maintain and update a database of health-related inferred by or from patients. The Internet of Things enables hospitals to track, monitor and update patient information in a systematic manner. This patient related data could include reported outcomes, medical-device data, and wearables data. Computational methods of analytical support, known as augmented intelligence, are collectively used to analyse information. This type of an enriched database largely assists healthcare professionals in better decision making and providing superior patientcare.

- **Proactive Replenishment of Supplies**– Internet of Things ensures better inventory management in hospitals and healthcare organizations. An IoT-connected medical device can send signals when critical operational components are being depleted. For example, the helium levels in an MRI machine need to be constantly checked to ensure that the equipment operates in a suitable manner. By using IoT-connected devices, field engineers can be sent out to a hospital before an MRI’s helium levels dwindle, preventing a total machine stoppage and patient rescheduling. Hence, this technology creates a system of real-time monitoring, tracking and immediate response.

REFERENCES

[1] J. Höller, V. Tsiatsis, C. Mulligan, S. Karnouskos, S. Avesand, and D. Boyle, *From Machine-to-Machine to the Internet of Things: Introduction to a New Age of Intelligence*. Amsterdam, The Netherlands: Elsevier, 2014.

[2] G. Kortuem, F. Kawsar, D. Fitton, and V. Sundramoorthy, ``Smart objects as building blocks for the Internet of Things," *IEEE Internet Comput.*, vol. 14, no. 1, pp. 44_51, Jan./Feb. 2010.

[3] K. Romer, B. Ostermaier, F. Mattern, M. Fahrmair, and W. Kellerer, ``Real-time search for real-world entities: A survey," *Proc. IEEE*, vol. 98, no. 11, pp. 1887_1902, Nov. 2010.

[4] D. Guinard, V. Trifa, and E. Wilde, ``A resource oriented architecture for the Web of Things," in *Proc. Internet Things (IOT)*, Nov./Dec. 2010, pp. 1_8.

[5] L. Tan and N. Wang, ``Future Internet: The Internet of Things," in *Proc. 3rd Int. Conf. Adv. Comput. Theory Eng. (ICACTE)*, vol. 5. Aug. 2010, pp. V5-376_V5-380.

[6] Z. Pang, ``Technologies and architectures of the Internet-of-Things (IoT) for health and well-being," M.S. thesis, Dept. Electron. Comput. Syst., KTH-Roy. Inst. Technol., Stockholm, Sweden, Jan. 2013

[7] Hood GW, Kappelhoff R, Hall KH (2010) US Patent No. 7,672,737. US Patent and Trademark Office, Washington, DC, pp 1–29

[8] Hosseinzadeh J, Hosseinzadeh M (2016) A comprehensive survey on evaluation of lightweight symmetric ciphers: hardware and software implementation. Adv Comput Sci Int J 5(4):31–41

[9]Yasir Amer Abbas, Razali Jidin, Norziana Jamil,Muhammad Reza Z'aba, Mohd Ezanee Rusli, Baraa Tariq,"Implementation of PRINCE Algorithm in FPGA,"International Conference on Information Technology andMultimedia (ICIMU), Nov-2014

[10] Fernando Melo Nascimento, Fernando Messias dos Santos,Edward David Moreno," A VHDL implementation of theLightweight Cryptographic Algorithm HIGHT, "Sep-2015.

[11] S.Sridevi, sathya Priya, P.Karthigai Kumar,N.M.SivaMangai, V.Rejula, " FPGA implementation ofEfficient AES Encryption, "(ICIIECS'15)

[12] J. Qi, L. Chen, W. Leister, and S. Yang, "Towards Knowledge Driven Decision Support for Personalized Home-Based Self-Management of Chronic Diseases," *2015 IEEE 12th Intl Conf Ubiquitous Intell. Comput. 2015 IEEE 12th Intl Conf Auton. Trust. Comput. 2015 IEEE 15th Intl Conf Scalable Comput. Commun. Its Assoc. Work.*, pp. 1724–1729, 2015.

[13] P. Rashidi, M. Ieee, A. V Vasilakos, and S. M. Ieee, "A Survey on Ambient Intelligence in Healthcare," vol. 101, no. 12, 2013.

[14] D. Naranjo-Hernández, L. M. Roa, J. Reina-Tosina, and M. Á. Estudillo-Valderrama, "SoM: A smart sensor for human activity monitoring and assisted healthy ageing," *IEEE Trans. Biomed. Eng.*, vol. 59, no. 12 PART2, pp. 3177–3184, 2012.

[15] B. Perriot, J. Argod, J. L. Pepin, and N. Noury, "Characterization of Physical Activity in COPD Patients: Validation of a Robust Algorithm for Actigraphic Measurements in Living Situations," *IEEE J. Biomed. Heal. Informatics*, vol. 18, no. 4, pp. 1225–1231, 2014.

[16] B. G. Lee, B. L. Lee, and W. Y. Chung, "Mobile healthcare forautomatic driving sleep-onset detection using wavelet-based EEG and respiration signals," *Sensors (Basel).*, vol. 14, no. 10, pp. 17915–17936, 2014.

APPENDICES

Code of the program

```
public class TEA {

    private static int delta = 0x9E3779B9;

    private static int[] key = { 78945677, 87678687, 234234, 234234 };

    public void encrypt(int[] v, int[] k) {

        int v0 = v[0], v1 = v[1], sum = 0, n = 32;
        int k0 = k[0], k1 = k[1], k2 = k[2], k3 = k[3];
        while (n-- > 0) {
            sum += delta;
            v0 += ((v1 << 4) + k0) ^ (v1 + sum) ^ ((v1 >>> 5) + k1);
            v1 += ((v0 << 4) + k2) ^ (v0 + sum) ^ ((v0 >>> 5) + k3);
        }
        v[0] = v0;
        v[1] = v1;
        System.out.println(v0 + "," + v1);

    }

    public void decrypt(int[] v, int[] k) {
        int v0 = v[0], v1 = v[1], sum = 0xC6EF3720, n = 32;
        int k0 = k[0], k1 = k[1], k2 = k[2], k3 = k[3];
        while (n-- > 0) {
            v1 -= ((v0 << 4) + k2) ^ (v0 + sum) ^ ((v0 >>> 5) + k3);
```



```
 v0 -= ((v1 << 4) + k0) ^ (v1 + sum) ^ ((v1 >>> 5) + k1);
```

```
        sum -= delta;

 }
       v[0] = v0;
       v[1] = v1;

       System.out.println(v0 + "," + v1);
    }

    public static void main(String[] args) throws IOException {

       TEA tea = new TEA();
       int n = 0;
       int cc[] = new int[100];

       Scanner input = new Scanner(System.in);

       for (int i = 0; i < 4; i++) {

System.out.println("Enter 4 number to encrypt: ");


       n = input.nextInt();
          cc[i] = n;

       }

       tea.encrypt(cc, key);
       tea.decrypt(cc, key);
}

    }
```