UNIVERSITY OF BAHRAIN

College of Information Technology



Secure Framework For IoT Data Traffic Minimization Using Zero Knowledge Proof And RC6 Encryption

A Thesis Submitted in Partial Fulfilment of the Requirements for the Masters of Science Degree in Cyber Security

Submitted By

Afia Murad Ashraf

202000120

Supervised By

Dr. Wael Mohamed Elmedany

(Associate Professor)

University of Bahrain

July 2022

University of Bahrain
Deanship of Graduate Studies
And scientific Research



جامعة البحرين
عمادة الدراسات العليا والبحث العلمي

Dissertation Deposit Form

Author Name:	Afia Murad Ashraf		
Email:	202000120@stu.uob.edu.bh	Contact No:	35387762
College:	**Information Technology**		
Department:	**Information Systems**		
Thesis Title:	Secure Framework For IoT Data Traffic Minimization Using Zero Knowledge Proof And RC6 Encryption		
Year:	2022		

Author's Declaration: I agree to the following conditions:

The above thesis will be available (in the University of Bahrain library and externally) and reproduced as necessary at the discretion of the University of Bahrain. It may also be digitized by the University of Bahrain and made available via the university's repository or via other parties on the Internet.

This condition shall apply to ALL copies including electronic copies.

The above thesis has been provided on the understanding that it is copyright protected material and that no quotation from this thesis may be published without proper acknowledgement.

Signature of the Author:	Afia Murad Ashraf	Date:	25-Mar-22

10 Approved at the University Council 6th meeting, 2013
In accordance with Decision No. 736/2013 dated 14/3/2013
Modified by University Council Decision No. 2043/2013 dated 20/11/2013.

DECLARATION

I declare that this work is the result of my own investigation and that it has not already been accepted in substance for any degree, nor is it currently submitted for any degree.

Signed: ---------- Date: 05/16/2022

Afia Murad Ashraf (Candidate)

The Thesis defense committee considers the thesis titled:

Secure Framework For IoT Data Traffic Minimization Using Zero Knowledge Proof And RC6 Encryption

Submitted by Afia Murad Ashraf to the College of Information Technology is satisfactory and acceptable for the Master of Science in Cyber Security.

The Defense Committee:

(Dr. Wael Mohamed Elmedany) Department of Computer Science University of Bahrain

SZeadally

(Sherali Zeadally) University of Kentucky
(External Examiner) Lexington

RKH

(Dr. RIYADH KAMAL MOHAMMED) Department of Computer Science
(Internal Examiner) University of Bahrain

ABSTRACT

Currently, the major challenge in IoT devices is to reduce the size of data, provide data authentication and encrypt the data. By keeping this view in mind, the current research idea is focused on minimizing data generation by using event based methodology. As As the event based methodology is a technique used for data generation and minimization so the data is minimized at first stage using motion detection sensor. For the purpose of authentication, the most famous technique of Zero Knowledge Proof will be used. IoT devices have a lot of security issues like unreliable accessibility,unauthorized access, encryption failure. To overcome IoT security issues, data encryption is addressed; based on RC6 (Rivest cipher 6) encryption technique. This research study proposed case study related to university based on real life data. This will be done by using events introduction method, in which devices are only activated to record data when an event has occurred. To cope with the security issues, Zero Knowledge Proof is a methodology in which one user can prove to another that the data is valid without providing any extra information about the data. With the help of RC6 algorithm using MATLAB, the unauthorized users will not be able to decrypt the data. Moreover, the proposed research idea is examined in the simulated environment for evaluation. The proposed method is compared with other methods in literature based on throughput, key generation time, average encryption and decryption time which showed that the proposed method is superior over the other methods.

DEDICATION

To my supervisor Dr. Wael Mohamed Elmedany for his kind patience, and for helping me with everything possible to develop this research work.

To my supportive family for their encouragement, and standing by my side in every aspect of my success.

And finally,

To my friends and colleagues for boosting my confidence, and their support throughout this journey.

ACKNOWLEDGEMENT

I would like to express my special thanks and appreciation to my supervisor Dr. Wael Mohamed Elmedany for his kind patience, and for helping me with everything possible to develop this research work. I would like to thank Dr. Wael Mohamed Elmedany for his kind support, and great assistance in developing this research work.

Contents

APPROVAL . . . . . A
DECLARATION . . . . . B
ABSTRACT C
DEDICATION . . . . . D
ACKNOWLEDGEMENT . . . . . E
TABLE OF CONTENTS . . . . . F
LIST OF TABLES I
LIST OF FIGURES . . . . . J
LIST OF ABBREVIATIONS L

1 Introduction **1**

1.1 Overview 1
1.2 Background 4
1.2.1 The IoT Fields Of Deployment 6
1.2.2 Perception Layer / Physical Layer 11
1.2.3 Application Layer 11
1.2.4 Network Layer 11
1.3 Problem Definition 15
1.4 Research Objectives 16
1.5 Research Significance 17
1.6 Research Limitations 17
1.7 Road Map 17

1.8 Summary 17

2 Literature Review **19**

2.1 Overview 19

2.2 Related Work 20

2.2.1 Data Minimization 20

2.2.2 Security At Physical Layer 30

2.2.3 Zero Knowledge Proof 42

2.2.4 RC6 Encryption Technique 45

2.3 Discussion 46

2.4 Summary 50

3 Methodology **53**

3.1 Overview 53

3.2 Proposed Strategy of Data Minimization 54

3.2.1 Case Study 54

3.2.2 Error Bound Lossy Compression Technique 57

3.2.3 Algorithm 58

3.3 Proposed Strategy of Physical Layer Security Using Zero Knowledge Proof 59

3.3.1 Overview 59

3.3.2 Proposed Zero Knowledge Proof Framework 61

3.3.3 Proposed Security Model for encryption at Physical Layer 62

3.4 Summary 64

4 Results and Discussion **67**

4.1 Overview 67

4.2 RC6 Simulation Results Based on Video Encryption and Decryption 68

4.3 Experimental Setup 70
4.4 Limitations of Proposed Model 73
4.5 Discussion 74
4.6 Comparison of RC6 with other Algorithms 75
4.7 Summary 80

5 Conclusion and Recommendations **81**
5.1 Overview 81
5.2 Conclusion 81
5.3 Recommendations and Future Work 83

References **84**
Abstract (in Arabic) . . . . . .

List of Tables

1.1 Attack classification and mitigation on IoT layers 13
1.2 Timeline For The Research Study 18

2.1 Analysis of proposed Ideas Related to Literature Review . . 52

4.1 Parameters For Video Recording in RC6 Algorithm 70

List of Figures

1.1 Major component of IoT structure and its applications. . . . 2
1.2 World population and connected devices. 3
1.3 Average number of connected devices per person. 4
1.4 Constituent elements of IoT 7

2.1 Interaction between IoT entities 23
2.2 Pub/Sub communication scheme 26
2.3 The Event-based Access Control Framework 27

3.1 Secure Structural Flow of Proposed Methodology 53
3.2 Main Picture of University with placement of sensors at different places 55
3.3 Placement of Sensors at different locations in university campus 56
3.4 Flowchart for the proposed data minimization technique . . 57
3.5 Algorithm for Proposed Compression Technique 59
3.6 Proposed Zero Knowledge Proof Data Exchange Framework . .61
3.7 Proposed Model for Encryption/ Decryption at Physical Layer Using Rc6 64

4.1 Video Encryption Method Using RC6 69
4.2 Video Decryption Method Using RC6 70
4.3 RC6 Encryption Algorithm 71

4.4 RC6 Decryption Algorithm 72
4.5 Proposed Video Encryption Process 72
4.6 Proposed Video Decryption Process 73
4.7 Key Generation time of different algorithms 76
4.8 Encryption Time versus Different Algorithms of Encryption 77
4.9 Decryption Time versus Different Algorithms of Dcryption . 78
4.10 Plot between Throughput and Different Algorithms of Encryption 78
4.11 Plot between Throughput and Different Algorithms of Decryption 79

LIST OF ABBREVIATIONS

IoT	Internet of Things
ZKP	Zero Knowledge Proof
RC6	Rivest Cipher 6
MATLAB	Matrix Laboratory
M2M	Machine to machine
RAMI	Reliability, Availability, Maintainability and Inspectability
PLS	Physical Layer Security
CIA	Confidentiality, Integrity, and Availability
DLTC	Direct Lightweight Temporal Compression
PoW	Proof of Work
PoS	Proof of Stake
PoET	Proof of Elapsed Time
DPN	Delegated Proof of Node
Pub/Sub Communication	Pub/Sub communication
EbAC	Event-based Access Control
ACL	Access Control List
CS	Compressive Sensing
MIMO	Multiple Input Multiple Output

D2D	Device to Device
ESR	Effective Secrecy Rate
SNR	Signal to Noise Ratio
SAN	Self Injection Artificial Noise
ESR	Effective Secrecy Rate
CBMD	Channel Based Mapped Diversification
CSI	Channel Status Information
OFDM	Orthogonal Frequency Division Multiplexing
BZKP	Blockchain-based Zero-Knowledge Proof
DES	Data Encryption Standard
AES	Advancesd Encryption Standard
DES	Data Encryption Standard
EDBC	Error Detection Based Channel
HPC	High Performance Computing

Chapter 1
Introduction

1.1 Overview

1.2 Background

1.3 Problem Definition

1.4 Research Objective

1.5 Research Significance

1.6 Research Limitation

1.7 Road Map

1.8 Summary

Chapter 1

Introduction

1.1 Overview

The world recently entered the digital age at the commencement of the late twentieth century, and the manner people interact and function dramatically transformed. Because of the continuous expansion of communication and even the World Wide Web, further Internet usage, known as the Internet of Things (IoT), has emerged. The idea of linking any device directly to the internet including other linked devices is known as the Internet of Things (IoT). The Internet of Things (IoT) is a network of interconnected devices and users that gather and analyze information about they are utilized and the world surrounding those specific devices. In addition, smart objects with built-in detectors are associated with an Internet of Things structural platform, which aggregates information from numerous devices and it uses analytics to deliver the most useful data with services that are tailored to certain purposes. IoT is a pervasive platform for which components communicate with really no human assistance. It is based on the method of controlling the external conditions by evaluating and analyzing information supplied by sensing systems (S. Li, Da Xu, & Zhao, 2015). Sensors are vital in the IoT natural environment because data is received or gathered by those same sensors and would then communicated towards the central authority

to subsequent processing (Porkodi & Bhuvaneswari, 2014). The microcontroller processor has been utilized in a plethora of applications throughout the last couple of decades. IoT adds a new module to such devices in the form of Internet connectivity. Smart products such as, smart phones, smart doors, smart televisions, and smart heaters communicate with one another over the Internet to convey information, thereby empowering humans with comfort. Figure 1.1 demonstrates the possibilities and development of the IoT paradigm (Vimal Jerald, Rabara, & Bai, 2015).

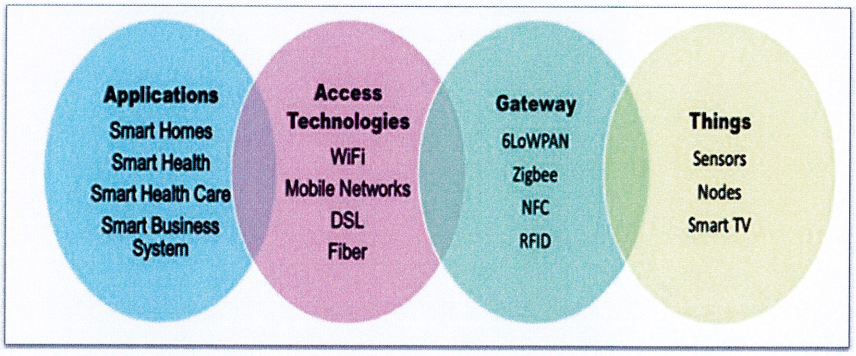


Figure 1.1: Major component of IoT structure and its applications.

According to a Cisco analysis, there were 13 billion world wide web gadgets in 2010. This then touched 25 billion on 2015; It will reach 50 billion in 2020, 75 billion in 2025, and 500 billion in 2030 (Evans, 2011), It will reach 1 trillion by the end of 2035. Another assessment conducted by the International Data Corporation predicts that by 2020, approximately 200 million gadgets would have an internet connectivity. According to the United Nations Development Programme, the worldwide population would approach 8.1 billion around 2025, and 8.6 billion in 2030, pertaining to the United Nations Department of Economic and Social Affairs. It is expected to reach 9 billion through the end of 2035. Figure 1.2 and Figure 1.3 is in form of graph, depicts the world population, active Internet-connected devices, and the average number of gadgets owned by a single person.

The notion of the Internet of Things (IoTs) uncovers the premise of

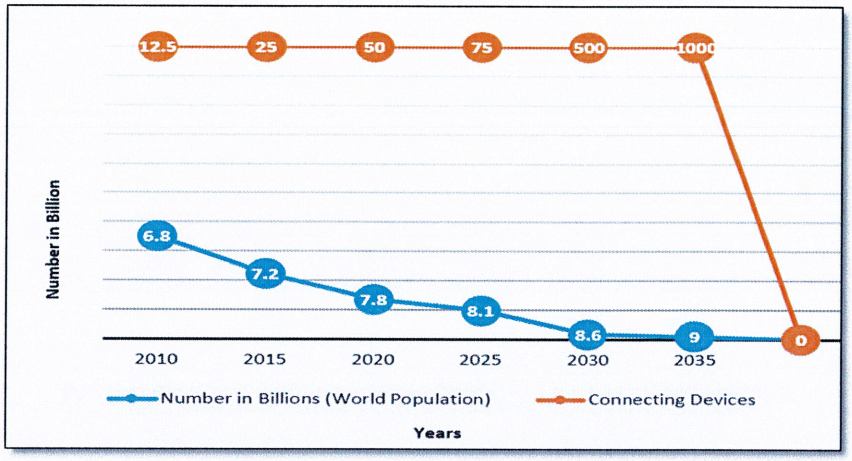


Figure 1.2: World population and connected devices.

connecting all digital and electronic objects into the world of information, which seems advocated for improvement of modern lives and investigating novel applications transcending traditional beliefs. The purpose behind IoT is for numerous electronics to work together effectively and consistently to replace each thing having accurate verification and scheduling. As the IoT phenomenon spreads the globe, people's lives are transitioning each hour. IoT has been employed in a variety of industries, including smart cities (Sanchez et al., 2014),(Zanella, Bui, Castellani, Vangelista, & Zorzi, 2014), since its inception in 2008 and 2009, it has expanded into industrial production, security, agricultural (X.-Y. Yu & Guo, 2020), and even ecology (Šulyová & Koman, 2020). In this regard, health care is one of the most suitable application fields due to its ability to offer ascent to several healthcare applications such as distant healthcare applications, degenerative conditions, or aged care, among others (Bellandi et al., 2021; Pang, 2013; Kwon, Hodkiewicz, Fan, Shibutani, & Pecht, 2016; Oddershede, Macuada, Quezada, & Montt, 2020; Rodrigues et al., 2018; Yoo, Han, & Chung, 2020). IoT likewise stimulates numerous new enterprise approaches. (Maiorescu et al., 2020) highlights why IoT systems arrange user behavior in order to generate effective social media marketing approaches.

The most challenging difficulties in an IoT context are security threats such as authentication, confidentiality, authentication protocols, system setup, evaluation, supervision, and data transmission (Jing, Vasilakos, & Wan, 2014). Smartphones and integrated devices, for example, may serve to accommodate a technological worldwide networking ecosystem that can aid to simplify lives through being responsive, reactive, and sympathetic to individual demands Nevertheless, because users' privacy may be infringed and even their own personal information divulged whenever a peripheral sensor is triggered or stopped (Sadeeq, Zeebaree, Qashi, Ahmed, & Jacksi, 2018), prevention cannot be guaranteed. The establishment and progression of the Internet of Things are heavily reliant on overcoming these challenges and opportunities (Sicari, Rizzardi, Grieco, & Coen-PorisiniSecurity, 2014).

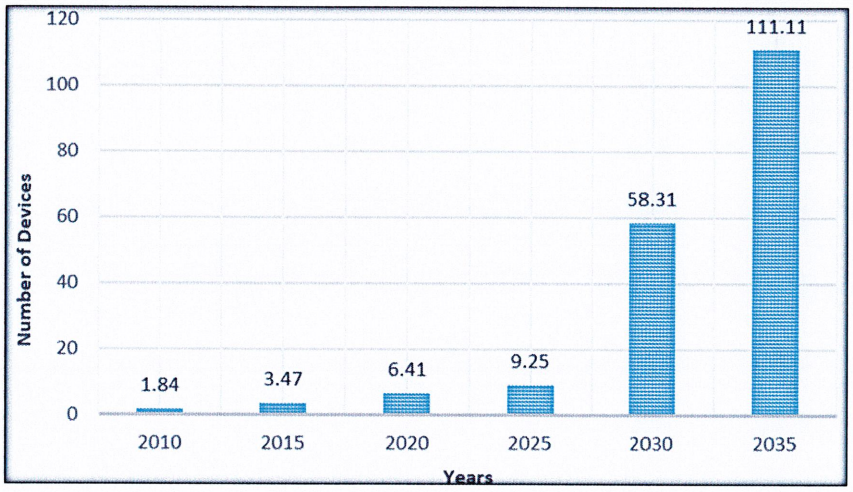


Figure 1.3: Average number of connected devices per person.

1.2 Background

The inclusion of IoT into everyday activities can be seen in a range of circumstances. Ever since inception from "Kevin Ashton" in 1999, IoT has entered into the general public's daily routines, but we've had a wide range

of implementations in a variety of fields such as, medicine, industry, agriculture, energy, defense and in the making of smart devices, homes and even cities. By using artificial intelligence and the World Wide Web, the universe is becoming stronger while also minimizing physical labor and becoming highly sentient(Balaji, Nathani, & Santhakumar, 2019).

The complicated aspect of IoT revolves around the fact that, because it is difficult to integrate many technologies into one, the system will attempt to securely link the devices, which will have constrained storage, compute performance, and power.(Ahanger, 2018). A few of the equipment in this group are only capable of sustaining a fundamental system of security protocols, and a few of these provisions are incapable of safeguarding the security and secrecy of the user's data (Madakam & Date, 2016). This implies that threat actors could always exploit a flaw in one of the gadgets and gain access. This article emphasizes the integration of IoT in numerous domains in our lives, as well as the intimidations it poses in those disciplines. The term "Internet of Things" was developed from the abbreviations "Internet" and "things," both of which are abbreviated to the popular IoT. The Internet is a collection of linked system that connects billions of people across the world using the standard Internet protocol suite (TCP/IP). The architectural flow of IoT can be well observed from the figure 1.4. The figure depicts that a person or entity can interact with other sensors to create a network, can communicate with the help of standards, to aggregate and analyze the augmented intelligence to observe the behaviour to act. a It is essentially a network made up of other networks, which are typically made up of millions of regional to international ,private, communal, industrial, educational, and government networks that are linked together using a wide range of fiber, electrical, and wireless connectivity techniques (Evangelos A, Nikolaos D, & Anthony C, 2011).

In the actual life, "Things" can be any item or person that can be dis-

tinguished. Frequent products encompass "things" that we don't generally think of as electronics in anyway, such as mobile devices and complex technical products that can be used by us on a continuous basis; For instance, meals, garments, furnishings, parts and hardware, commodities, goods, and particular objects, memorials and pieces of art, milestones, and all types of interchange, cultural, and refining (Sundaravadivel, Kougianos, Mohanty, & Ganapathiraju, 2017). That means that objects can be both alive and non-living, such as a freezer, chair, curtain, tube lamp, tray, and all other equipment or gadgets for the business. As a result, items in the material realm are now considered to as actual real-life objects (Valanarasu, 2019)

1.2.1 The IoT Fields Of Deployment

By 2020, it is expected that over 50 billion gadgets will be connected to the internet (Quora, 2013), This sector is anticipated to have a considerable number of applicability both in the present and upcoming future. IoT is blossoming in multiple areas, from monitoring a baby in an incubator to assisting a senior citizen. With such significant growth predicted, this section will provide a quick overview of IoT applications in a variety of household and industrial settings.

a. Smart environment

Considering we live in an automated culture, a smart habitat would encapsulate this pattern by integrating computers, cellphones, and the internet into our daily lives. Smart city, on the other hand, refers to automation of a complete city and administering everything through the use of the internet in the perspective of IoT. Various applications, ranging from signalized intersections management to environmental monitoring, are in the works. Sensors will assume a critical role in IoT rollout in a smart city. A smart city should incorporate certain essential automation systems that act as the economy's core. Tracking parking facilities arrangements, monitoring tec-

tonic waves in structures, monitoring pollutants and radioactivity in a city, handling traffic, crisis restoration, garbage management, logistics, and many more are just a few illustrations.

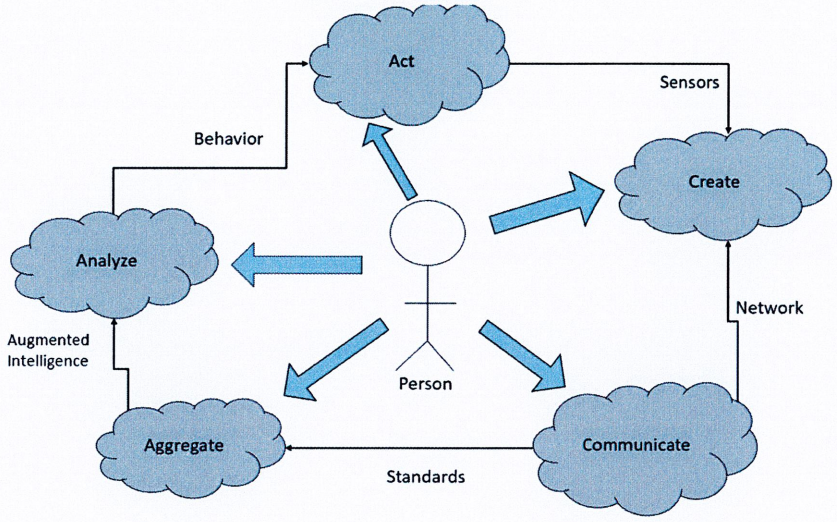


Figure 1.4: Constituent elements of IoT

- Domestic applications: At the domestic level, the home automation business is the best illustration of IoT applications. Sensors connected to a user's water reservoir allows them to control how much water is used from it. Turning on the air conditioner before arriving home to keep the room cool, and remotely controlling all electronic and electrical gadgets at home using a smart phone. Users may be able to enhance their living environment by documenting parameters such as ambient temperature, dust level, acoustics, and even oxygen level. A fascinating feature of home automation is the ability to track one's carbon output by keeping an eye on power usage, water, biological disposal, and food waste.

- Industrial applications: Supply Chain Control keeps track of storage conditions and inventory control for accountability reasons along the

distribution chain. A smart product management solution could control the cycling of products on shelves and in warehouses. The Internet of Things can be used to analyze ozone levels in food factories throughout the drying process. Targeted irrigation in dry regions to limit the volume of water consumed would boost agricultural performance. The capability of tracking patient health status in hospitals and nursing homes is a valuable tool in the health-care industry.

- Security and Emergencies : Observation via Surveillance cameras is accessible 24 hours a day, seven days a week, which is a unique feature in terms of securing facilities. These cameras might be viewable via the internet just about anywhere in the globe. A recent addition to its stream is perimeter access control to limited areas and identification of people in non-authorized regions. To avoid faults and deterioration, liquid detection is used in data centers, warehouses, and critical building areas, Levels of radiation in the vicinity of nuclear power stations are being detected in a widespread way in order to trigger leakage alerts, assessment of concentration in the atmosphere and spills in industrial environments, chemical plants surroundings, and mines, are among other things.

- Logistics and Transport : A novel unconventional application is the surveillance of shocks, strokes, container openings, and cold chain management for insurance reasons. Single component searching in huge surface areas like warehouses or harbors, diagnosis of storage problems, fleet mapping, and so on are just a handful of good Logistics system application. IoT has a lot of uses in the transportation business. The transportation business has been transformed to a new level thanks to GPS, V2V, and V2I communication. Machine to machine (M2M) technology is gaining momentum. If vehicles interact with

one another, the risks of accidents and accidents are greatly reduced, and there could be a surge in the development of smart transportation infrastructure in the future. IoT allows for tracking public transportation, knowing traffic and pedestrian concentrations, recognizing road deterioration, avoiding crashes, and improving travel routes, among many other functions.

b. Security in Automation Systems: In the area of IoT, it offered a categorization for security and safety terminology. This illustrates vulnerabilities originating from IoT automation's Machine to Machine (M2M) connectivity features. M2M works without the need for human intervention. (Kabulov, Normatov, Boltaev, & Saymanov, 2020). In sensor nodes, constrained gadgets with no power and unique processing, as well as limited security capabilities, are utilized to address automation challenges. In terms of applications, the IoT world is huge. (Kabulov, Urunbaev, Normatov, & Ashurov, 2020) IoT system requirements can vary based on application field. The following should be considered for systems to operate within the IoT automation system and the IoT domain (Kabulov, Urunbayev, & Ashurov, 2019):

- Compatibility across equipment and software
- Multidimensional
- Real-time functioning
- Security
- Technical simplification

In the industrial sector, automation is also advancing. Industrial systems are subject to different, more stringent safety regulations than IT systems. The CIA's well-known aims of confidentiality, integrity, and availability can be used to describe these needs. The topic of 4.0 and IoT automation systems has sparked a huge amount of attention in this field. (Kabulov & Nor-

matov, 2019). Industry 4.0 is the result of the convergence of numerous technologies. It, like the Internet of Things, is renowned for its heterogeneity. As a result, the requirement to figure out how these current technologies would look is integrated, for example, a reference architecture is necessary. There have been a number of initiatives thus far. The Industrial Internet Consortium (IIC) is working on the Industrial Internet Recording Architecture (IIRA), which is based on four tiers of "point of view" in industrial Internet systems (IIS).

Whereas RAMI 4.0 concentrates on automation technology, IIRA wants to introduce IoT to a broader range of industries, including power, medical, and transport. Both of these architectural elements have a lot in common. In CPSS, safety is extremely crucial, especially when it comes to the upgrading of industrial systems that are regulated by linked ICT aspects. Despite the fact that existing reference design patterns do not adequately address security, the link should incorporate security considerations. RAMI 4.0,looked into the potential of establishing a security perspective. We must evaluate the threats that exist in an automated situation while integrating protection through a hierarchical axis (Kabulov, Normatov, & Ashurov, 2019).

IoT devices have a unique layer-based architecture. IoT devices. TCP/IP, are having three separate operative layers (Iqbal, Suryani, Saleem, & Suryani, 2016) (Z. Yan, Zhang, & Vasilakos, 2014) (Zhao & Ge, 2013): the perception layer, network layer, and application layer. Because every layer performs a separate job, each layer faces its own set of risks. Furthermore, every layer is linked to and reliant on the functions of the others. As a result, if any of those layers is secure, the others must likewise be secure. The brief overview of these layers is described as:

1.2.2 Perception Layer / Physical Layer

The responsibility of this layer is data collection in IoT devices. Each IoT device has a purpose that involves the collection of data. As a result, this specific layer employs Zigbee, RFID and other varieties of sensors (Bansal, Nanda, & Husain, 2021). The perception layer must be protected since it receives huge volumes of data that could be malicious or harmful. Because IoT devices are typically self-contained, attackers can simply exploit them. In the perception layer, considerable security could be implemented. Anomalous sensor reading and Cryptographic elements detection are two examples (Yang, Wu, Yin, Li, & Zhao, 2017).

1.2.3 Application Layer

The application layer is the most diverse and sophisticated IoT architecture layer. Because there are numerous diverse manufacturers and devices, there is no common system for application layer development. At the application layer, there are a range of challenges. Data access rights and verification, are the major ones among all. Data confidentiality and data recovery are also impacted by the application layer. The huge transfers of information and data, paired with the number of devices and ports, make it difficult to safeguard that data effectively. Ultimately, like with other types of applications, it is still the threat of application layer problems (Zhao & Ge, 2013). Furthermore, security risks might arise when developers do not employ standardized code in their services (Swamy, Jadhav, & Kulkarni, 2017).

1.2.4 Network Layer

In IoT, the network layer integrates everything and permits people to be informed of existing environment.A powerful network is required for information exchange and the provision of services from a device. The underlying

concerns should be considered at the networking layer:

- Access control techniques include the management of permanent, wireless, and wireless connections.
- Security requirements for Quality of Service (QOS)
- Techniques for data mining
- Among these challenges are safety and confidentiality.
  Information transparency and human privacy are vital since IoT connects countless personal items, constituting a privacy risk. Existing network security solutions can offer a foundation for privacy and security in IoT, but further work is required (Gokhale, Bhat, & Bhat, 2018)

Because sensors and actuators are the physical building blocks of automation IoT systems, the bottom layer is referred to as "sensors and actuators". The layer above it is referred to as "networking," and it addresses all connection concerns between layers 2 and 6 of the ISO OSI model, encompassing diverse network typologies, aggregations, and methods of transmission. The "Data Processing" layer encompasses all methodologies, tools, and equipment that aid in the extraction of useful information from acquired data. The "Application" layer contains the system's fundamental management mechanisms, which are built on the complete IoT architecture - the strongest of logic, as well as the system's setup,and the(Madrahimova & Yarashov, 2020) presentation of its state.

- Technology, architecture, and tool decision
- Project planning setup, scripting, and authentication
- Rollout and licensing;
- Administration and service

Table 1.1: Attack classification and mitigation on IoT layers

Layer	Threat type	Mitigation
Physical	Tampering	Tamper-resistant packaging
	Denial of Service	Spread-spectrum techniques
Networking	Denial of Service	Active firewalls, Passive monitoring (probing), Traffic admission control, Bi-directional link authentication
	Eavesdropping	Encryption, authorization
Data processing	Back door attack	Properly configured firewalls on all system entry point
	Social engineering	Educating employees to security awareness
	Exhaustion	Traffic monitoring
	Malware	Malware detection
Application	Client app	Anti-virus filtering
	Comm. channel	Proper authentication, authorization, integrity verification
	Integrity	testing
	Modifications	validation
	Multi-user access	Process planning and design
	Data access	Traceability

Table 1.1, gives a brief overview of different layers including physical, networking, data processing and application layer with their threat types and how to mitigate them. This table provides a comprehend detailed analysis of attacks at different layers and how to mitigate those attacks and threats.

Cyber security has always been a concern for the Internet of Things. To address the issue of cyber security, it is necessary to evaluate the many forms of assaults that can be launched against a system, as well as the defensive measures that need be implemented based on those characteristics Substantial outcomes will be gained if the projected IoT system incorporates cyber security into its structure (Kabulov, Yarashov, & Vasiyeva, 2021).

Earlier, the implementation of a spread spectrum technique (e.g direct sequence coding, frequency hopping) to avoid spying was the major goal of physical layer stability. Because if an intruder uncovers that communication is going in place, the overall platform is jeopardized; The physical layer generally hides the communication that is happening at the moment (Pecorella, Brilli, & Mucchi, 2016a). Intrusion discovery and the incapacity of signal cloning have been the only ways to achieve absolute anonymity (Bennett & Brassard, 2020a). Nevertheless, because of the use of feeble signals,

depending on such affects results in incredibly limited signal transmission (Pecorella et al., 2016a). Despite the fact that study into PLS approaches has yielded positive results, developing PLS solutions for IoT applications remains difficult. PLS for IoT applications is still difficult, despite the use of advantageous approaches. In a nutshell, the Internet of Things has four characteristics: minimal cost, broad coverage, massive networks, and a variety of services. The question of how to come up with PLS procedures that are well matched to these four features is yet open (Sun & Du, 2018a). The primary focus of this work is on an orientation to the basic tenets of physical layer security, as well as illustrated PLS security mechanisms, PLS protocol architecture difficulties, and designing IoT-oriented PLS alternatives.

The diverse applications of IoT like smart security, transport system and smart city etc. can ensure convenience to the users, but it cannot guarantee the validity and authentication in terms of confidentiality, integrity, and availability (CIA) (Akyildiz, Su, Sankarasubramaniam, & Cayirci, 2002). An invader captures authority of the IoT devices and the communication channel. It will have a negative impact on the privacy of the overall infrastructure to which devices are linked. There has been a lot of interest in developing security measures related to physical layer's communication properties (Ye T & ZH, 2012). It is primarily concerned with the symmetric cryptographic system and may not assure integrity because of key exchanging among entities. Furthermore, security service providers . In addition, provide an impenetrable security mechanism that prevents listening parties from gaining unwanted input or access (Achary, 2021).

In the past, stability at the physical layer was primarily targeted as the adoption of a spread spectrum approach (direct sequence coding, frequency hopping,etc.) to prevent espionage. The physical layer normally conceals the communication that is currently occurring because if an attacker dis-

covers that communication is taking place, the entire system is threatened (Pecorella, Brilli, & Mucchi, 2016b). Perfect secrecy can only be attained by intrusion detection and the inability of the signal cloning (Bennett & Brassard, 2020b). However, the reliance on such impacts leads to extremely low signal transmission due to the usage of weak signals (Pecorella et al., 2016b).

Although the research of PLS techniques has reached fruitful outcomes, it is still challenging to develop the PLS solutions for IoT applications. Even because of beneficial techniques, PLS for IoT applications is still challenging. In short, IoT has four properties: low-cost, extensive coverage, enormous networks, and a diverse selection of services. The subject of how to devise PLS techniques that are well suited to these four characteristics remains unresolved (Sun & Du, 2018b).

1.3 Problem Definition

1. IoT generates a lot of data and minimization is not done
   The Internet of Things goal has evolved over the last few years from a conceptual framework to a main objective across various businesses. Organizations are seeking for new methods to use and manage and handle the data collected when they deploy IoT equipment into respective networked architectures.
2. How the data will be secured on Physical layer?
   The physical layer is vulnerable to a variety of threats, including malevolent insiders, malfunction or sabotage, degradation, overburden, natural disasters, and so on. Even the most seemingly trivial component, such as a connector, can bring an entire system down if it is compromised or attacked. At the same time, the physical layer might serve as final line of defense. One could be the victim of a

denial of service attack. In this instance, the only way to save the network is to provide measures to keep the physical layer secure.

3. How to make the data secured through an appropriate encryption algorithm?

   We need to keep the data away from unauthorized user so that no one can access the data without having key. To keep the data secure and away from an authorized user, encryption is the necessary tool to be implemented. But the main question is, the way to provide an encryption technique through a way which is more secure, effective and fast among others.

1.4 Research Objectives

1. The aim of this research work is to propose a framework for minimizing data generation of IoT devices (with the help of different sensors at different positions to detect and record video of a certain time when an event occurs, these sensors will capture and record video at different positions when a certain motion is detected and its changed from '0' to '1')
2. The captured data is authenticated by using Zero Knowledge Proof while the encryption is done using RC6 for data security (as RC6 is having low complexity, faster and lightweight encryption algorithm).
3. The proposed framework will be tested to evaluate the overall performance on the basis of integration of data minimization, embedding of data in Zero knowledge proof and encryption using RC6.
4. Finally, the proposed framework will be compared with existing solutions.

1.5 Research Significance

The significance of the research focus on the security of the data in the terms that the encrypted code cannot be exploited by the third person. The security of the data should be accurate and privacy of the data should not be affected.

1.6 Research Limitations

There can be few limitations given below:

1. The generated data might be different at different places, for example: if it is used for hospitals, there can be the chances to generate different types of data
2. The gathered data is also a limitation as well that whether we would be successful in terms of gathering data.

1.7 Road Map

The road map is the utilization of time for completing an individual task and it gives an overall time frame to complete each task in order to perform each task efficiently in the specified time slot. Table 1.2 depicts the time line for this research study.

1.8 Summary

To summarize the steps of the research work, following are the steps written in brief:

1. At investigative stage, Study Qualitative previous methods of data minimization, authentication, and encryption in IoT for finding related technique and solutions.

Table 1.2: Timeline For The Research Study

Task Name	Duration	Start	Finish
Master Thesis	150 Days	February 1, 2022	June 30,2022
Draft Proposal	20 Days	19 January, 2022	9 Feb, 2022
Submit Proposal	1 Day	10 Feb, 2022	10 Feb, 2022
Review Comments and Refine Proposal	11 Days	11 Feb, 2022	21 Feb, 2022
Presentation In Seminar	1 Day	21 Feb, 2022	21 Feb, 2022
Review and Submission of Revised Proposal	2 Days	21 Feb, 2022	23 Feb, 2022
Design Thesis Document (Draft Contents)	3 Days	24 Feb, 2022	26 Feb, 2022
Literature Study	6 Days	27 Feb, 2022	Monday 7 March, 2022
DataSet Collection	6 Days	Tuesday 8 Mar, 2022	Tuesday 15 March, 2022
Data Minimization Using Sensor	5 Days	Monday 16 Mar, 2022	Tuesday 22 March, 2022
Study of Algorithm ZKP Framework regarding Design	5 Days	Wednesday 23 March, 2022	Tuesday 29 March, 2022
Designing of ZKP Framework	4 Days	Wednesday 30 March,2022	Monday 4 April, 2022
Implementation of RC6 Using MATLAB	8 Days	Tuesday 5, April, 2022	Thursday 14 April, 2022
Security Analysis	3 Days Days	Sunday 17 April, 2022	Tuesday 19 April, 2022
Thesis Document Writing	40 Days	Sunday 6 Mar, 2022	Tuesday 19 April 2022
Review Document	6 Days	Wednesday 20 April, 2022	Wednesday 27 April, 2022
Submit For Publication	1 Day	Thursday 28 April, 2022	Thursday 28 April, 2022
Prepare Presentation	3 Days	Tuesday 10 May, 2022	Thursday 12 May, 2022
Present and Demonstrate	.....	According to allocated Date	According to allocated Date

2. The research work aims to reduce data generation by using events, for authentication and encryption of data, zero knowledge proof and RC6 will be integrated.
3. Matlab software was used to conduct the experiment and evaluate the proposed method.
4. Comparison of proposed technique with other techniques with respect to data efficiency of encryption/ decryption in RC6.

Chapter 2
Literature Review

2.1 Overview

2.2 Related Work

2.3 Discussion

2.4 Summary

Chapter 2

Literature Review

2.1 Overview

The following study focuses on three tasks: data minimization, security at the physical layer via Zero Knowledge Proof, and RC6 encryption. The goal of this research is to establish a framework for minimizing data generation in IoT devices using various sensors at various locations to detect and record video of a specific time when an event occurs. These sensors will obtain and record video at various locations when a specific motion is detected and its value is changed from '0' to '1'. The created data is verified using Zero Knowledge Proof, and the data is encrypted using RC6 for security. RC6 is a low-complexity, quick, and lightweight encryption technique. The proposed model will be put to the test to see how well it works. The prior work related to data minimization, prior work in the physical layer with Internet - of - things physical layer IoT solutions and zero knowledge proof is described in chapter 2

2.2 Related Work

2.2.1 Data Minimization

The Internet of Things (IoT) is a network of physical objects that includes embedded sensors, actuators, and network interfaces and has a substantial economic impact (Kshetri, 2017). Huge amounts of data are compiled and analyzed through an ever-growing set of applications that aim to meet the diverse and miscellaneous needs of both rural and urban environments, so that manufacturing and service processes can be restructured and streamlined through informed decisions and controls. Smart cities, smart agriculture, smart manufacturing, parking and water management, traffic management, e-Health, education, and environmental monitoring are just a few examples of IoT applications (Staudemeyer, Pöhls, & Watson, 2017).

IoT devices require right sensor to detect data in the right area. The collected data can vary depending upon the nature and purpose of IoT device. IoT devices strengthen the certain areas with methods, procedures and technologies and mange different factors including energy management, security, and interactive communication strategies. IoT isn't the only technology—rather, it's the only one that matters. The Internet of Things (IoT) is a collection of many technologies that interact in a cycle. The purpose of IoT technology in all of the aforementioned spheres of life is to increase the quality of life while reducing manual input (Geraldo Filho et al., 2019)

The data produced from innumerable IoT devices is an essential data for application in creative services. In the previous year's IoT technologies have shown a good progress, however there are still a lot of practical threats. Furthermore, IoT environment network architecture has few significant issues regarding hierarchy and centralization. IoT network architecture resembles the legacy network architectures as it is the extended form of existing architecture. No doubt, the fundamental purpose of both types of architecture

is transmission of data, the data transmission scheme in the legacy network is not adequate regarding IoT environment. The legacy internet architecture faces various constraints in the form of power consumption, computing power requirements etc, in IoT environment. The problem can be overcome by decentralized and distributed approachability in IoT environment. It argues that in an IoT environment, secure transmission with decentralized and widespread connectivity is essential (Fang et al., 2018).

As IoT is touch important, colonial collection and accrued intensity of transmitted information, can roll the action and efficiency of complexed applications. Thus shrinking method is another approach for direction complex aggregation. DLTC (direct lightweight temporal compression) is considered to be one of the compression methods (Klus et al., 2021). DLTC has been formed for the use in low-latency and pale coefficient monitoring devices. The major purpose of DLTC scheme is to decrease information amount for quick transfer and increase space capacity, with the ability to reform the precise entity as precisely as possible at any random occasion. Another technique worth mentioning here is machine learning which increased significance in numerous study areas, due to its huge number of pattern discovery applications (Reyes-Campos et al., 2021).

Due to the changing circumstances of the environment, individuals tend to improve their behavioral patterns to have a better adjustment to their environment. The observations regarding the actions and their effect in the environment results in automatic recognition of those behavioral patterns. IoT helps in discovering resident's behavior patterns regarding a home or any commercial building. (Krishna, Le Pallec, Mateescu, Noirie, & Salaün, 2019) officially recognized that IoT consists of sensors, actuators or other physical devices and software components which helps to transfer information to achieve service to end users. This highly intellectual platform is obtained by residents' behavior patterns with the help of machine learning

algorithms with the main purpose of developing an energy saving platform that uses machine learning and IoT.

Furthermore, IoT security is another big challenge keeping in view the illegal right of entry, threats and attacks as a complete system. The essential safety parameters are confidentiality, integrity and availability which make the system very difficult to achieve every parameter since IoT devices posses' limited power. Simultaneously, the protection of availability of data to its legitimate user is also verified.

As a result, authorized users can be verified with the use of access control security measures in password or token authentication (Anderson, 2020). Nonetheless, research on access control is primarily concentrated on its hardware rather than software components. The access command resolution is practical, by an assets policy also identified as insurance power, where the rules are constituted and established. In IoT software components, event based access control structure of IoT requires access control management and security requirements for integrity, authenticity and data privacy for management IoT software components. IoT applications that are running on operating systems are activated by actions. The action based approach basically comprises of five modules: sensor module, processing module, actuation module, module of execution and module of communication as shown in Figure 2.1 (Zulkipli & Wills, 2017). The application and efficiency of work, depends upon the interaction between these modules. All interactions are depending upon the occurrence of the event and vice versa. In sensor-based scenario, the processing depends upon the filtration of the incoming data prior processing. In processing module an access control event in the scheduler is important before the event generation. The control of data and processes will be administered by access control event before further processing. This control policy is needed for the purpose of managing the network capabilities, memory space and energy usage in the

IoT.

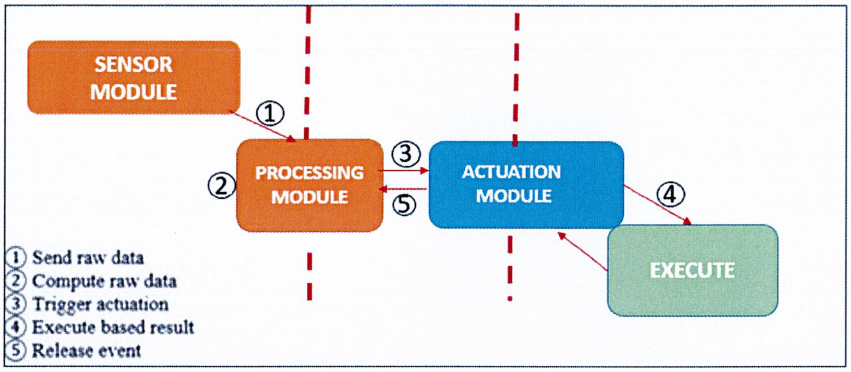


Figure 2.1: Interaction between IoT entities

In order to discuss different compression techniques in IoT, contribution of various researchers cannot be ignored. To exhibit all the compression methods and their results, here is the description of major contributions based on IoT architecture and services.

1. (Consensous Algorithm) The strategy of block chain systems, focuses on all the nodes, which must have same transaction records. The block chain system uses consensus algorithms, which focus on transaction strategy of a block. As discussed above, decentralization is the main concern in attaining efficiency, therefore consensus algorithms also focuses on decentralization control distribution information(Yim, Yoo, Kwak, & Kim, 2018). These consensus algorithms have many limitations regarding performance and power utilization in terms of permission less block chain systems. These limitations were controlled by the following methodologies in the past few years are discussed below:

   (a) PoW (Proof of Work)

   The PoW consensus algorithm is used to find an exact hash value in order to construct an authentication tokens packets, in the

block chain system (K. Yu, Arifuzzaman, Wen, Zhang, & Sato, 2015). In this method, the miners need to ascertain the hash value, Then, as the miner locates a hash function that has been defined, a new chunk is generated every time.

The following function express the hash value of the block determined by the formula (D, 2^{256}-1) where Max being maximum amount of difficulty. Bitcoin system uses random block generation procedure, and it selects the longest chain to handle consistency of block chain. The biggest disadvantage of PoW is that it consumes an excessive amount of energy (Christidis & Devetsikiotis, 2016).

(b) PoS (Proof of Stake)

PoS is a consensus mechanism for presenting participant, owning assets which is recommended as an alternative to PoW in order to prevent excessive energy consumption (Voulgaris et al., 2019). PoS differs from PoW in that under the PoS process, miners produce a new block based on the assets they own. In PoS, the hash function is described as follows:

$$Hash(hash(Block_{prev}), A, TS \leq Bal(A)Max/D \qquad (2.1)$$

In the above expression, $Block_{prev}$ is the earlier chunk, address is donated by A and timestamp by TS. To keep the balance of address A Bal (A) is used while Max is the maximum amount of difficulty similarly in PoW. In this method, coin age and weight are being applied so stakeholders, with more assets have an edge. As this blockchain method is used to evaluate block generation ratio, however, the PoS process has drawbacks, that hinder reality-based and practical consensus. To solve these issues, the Delegated Proof of Stake (DPoS) methodology was proposed. DPoS has the block generation authority and with the help of

election system, a new valid block is generated, and consensus is checked. It results in reducing time and cost as compared to other mechanisms (L. Li et al., 2018).

(c) PoET (Proof of Elapsed Time)

Another consensus algorithm is PoeT being an improved method that uses less energy and provides similar defense as PoW. This security module focused on Intel SGX (Software Guard Extensions) and it works in a way that many nodes are participated to elect one leader based on efficiency and fair approach. The leader is elected by the node on the basis of CPU commands, which offer security and randomness. Its accuracy is based on nodes acting fairly when it comes to waiting for a randomly selected time period. The PoET can offer a decision of effective consensus, but one must use Intel SGX (Software Guard Extensions) (Uriarte & DeNicola, 2018).

2. Pub/Sub communications

There is another technology in comparison with legacy TCP/IP named as ICN (Information Centric Networking) which is comparatively more effective than TCP/IP networking technique based on information cashing process, forwarding technique. This depicts that ICN technology is main infrastructure of coming time, and Publish/ Subscribe is one of the technique in the same direction which will increase the efficiency of future internet (Parizi, Dehghantanha, et al., 2018). The Publisher and subscriber communication technique is an asynchronous communication method and is well described in Figure 2.2. Publishers and subscribers utilize an event bus, which maintains asynchronous event-driven data transmission. It is well suited in IoT environment, as in an IoT environment, the data is recorded by sensing, capturing and recognizing etc. It means data is generated whenever an event will occur.

Few examples of such successful strategy are DDS (Data Distribution Service), MQTT (MQ Telemetry Transport) and so on.

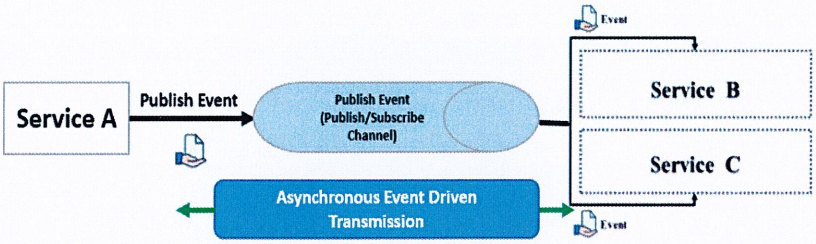


Figure 2.2: Pub/Sub communication scheme

3. A DPN (Delegated Proof of Node) Mechanism
   The scheme involves numerous nodes, having computation power for developing a blockchain; this area is named as mining zone. The mining zone nodes accomplishes authentication request received from IoT nodes. The information received is reviewed and compared to previous blockchain messages. As a result, a new block will be added to the blockchain by the miner node. Revert the response to the IoT node if the required data isn't encrypted (Yao, Jing, et al., 2018). The algorithm of DPoN is:

$$hash(hash(Block_{prev}), A, TS) \leq D_{node} STA(A) Max/D \qquad (2.2)$$

   This scheme consists of two steps; The first is the node procedure, based on blockchain technology, with the Pub/Sub approach as an integrity. The second method is synchronized information transfer, which is facilitated by the Pub/Sub mechanism and is based on blockchain technology; however, needs more autonomous and diversified computing for node management.
4. Algorithm C4.5 and Weka API
   Another proposed solution made use of the C4.5 machine learning

algorithm and the Weka API to provide configurable strategies for observing behavior patterns (Kim, Min, & Kim, 2019). The data obtained from different devices are analyzed by Weka API and implemented by C4.5 algorithm, which allows to prepare decision trees, which serve as a base for effectiveness using Machine learning technique and IoT paradigm. But implementation of more vigorous and complex classification algorithms such as Random Forest is considered for a possible expansion, in enactment of expectation process, of involuntary control of home automation devices.

5. The Event-based Access Control (EbAC) Framework The structure is primarily focused on the control and management of event handler to operate data. The access control event-based controller and policy module engaged in the event handling process are the main emphasis of the process model as described in Figure 2.3 (Zulkipli & Wills, 2017).

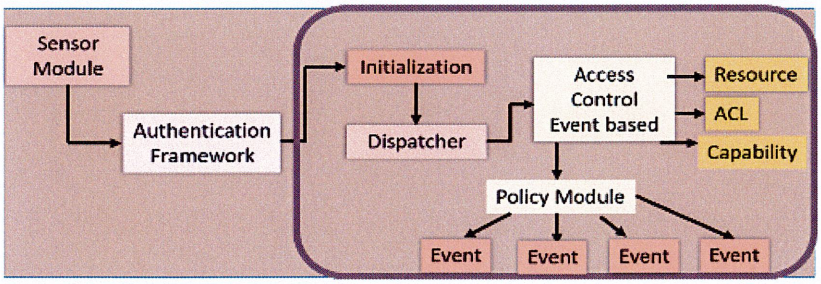


Figure 2.3: The Event-based Access Control Framework

In the process, the dispatcher initializes the event and availability of resources is checked by access control list (ACL). This policy is used to check events that whether they are allowed or blocked. After execution process, the event will occur. The framework still requires additional examination comprising of technological applications.

6. Contiki Operating System

This approach used to help a kernel developer port the operating system to any other platform or to develop supplementary device drivers for an existing platform (Dunkels, Gronvall, & Voigt, 2004). This process is attempting to provide a wide indication of the Contiki operating system, and as well as supply a thorough examination of some of the supreme vital features of the system. But additional topics such as multi-threading within a protothread, dynamic loading and unloading of software as well as the Contiki Toolkit GUI are few additional areas that could be discovered in a future hike.

7. Direct Lightweight Temporal Compression Technique
   The expression "direct" in DLTC represents a straightforward approach. The main goal of this strategy is to reduce the amount of operations performed by the algorithm, reduce the reconstruction error, and prevent generating data points that do not exist in the original set (Klus et al., 2021). But it still requires improvements in, reduction of error, reduction of capabilities and reduces amount required operations.
8. Compressive Sensing Technique
   Compressive sensing (CS) is another compression technique usually used for images at different time intervals for compression of data in IoT applications. In (Reyes-Campos et al., 2021) a multi-signal compression technique based on fuzzy algorithm was proposed. This technique involved the compression of data by using a wireless sensor on multi-signal environment and compressed the data by approximately two times. Another technique proposed by (Gaeta, Loia, & Tomasiello, 2015) is 2D lifing wavelength multi-signal data acquired from various sensor nodes, is compressed using a transformation. The proposed technique achieves compression ratio of 1.33. Moreover, these techniques can recover data accurately. The CS technique en-

sures signal recovery at an appropriate rate when dealing with non-sparse multi-dimensional signals, with different scales of values by employing signal sparsity; nevertheless, the CS methodology suffers when dealing with non-sparse multi-dimensional signals with varied scales of values.

In this section, we discussed the performance and effects of all of the algorithms related to compression techniques. Different algorithms have been described in which few have edge on the basis of efficiency, few works on high consumption of energy, most of the discussed algorithms focused specifically on developing the blockchain, but time transition usually becomes the most concerning constraint. Regarding the compression of data and event generation, usually requires additional devices for verification of algorithm authorization. But the proposed algorithm is focused on compressed lossy based technique, which is simple, efficient suitable for multi-repetitive events, most appropriate for compression purpose and reduces time of transition in efficient manner.

Basically, these all techniques are implementing compression technique, on low compression ratio, tested on real devices. In the following section, compressed lossy based technique is presented with the sensor which in return, expected to yield compression ratio and recovery accuracy. The proposed strategy will work on the mechanism if an event occurs, the data will record that event and the data will be compressed based on that event.

For securing optimized results, the choice of algorithm and choice of sensor plays a vital role. Different sensors are used differently based on voltage, light, humidity and temperature. The selection of both algorithm and the sensor affects the performance in terms of energy consumption, compression ratio and average absolute error (Hussein,

Abdullah, & Alduais, 2020).

Another compression technique is provided by (Abed, AlKandari, Al-Rasheedi, & Ahmad, 2020) for image compression. This compression algorithm is based on FPGA to excel the compression process, reduce the latency and inaccuracy. This unique technique comprises of a division of a single array into two subarrays, in parallel, which accelerates the compression process and give results of both subarrays in optimized efficient and less amount of time.

2.2.2 Security At Physical Layer

The physical defense infrastructure is crucial in all aspects of cyber security. Considering cloud servers and corporate headquarters are sheltered outside closed door meetings, physical security is commonly assumed for being robust. Without several more IoT devices in the environment, businesses can't consider physical layer security taken lightly. A vulnerability of the physical IoT security mechanism could allow malicious adversaries to get details concerning an IoT device, replicate the certain data stored or acquired from a device, and possibly affect its programming. Physical access to IoT devices could enable physical manipulations, optical or electromagnetic fault injection, side-channel investigation, configuration updates, and other cyberattacks. An infected IoT device has the ability to acquire exposure to other parts of network. In conjunction to cyber-attacks, physical security risks exist, Theft and vandalism, flooding, damage from leaks, fire, electrical natural catastrophes, surges, accidents, overheating, and other factors make IoT devices susceptible. Two distinct prerequisites for achieving authenticity and secret communication at both ends in the physical layer for Io devices are a secure architecture platform and decreased resources. Different solutions are explored as recommended practicable approaches and validated as effective methods following evaluation for delivering an IoT secure structural

platform at the physical layer. The strategies are centered on the main goal of ensuring secure message transmission while minimizing weaknesses and assaults. This section provides a variety of secure techniques to demonstrate the work that has been achieved in former years to make the physical layer secure for IoT. In this section, we provide a comprehensive overview of the conceptual basis of physical layer security challenges, as well as techniques presented by many researchers in maintaining the physical layer protected and reliable.

1. Anti Jamming

   Jamming has long been thought of as a negative aspect of communications networks. Jamming can produce interference with the sent signal, causing the decryption processes at the received signal to be impaired. When jamming (e.g., a fabricated noise signals) is directed against an unauthorized person, however, it might damage the eavesdropper's spectral efficiency. Following that, if the eavesdropper's channel state is deteriorated to a specific level (i.e., lower beyond that of the authorized received signal), perfect secrecy can be established, corresponding to the wiretapping network scenario (Huo, Tian, Ma, Cheng, & Jing, 2017).

   A lot of research have been conducted with a variety of recommended strategies, with jamming being one of the most significant and promising. Jamming has long been thought of as a method of creating unwanted interruptions in order to disrupt conventional communications (Q. Yan et al., 2016). Nonetheless, when employed properly, such as jamming at unauthorized persons with a right approach, it can be advantageous. A jamming technique, in particular, governs how an artificial distortion transmission is transmitted to eavesdroppers in order to successfully decrease their channel characteristics from effective interpretation.

To accommodate the growing need for wireless communication systems, (Q. Yan et al., 2016) suggested Massive MIMO networks. It takes advantage of a large density of transmitters at the docking station and uses rudimentary transmission computation to accommodate a modest number of consumers. It really has recently become a significant research subject as a viable technology for prospective communications networks. Humongous MIMO transmission presents new issues in the design of jamming systems. Firstly, when the count of antennas increases, propagating false noise transmissions in the authorized channel's positional null space may become impracticable due to the null space's computation overhead, which is primarily considerable for the large-dimensional channels vector. Secondly, due to the obvious large number of antennas accessible, randomized and independent manufactured interference may be averaged out, rendering unified jamming lesser effective. Finally, pilot contaminated might have a negative impact on channel identification, resulting in incorrect jamming pattern development and encryption performance problems. As a result, innovative jamming strategies for Massive MIMO networks will be required to overcome certain issues.

2. Artificial Noise Injection

   In the model presented in (Letafati, Kuhestani, Ng, & Beshkani, 2020), a thorough research was supplied for insuring privacy information and transmission dependability in a D2D (Device to Device) communication system. The author detected a passive intrusion detection system and also an active Adversary Jammer in the specified network. The Artificial Noise approach was utilized to ensure hidden communications, and thus the terminals used Frequency Hopping technique to strengthen overall susceptibility to jamming assaults. The research study created a unique restricted formulation for the ESR (effective

secrecy rate) measure for this system model to verify the usefulness of the suggested technique. Moreover, a statistically efficient authority allocation technique was established to enhance the systemically secrecy performance ESR. (Tang et al., 2020) proposes a physical layer-based secret key exchange mechanism both for MIMO (multiple input-multiple output) IoT devices that reduces the propagation delays caused by key extraction in MIMO IoT devices. Such is precisely the proposed method addresses both private key distribution and communications. It's accomplished with MIMO self-injection AN (SAN) transmission, which aims to optimise the transmitted SNR (signal to noise ratio) at diverse antennas of a permissible IoT network, based on the significance of confidential key distribution to user. The solution presented above only requires either device to transmit piloted signals towards the unauthorized, reducing overall IoT network disruption and overhead expenses even while reducing the risk of sensitive data breaches toward other IoT customers and eavesdropping devices

3. Channel Based Bit Flipping

   In the investigation (Hussain et al., 2021), the researcher employed grey coding to construct a low physical layer authentication approach over an Internet - of - things based health monitoring system in attempt to safeguard exchanged medical statistics despite keeping biological parameters. The analysis focused on a number of established competitive contexts in which an adversaries may listen in on transmissions and estimate underlying payload utilizing current packets inspections approaches. The research found that the implemented physical based authentication solution efficiently secures patients transmitted information, particularly when it is accessed through an adversarial. Stream mapping variation (CBMD) is additional technique

presented by (Pechetti, Jindal, & Bose, 2018), which tries to increase confidentiality at the uppermost layers of resources limited interconnected systems. When the true recipient is sufficiently isolated from the attacker, the maximum feasible signaling falsified alarm ratio (SER) can be reached at the eavesdrop by effectively establishing a map choose approach. So when principle and adversary pathways are interlinked, requirements for activities at the opposition and authentic destinations on the matching optimal output have been devised. The simulations outcomes show as the adversary's enforced SER is fairly considerable within a legitimate circumstance with connected network. The above strategy confuses an eavesdropper by utilizing the natural unpredictability of the electrostatic network as well as the various translations allowed for M-ary frequency attenuation and modulation scheme (M-PSK) configurations. When the permitted and observed channels become mutually exclusive, the eavesdropper is shown to exhibit a symbolic error rate (SER) around M1/M. When the channels are interconnected, although, effective and inadequate approaches for their individual optimal results are developed at the source and illegitimate participants. CBMD's proposed approach enhances integrity just at physical layer of finite resource IoT endpoints in an outlay manner. Whenever the authentic transceiver is successfully separated from the perpetrator, it has been demonstrated that the biggest possible SER may be formed just at perpetrator by efficiently designing a navigational selection mechanism. As a result, when the basic and adversarial networks are linked, the characteristics of procedures on the combative as well as genuine nodes were identified regarding their respective optimum performance. In a genuine situation with interconnected streams, the enforced SER at the adversaries is fairly substantial, according to the simulation results. As illustrated

in (Pechetti et al., 2018), CBMD is an efficient and restricted approach for boosting its ABER during an intercepting as well as rendering the function challenging in data processing. This has been further observed that whenever the approved and unapproved communication channels are independent, the proposed technique induces an ABER of 1 2 by choosing an appropriate flipping breakpoint at S (D). For the interconnected circumstance, the appropriate barrier at Intercepting and S(D) with their respective appropriate adjustment were computed. A channels basis mapped diversification (CBMD) approach for a sources (S) as well as destination (D) pairing would be employed to enhance the averaged bit errors rate (ABER) for an unapproved entity (E). Whenever the S D as well as S E streams are autonomous, CBMD yields an ABER of value 0.5 pointing E. In the instance where S D and S E are related (according to E's closeness towards D), the study has created a beneficial mechanism pointing E which contributes to comprehensive effectiveness on E.

4. Secret Key Generation

   (Margelis et al., 2017) proposes SKYGlow (Secret KeY Generation for Low Wattage Applications), a physical layer secret key manufacturing strategy for IoT applications. In contrast to previously described roughly equivalent systems, SKYGlow optimizes key generator accuracy by introducing a Discrete Cosine Convert (DCT) procedure. The effectiveness of SKYGlow was assessed employing real data from an experiment with multiple off-the-shelf IEEE 802.15.4 broadcasters utilizing the Texas Technologies CC2650 microprocessor. SKYGlow employs a DCT process on the raw RSS data, resulting in increased efficiency and sufficient variability to obviate a requirement on a discrete amplifiers component. The method could be fine-tuned by transforming the RSS sequence utilizing the DCT,

as possibly a bit enhanced components could be eliminated arbitrarily. Lastly, Slepian Wolf Packing is employed to verify evidence. The research showed how SKYGlow can generate 1.66 confidential information per packet on mobile devices and 1.77 hidden bytes each packets of static devices, surpassing conventional state technologies for connected systems and allowing both for faster and highly effective disguised generation. (Ali, Sivaraman, & Ostry, 2013) is the first to employ communications channels to create private keys in the critical and specific context of body-worn healthcare implants. The investigator placed the concept to the test using off-the-shelf technology as well as each unit placed on the human body in scenarios similar to those encountered in real-world applications, like as an inside office. Notable contributions to proposed study encompass the number of things: (1) The discovery of non-simultaneous networked inquiring by connecting end-points as the primary mechanism of identification confirms the contradiction. (2) creating a viable filtering approach to minimize this disparity, substantially improving signal connectivity between the various endpoints while keeping essential diversification and (3) demonstrating that by limiting key production to intervals of substantial channel variance, they can achieve better key consensus. In multiple example body-worn circumstances, the existing research has demonstrated that the method effectively construct private patterns with 99.8% participation, yielding in closer corresponding 12 8-bit key each half hours. The method is restricted, does not involve sophisticated channels examination nor key reconciliation, as well as creates strong vital components at a rate that allows for key renewing to proceed in phases. Regardless of the fact that continual patient monitoring devices receive medical readings numerous time every second, they frequently analyze them in endpoints (for exam-

ple, by synthesizing or aggregating) before transferring the findings to the control central area, lowering radio transmission. The goal of the study was to acknowledge the inquiry as rapidly as feasible (typically 10-20ms), permitting the both endpoints of the connections to examine the channels within rapid succession.

5. Optimal Quantization

   (Wang & Liu, 2020) proposed a pathway determination strategy based on a decision tree enabling secure double hop wirelessly systems. Input characteristics are produced by the suggested security rules of authentic and reliable channel status information (CSI). To investigate the influence of compression settings, the researchers created three separation criteria: shared information, characteristic selecting ratio, and Set of standards. The study compared the decision-tree-based method to other comparison methodologies such as optimal selections to see how effective it is. Whenever the normalization variables are calibrated appropriately, the selection tree-based approach produces confidentiality comparable performance to optimum selection findings, according to simulation data. Following to a cost research, the decision-tree-based approach has lower processing complexity, smaller comments quantities, and fewer untrusted CSI demands. In this study, deep learning was employed to solve the problem of secure packet relaying using a data-driven strategy. Secured relays decision was made into a multi - class classification challenge, which was solved using a decision-tree-based approach with three segments: training query processing, decision tree formation, and channels decision forecasting. A functionality approach is offered that quantizes the proper CSI of eligible and observing channels to continuously provide information in order to meet with the selection tree's need that input data assume unique values. As a consequence, decision relayed

infrastructures merely quantified CSI inputs, using far fewer bits in the predicting stage. The author also constructed three originally meant, namely memory recall, information gain proportion, and Gini index, for enhancing decision tree projections and improving compression choices. According to simulation results, the proposed decision-tree based methodology should achieve adequate findings in perspective of mean secrecy levels simultaneously decreasing computational complexity and feedback amount if the normalizing constants are adjusted appropriately. Another study (Soni, Upadhyay, & Kumar, 2019) proposed a wireless private key generation approach by pre-processing the transmit power signal (RSSI) of transmissions sent across Alice and Bob using sliding frame averaging (MWA). The recommended approach performs significantly better at low SNR levels. The amount that the RSSI design's standard error improves defines the width of the movable panel. To decrease recurring errors and improve bit discrepancy (BDR), it is also advised that the pre-processed RSS signal be quantified utilizing a Lloyd-Max centered quantized. The results show that using the suggested technique and the defined time window, the bits discrepancy rate (BDR) significantly improves at lower power. Spontaneous testing on the produced keys using the National Center for Standards and Technology's (NIST) randomized test set is also used to assess the success of the suggested approach. The extent of the moving window was determined using the correlations matrices and measures of variability of the RSS circuit layout. The study used the Lloyd Max approach, which reduces bit disagreement, to achieve the maximum deformation. Moreover, with baseline SNR of 16 dB, an increment of around 42 percent in BDR was identified at a specific window dimension comparison to non-average paradigm (m=1). According to simulation results, the proposed processing technique

appears to improve BDR largely in the weakest SNR region, making it suited for over-crowded IoT networks.

6. Compressive Sensing

   IoT devices must be capable to operate autonomously for long periods of time and be recharged with an on-board power. IoT nodes power consumption should indeed be lowered to meet these objectives. It mandates the hardware's energy generation as well as the competency of communications standards and procedures, as well as software that executes specific specifications and preventative procedures to keep interaction among two ends unharmed. As a result, the computing ability of these subsystems is frequently insufficient to run a comprehensive software application devoted to mitigating attacks (Bashir & Mir, 2018). Certain suggested works have been thought out by taking this element into account. According to the material offered in (Liu, Hu, Sun, Du, & Guizani, 2020), physical layer secrecy (PLS) appears to be a realistic technique for securing wireless technologies because orthogonal frequency division multiplexing (OFDM) is widely used. On either side, most existing OFDM-based PLS systems possess limited mobility in their secret keys, typically are established considerably prior to actually data. The combination of OFDM with spectral sensing (CS) provides a powerful resolution to the issue. The current study proposed the PLSSCS physical layer protection scheme for OFDM-based IoTS systems as a result of the proposed strategy. By employing channel assessment rather than of far before data, it can mitigate for the disadvantage of key removal. To improve IoT security, the suggested PLSSCS may be used as a P-box cypher basics that modulates with the alterations of OFDM packets.

7. Fountain Coding

   A novel transmission technique (Sun, Ren, Du, & Wang, 2016) was

developed to enable a DF-based (decode-and-forward) hop-based collaborative platform. This cutting-edge technique combines fountain coding on the application layer with collaborative jamming on the physical layer. As a consequence, the legitimate beneficiary will very likely collect many fountain packets before the eavesdropper, therefore increasing transmission camouflage. By using Foundation Coding, packet transmission security could be guaranteed as the subscriber acquires numerous fountain packets just before undercover informant. A cyclic rotation-based jammer strategy is meant to strengthen the channel state discrepancy between the source and destination of aggressor transmissions in order to achieve this criterion.

A fountain-coding based transmission system was devised in another research effort described in (Sun & Xu, 2018) to secure transmission across decreasing wiretap channels. It clarifies the well-established unique strategy to developing new fountain code, which dynamically modifies a coding style centered on disruption predictions and limited responsiveness. The suggested encoding architecture is compliant with the time-changing channel characteristics of an authorized network, not with the networks concerned with eavesdropping interconnections. As a result, there is no risk of data leak, and the genuine recipient's lag time requirements are also met. The suggested fountain coding method was designed to prevent data leakage in degraded wiretapping networks by predicting interruptions. By exploiting interruption projection and constrained responsiveness, the fountain encoder dynamically adjusts the coding parameter, assuring that the legal beneficiaries receives the specified number of encoded and protected packets well before unauthorized individuals, ensuring interaction exclusivity.

The deep analysis of all the proposed strategies by different tech-

niques have been discussed with their major contribution in different techniques including anti jamming, artificial noise, Channel Based Bit Flipping, secret key generation, optimal quantization, comprehensive sensing and fountain coding. Different strategies proposed their different models as described in Table below.

Most of the proposed techniques fulfil CIA (confidentiality, Integrity and Availability) but if the technique is focusing on integrity, then confidentiality and non- repudiation is not fully covered and vice versa. So a proposed technique is needed to be developed to keep the physical layer secure in terms of data transmission and receiving at receiver end. By keeping this consideration a technique of RC6 is applied to keep the physical layer safe for IoT data. RC6 is advanced encryption technique which is fast, less resources required and having a strong encryption power. The main debate is the secure communication by using an authentic source at physical layer. By keeping this ultimate goal in mind a proposed strategy has been introduces by using RC6 Encryption/ Decryption technique in which Alice sends an encrypted message to Bob and will be decipher and decrypted. The decryption will restore the same unique information that initially sent for transfer, which the Bob can decrypt right now. The encryption/decryption strategy for generating the encrypted message for reliable communication is the main contribution herein. Ultimately, the communication's authenticity may be verified by decoding the encrypted message, which will return the similar previous message sent from the Alice.

2.2.3 Zero Knowledge Proof

Goldwasser, Micali, and Rackoff proposed zero knowledge proofs (ZKP) in 1989 (Goldwasser, Micali, & Rackoff, 1989). It is possible to demonstrate that a statement regarding secret data is correct using this type of cryptographic primitive without revealing any other information on the secret data. Ever since, ZKP has grown in importance as a field of study, owing to its ability to provide a novel description of said complexity class NP (Non Deterministic Polynomial) utilizing interactive programs, as well as its utility in the construction of numerous cryptography algorithms. If provided the component x,(Morais, Koens, Van Wijk, & Koren, 2019):

$$L\varepsilon NP \tag{2.3}$$

A prover can persuade a verifer that x does really belong to L, i.e. that there is a witnessed 'w' regarding 'x'.Particularly one is concerned in proof of knowledge (PoK), in which the prover cannot primarily persuades regarding the identity of a witness, but also reveals particular the prover acknowledges that witness.Conciseness is a desirable feature of these proof methods, which means that the proof volume is minimal and can be confirmed speedily. zk-SNARKs are a type of such design (Groth, 2010). ZKP is now being utilized to add anonymity to DLT (Distributed Ledger Technology) and blockchain systems. For example, ZKP enables the creation of customized payment cards, To brief, ZKP allows parties to send virtual currency while concealing not just their names but also the amount being sent, called denomination. ZKP can be used to obfuscate this information yet nevertheless allowing payments to be validated (Morais et al., 2019). Few contributions are discussed below to emphasise the importance of ZKP.

1. **Port knocking**

   Port knocking provides a mechanism for validating clients and authorizing their desired actions through a closed posture firewall, allow-

ing servers to provide services to authorized clients without having to open ports within the firewall. Port knocking advancements had already reflected in an expansion in design complexity, restricting port knocking approaches from achieving their full capacity. 'Crucible' is a revolutionary port knocking solution that offers a safe authentication technique with great usability and stealth features, enabling server and service to stay undetected and secured. Crucible offers an unidirectional system in which the client just needs to remember a command, the server's IP address, and a password. The solution is being promoted as a way to defend servers from everything from port scanning to zero-day exploits. Cryptographic hashes were generated using chaotic systems to act as a randomized validator for both the client and the server. Crucible uses a solitary packet among client and server to authorize commands, having a payload that is probably unrecognizable from a randomized number. Crucible has a basic, secure, and stateless design. It is portable, and to authenticate, the user simply has to remember an IP address, a password, and a query name (Major, Buchanan, & Ahmad, 2020).

2. **Blockchain-based zero-knowledge proof model**

   The digitization of patient medical data and the sharing of part of that data with entities outside of protected networks could raise serious privacy and integrity problems. The BZKP (Blockchain-based Zero-Knowledge Proof) model is an IoT-based diagnosis paradigm that combines a zero-knowledge proof solution to be developed for protecting patient privacy and provides patients' prior agreement on any access to their data, particularly their medical status and payment history. The suggested model is being developed to enable a flexible and comprehensive data exchange architecture that ensures sensitive data privacy while ensuring high availability. It also uses the blockchain's

immutability properties to guarantee great data trust and integrity. To address the difficulties of traceability and confidentiality in Bahrain's smart cities, BZKP is built on pre blockchain accessibility tokens. As a corollary, the paradigm enables various stakeholder to interact patient data in a secure and trusted manner while retaining privacy, trust, and high availability. The tokens, which provide programmable actions for streamlining the prescription dispensation procedure for independent pharmacists in a decentralized system with high confidence, can be employed with the zero-knowledge proof. The incorporation with the zero-knowledge proof using the blockchain allows for the execution of blockchain queries without disclosing any additional information, ensuring the privacy and security of patient data (Al-Aswad, El-Medany, Balakrishna, Ababneh, & Curran, 2021)

3. **Zero-Knowledge Proof-of-Identity (zk-PoI)**:
   In order to remove the inadequacies of Sybil resistant methods such as Proof-of-Work (i.e., rising power and physical expenditures) and Proof-of-Stake (i.e., investment hoarding and fairly low volume of transactions), Zero-Knowledge Proof-of-Identity from trust - worthy public credentials (e.g., government identification cards and/or ePassports; eSIM) is presented to permissionless blockchains. When implemented on a blockchain employing a consensus process centered on cryptographic randomly selected nodes, ZK-PoI effectively restricts the amount of processing nodes a single user may run while keeping membership available to everyone, avoiding the challenge of full decentralized and the blockchain scaling hypothesis. A zk-PoI bitcoin is shown to have the essential favorable qualities in resolving among the most important concerns in blockchains:

   - A mechanism for issuing bitcoin incentives depending on a distinctive Nash equilibrium that is motivation.

- Mining's strict dominance above every other PoW/PoS bitcoins, resulting in the zk-PoI cryptocurrency gaining the preferred choice of mine workers, has been shown to satisfy a Nash equilibrium as well as the Evolutionarily Sustainable Strategic plan.
- The cost of Crypto Anarchy is paid by PoW/PoS cryptocurrencies, which is redeemable by the maximum effectiveness of zk-PoI, which accomplishes the societal equilibrium.
- Because of the cheaper costs of its network, it has reached a distinct equilibrium in which it outperforms conventional modes of insurance.

The adoption of zero-knowledge protocols ensures that the accuracy of the Sybil-resistant, anonymized identification recorded to the permissionless blockchain can be verified by the public (Sánchez, 2019)

2.2.4 RC6 Encryption Technique

RC6 is a sequel to RC5. It is a symmetric block cipher. RC6 is also known as RC6-w/r/b, with the w, r, and b requirements suggesting the duration (in bits), number of repetitions, and asymmetric encryption in bytes, respectfully (Enugu, 2008). The RC6 is a linear expansion of the RC5, and instead of the two registers used in the RC5, it uses four 32-bit registers. The usage of 32-bit entries in RC6 is justified by the reality that each spinning is executed repeatedly. RC5 allows one spin per half round, whereas RC6 allows one spin per half round. More bits are used to define the amount of rotations every round (Faragallah et al., 2020a). The usage of 32-bit registers in RC6 is motivated by the fact that each round has two spins, as opposed to one spin in one half round in RC5. More bits are utilized to define the amount of rotation in each round. For more details on the RC6 encryption/decryption algorithm, the reader might refer to (Paje, Sison, &

Medina, 2019)(Pachghare, 2019).The block length of RC6 is 128 bits, while key sizes of 128, 192, and 256 bits are allowed, with a maximum key size of 2040 bits. RTL depicts the signal flow in digital circuitry. It's set up to support a wide range of round counts, word lengths, and key sizes. RC6's structure is nearly identical to that of RC5, including compute rotations, modularity addition, and XOR operations. RC6 can be thought of as a mixture of two RC5 encryption procedures that happen at the same time or in parallel.

To protect recorded and transferred image data against malicious assaults, a variety of cybersecurity techniques are used, including digitally signed verification and cryptography techniques(Faragallah et al., 2020b). Conventional cryptography systems such as IDEA, DES, RSA and ElGamal are based on difficult computational calculations (Nemati & Yang, 2010).

RC6 was created in 1998 as a modification of RC5 to meet the criteria of the Advanced Encryption Standard (AES). To overcome the constraints of classic ciphering approaches, it makes extensive use of data-dependent rotations. It uses four 32-bit registers and adds numeric multiplication as a supplementary operation, resulting in a considerable increase in the diffusion achieved each iteration (Adhie, Hutama, Ahmar, Setiawan, et al., 2018). It is capable of processing 128-bit blocks and is simple to construct. As a result, the level of security and throughput is increased.RC6 statistics provide a strong indication of encryption strength and the difficulties of cracking the code(Faisal & Ameer, 2020).

2.3 Discussion

Internet of things shows a very imperative part in this recent world. It authorizes the world with smart homes, smart cars and plenty of other things. The IoT have different advantages i.e. automation, control, communica-

tion, monitor and the most important it is not expensive as well as saves time. IoT has the ability to connect together with other devices with the help of machine to machine (M2M) approach, which results in transparency in results with greater quality and lesser problems(Elrawy, Awad, & Hamed, 2018). IoT offers the facility of connectivity of physical devices using wireless communication, as it was difficult to communicate without human interaction but IoT made it is possible and produces efficient results in output.

The Internet of Things (IoT) is a structure of physical items with integrated sensors, controllers, and networking devices that has significant economic implications. Huge volumes of data are acquired and analyzed using an already range of applications aimed at meeting the different and multifarious needs of both rural and urban areas, in order to reorganize and expedite manufacturing and service operations across enlightened recommendations and limitations. IoT applications include digital infrastructure, precision agriculture, intelligent systems, parking and land management, intelligent traffic, e-Health, youth development, and process sensing, to highlight just some. To acquire sensitive information in the proper location, IoT devices require the right sensor. Relying on the nature and intention of the IoT device, the evidence gathered may differ. IoT systems use methodologies, techniques, and technological innovations to reinforce specific regions and handle various elements such as energy conservation, reliability, and online collaboration tactics. The Internet of Things isn't the only technology available; rather, it's the single most powerful technology that applies. The Internet of Things (IoT) involves a conglomeration of interconnected technological solutions. In all of the aforesaid domains of life, the ambition of Industry 4.0 is to strengthen standard of life while eliminating manually intervention.

The content generated by a large number of IoT platforms is critical for use in imaginative infrastructure. IoT technologies have made significant

development in the preceding year, but there are currently great practical challenges. Additionally, the network design of an IoT environment has a significant important challenges with dominance and consolidation. As an enhanced form of current design, IoT network architecture parallels legacy network infrastructures. Without a doubt, the essential function of two very different types of architecture is data transfer; nevertheless, the legacy network's data transmission strategy is insufficient for the IoT network. In the IoT environment, legacy internet architecture confronts different constraints such as conversion efficiency, computing power consumption, and so forth. In an IoT framework, the challenge can be alleviated through decentralized and distributed approachability. It contends that secure communication system with unstructured and extensive interconnectivity is critical in an IoT virtual environment. Nevertheless, IoT confidentiality is a significant difficulty when considering illicit entry, vulnerability, and assault as a comprehensive network. The three most important safety parameters are secrecy, authenticity, and accessibility, all of which are challenging to satisfy because IoT devices have legislative resources. Concurrently, the security of data available to its genuine user is confirmed. As a consequence, registered participants can be authenticated using login information or credential verification and access control security mechanisms. Consequently, access control research is generally focused on the infrastructure rather than the software modules. The resolution of access commands is made possible by an assets policy, also known as insurer power, in which the guidelines are formed and enforced. The event-based intrusion prevention structure of IoT software components necessitates authorization governance and cybersecurity needs for authenticity, identity, and data confidentiality for IoT software application management. In all elements of cyber security, the physiological protective infrastructure is essential. Physical security is usually thought to be robust because virtualization workstations and organizational locations

are housed outside closed door meetings. Organizations non-performing handle physical layer security lightly till there are numerous enough Devices connected to the internet in the environment. Malicious adversaries could exploit a vulnerability in the tangible IoT security measures to obtain information about an IoT device, copy data saved or obtained by the device, and perhaps modify its programming. Direct access to Internet of Things devices could allow for physically interventions, optical or electromechanical fault detection, side-channel probing, connection modifications, but rather other cyberattacks. A malicious Sensor node has the capacity to get access to other network components. Physical security hazards occur in addition to cyber-attacks. IoT devices are vulnerable to theft and destruction of private property, extreme weather conditions, and damage from leakage, fire, electrical natural disasters, surges, collisions, electrocution, and other circumstances. A secure architecture platform and reduced resources are two distinct requirements for guaranteeing integrity and concealed transmission at opposite outer edges in the physical layers for connected systems. Following an investigation for supplying an IoT safe architectural framework at the physical layer, many options are studied as advertised feasible techniques and confirmed as beneficial methodologies. The tactics are focused on guaranteeing effective network communication while reducing susceptibility and attacks. ZKP, a cryptographic mechanism that has been utilized to guarantee confidentiality by architecture in the environment of DLT and blockchain, is a different approach to safeguard privacy information. In a nutshell, ZKP allows a prover to persuade a verifier that a specified statistic is correct without disclosing any more information than is strictly essential to persuade her. In conclusion, ZKP enables the proof that a concealed input value conforms to a precise interval. If we restrict this domain as all integer among 18 and 200, for example, an individual can use the ZKP methodology to demonstrate that she is over 18. This allows her to consume a

specific service in accordance with a set of rules, because without revealing her exact age. When it comes to trading platforms, when party A chooses to send money to party B, ZKP can be used to show that the amounts of currency in the transactions is positive; instead, if the quantity is negatives, the transaction will send money in the direction opposite, from B to A. For private, lightweight server identification, zero knowledge techniques were introduced. In a nutshell, ZKP allows counterparties to send simulated currency while hiding not just their identities however also the amount actually delivered, known as denomination. ZKP can be deployed to obscure this data while still allowing for payment validation.

A range of cybersecurity measures, especially cryptographically verification and cryptography techniques, are employed to secure captured and transferred imagery data from malicious attacks. Conventional cryptography systems such as IDEA, DES, RSA and ElGamal are based on difficult computational calculations. In 1998, RC6 was developed as a refinement to RC5 to handle the Advanced Encryption Standard's requirements (AES). It makes massive use of computation rotations to circumvent the limitations of standard ciphering algorithms. It employs four 32-bit registers and adds numeric multiplied as an increase in the complexity, leading in a significant increase in the diffusion achieved with each cycle. It can handle 128-bit blocks as well as is precise to construct properly. With a outcome, both security and bandwidth have improved. The strength of encryption and the difficulty of unlocking the code can be determined using RC6 statistics.

2.4 Summary

This section covers the work done in data minimization in which different strategies based on data minimization has been discussed, security at physical layer has been also discussed in detail in which a deep study of all pre-

sented strategies utilizing various techniques has been discussed, along with their important contributions in many techniques such as anti-jamming,artificial noise, channel-based bit flipping, secret key generation, and optimal quantization, comprehensive sensing, and fountain coding are just a few of the features available. Various strategies were proposed. several models, as seen in table 2.1. Moreover, work done on basis of ZKP has also been highlighted. As encryption/ decryption technique used is RC6, so RC6 has also been discussed in this section.

Chapter 3
Methodology

3.1 Overview

3.2 Proposed Strategy of Data Minimization

3.3 Proposed Strategy of Physical Layer Security Using Zero Knowledge Proof

3.4 Summary

Table 2.1: Analysis of proposed Ideas Related to Literature Review

S.No	Techniques	Proposed Methodology	Effectiveness
1	Anti-Jamming	Artificial distortion transmission by Massive MIMO network yan2016jamminghuo2017jamming	Advantage Effective Interpretation Disadvantage Multiple frequencies
2	Artificial Noise	Frequency Hopping technique letafati2020physical	Advantage It provides very robust transmission path in the presence of interferences such as multipath, noise and other wireless transmissions Disadvantage Needs complex, costly digital frequency synthesizers required to be used.
3	Channel Based Bit Flipping	Used Grey Code hussain2021testbed Proposed Stream mapping variation (CBMD) pechetti2018exploiting	Advantage: With digital circuits it is easy to distinguish between two voltage level Disadvantage: very difficult to come up with an arithmetic logic unit to support Gray code Advantage Fast approach Disadvantage Highly expensive in resources
4	Secret Key Generation	SKYGlow (Secret KeY Generation for Low Wattage Applications) margelis2017physical Body-worn healthcare implants ali2013eliminating	Advantage DCT possesses several traits make an effective tool for image compression Disadvantage Quantization needs to be handled Advantage Fast recovery of patient, less damage to patient Disadvantage Nerve damage, infection, and life span on batteries
5	Optimal Quantization	Decision tree enabling secure double hop wirelessly systems wang2020data Wireless private key generation approach by pre-processing the transmit power signal (RSSI) utilizing a Lloyd-Max soni2019wireless	Adv. Clear Visualization, Simple and easy to understand Dis. Over lifting, invariant, affected by noise, not suitable for large data sets Advantage reduces bit disagreement, to achieve the maximum deformation
6	Compressive Sensing	OFDM-based PLS systems bashir2018internet	Advantage mitigate for the disadvantage of key removal Disadvantage Not used as P-box cypher basics that modulates with the alterations of OFDM packets.
7	Fountain Coding	Fountain coding method 8570807	Advantage prevent data leakage in degraded wiretapping networks Disadvantage Small block length can cause these performances to drop by a large margin and lead to increased latencies within the storage system.
8	(Proposed Technique): Error detection Based Channel (EDBC)	Proposed Model for Encryption/ Decryption at Physical Layer Using RC6	Advantage Reduce Complexity through Encryption / Decryption and Error Detection at same time. Small block length can cause these Secure Transmission because of RC6 encryption/ decryption technique lowering in hardware utilization (power consuming reductions and space utilization) because of encryption and channel encoding into a single operation

Chapter 3

Methodology

3.1 Overview

This section covers the main working of all the tasks including data minimization, physical layer security using zero knowledge proof, and data encryption using RC6. Firstly, data is compressed and minimized as minimized data needs to be secured so security framework is proposed to keep data secure at physical layer using zero knowledge proof algorithm and then the data is encrypted using RC6 encryption technique to keep the data away from unauthorized user. Figure 3.1 represents the secure structural flow of tasks and methods.

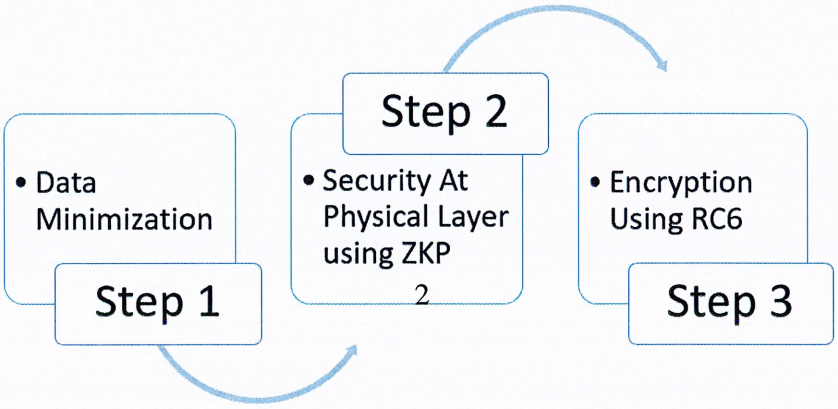


Figure 3.1: Secure Structural Flow of Proposed Methodology

3.2 Proposed Strategy of Data Minimization

This section covers the proposed methodology of data minimization technique in IoT. In the proposed methodology motion detection sensors will be placed at different location of the university campus so that they can sense the movement of an object based on the placement of sensors. Furthermore, these sensors will be attached to video capturing devices. The video recorders will be in sleep mode and no data will be stored during this time. Once the sensors senses an object a signal will be sent to video recorders to make them awake for the purpose of data recording. In order to describe the scenario, Figure 3.2 represents the main picture of the university on which different sensors will be placed at different places. For example, motion sensors are placed at university campus are shown in Figure 3.3. These motion sensors will be covering the entire area of the campus. Assume that the video recorders are in resting state of "0" which means that no data storing is being done. In case an object is sensed by motion sensors, a message will be sent to the video recorders to changing its signal state from "0" to "1" meaning wake up. As the camera is in the state of "1" the data storing will also start. The data storing will be continuous for the period of time in which sensors keep on sensing the object. Once sensors do not sense any object in the area, data storing will be stopped and the camera will go back to state of "0". The proposed methodology is very effective in terms of data transmission and storing energy utilization and increase in productivity, can be discussed with the help of case studies.

3.2.1 Case Study

In order to record/store the motion occurred, there are different sensors with cameras displayed at different positions in order to sense and capture the in and exit motion of the student arriving at university campus.



Figure 3.2: Main Picture of University with placement of sensors at different places

The strategy comprises of different sensors with cameras at different positions in a university campus. The purpose of these different sensors with cameras at different positions is to detect and record video of a certain time when an event occurs. The sensors with embedded cameras would be situated at different positions of the university campus. These sensors will capture and record videos at different positions when certain motion is being detected at these positions. The installation architecture of sensors with cameras can be described as:

- Sensor 1: Store video recording at the entrance of the university
- Sensor 4: Store video recording at the exit of the university
- Sensor 2 and 3: Store video of any motion observed as the student moves after entering the campus.

Taking into consideration, regarding the above mentioned scenario, being described in the Figure , when a car/ student in person enters through entrance, sensor 1 at entrance will detect the motion and its state is changed

from ‘0’ to ‘1’. it will start recording as the car/student approaches to any 2 and 3 by as the car or student proceed further or any motion occur.It means that as the object gets closer to the sensor, the motion is detected by that sensor and specifically, start video recording and this video recording will stop automatically as the object move little far from the range of sensor thus its state is changed from ‘1’to ‘0’. Now simultaneously, following

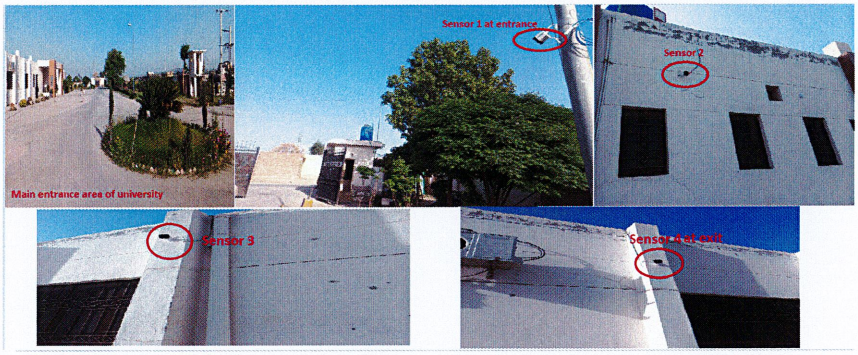


Figure 3.3: Placement of Sensors at different locations in university campus

The same technique and procedure, as the car approaches to sensor 4, sensor with camera installed here will do the same video recording on detection of an object; observed in the range. When the car is ready to exit, the sensor with camera at exit of University detects the motion and captures video and as the car leaves the campus, and drives out of the range of the sensor, its state is again changed to idol position ‘0’. Figure 3.3 is the combined picture of placement of sensors at different locations in a university which clearly shows that different sensors at different locations are placed to detect the motion of an object. It is obvious from the above mentioned scenario that this is a repeating process in terms of motion detection and video recording as an event occurs. This repeating process will be continued until motion is observing by that sensor and state of sensor is ’1’. As the student/ car or any other object moves away from the sensor, the state of the sensor will be changed from ’1’ to ’0’. So, as the student or any other object enter in university campus as shown in Figure 3.3, student will pass

by sensor 1, which is just in the entrance, the sensor will come in dynamic state and start recording the motion until the object moves away. The process can be described in the flow chart in figure 3.4. The flowchart in Figure 3.4 represents the motion detection scenario that when a motion is detected by sensor, event will occur and video will be recorded. But if motion is not observed and also if the object moves away, the sensor placed at specific location will be at static state.

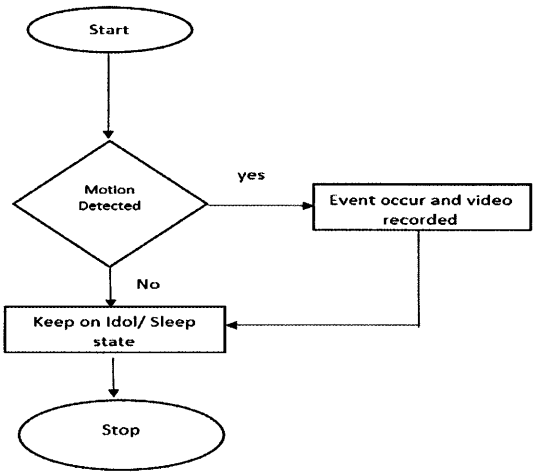


Figure 3.4: Flowchart for the proposed data minimization technique

3.2.2 Error Bound Lossy Compression Technique

The proposed strategy is based on error bound lossy compression technique. When compared to lossless compression, the lossy compression method provides better compression results (Cheng, Guo, Wang, & Yang, 2016). Lossy algorithms is usually used to achieve three times more reduction as compared to existing lossless algorithm. This study is about a "High Performance Computing Application" lossy compression method (HPC). The work also focuses on compressing multi-repetitive series in the most effective way feasible and reducing transition time. To start with, the algorithm

consists of an array MxN array (where M and N represents number of rows and columns). It is considered that data is transmitted at different nodes 'i' over different period P at different time interval 't'. If the motion is detected in the sensor, the energy state and state of sensor is detected which change its state from 0 to 1. This will lead to video recording process which starts the process of compressing the video as received at different nodes over Period p at time interval t.

3.2.3 Algorithm

Figure 3.5 represents the algorithm focus on detection of sensor's static or dynamic state and storing the video if it senses any movement in that specific area which is observed at different intervals of time. The proposed algorithm records the video in case of any motion detection just for maximum utilization of memory and storage capacity. If the motion is detected, the state of sensor is changed from static to kinetic and it will collect data, store video and compress the video in binary form. This is multi- level process which will continue as the object is detected again and again. The algorithm is designed on the same strategy based on motion detection representing in above Figure 3.3 and flow diagram representing in Figure 3.4.

Algorithm in figure 3.5 represents the complete guideline for data minimization process with embedding of sensors. This algorithm was followed to record the video at university campus which really turned out an efficient approach as motion is only observed when the event will occur and state of sensor will change from 0 to 1 at that time only, which means that only for that specific time the video will be captured. This in return, achieve our one of the goal to minimize IoT data traffic. Here is this figure 3.5, the algorithm will start working if there is motion detected and its represented by first statement of the algorithm which is energy > 0 and if motion is detected by sensor, in that case the recording of the video will start only. As

3.5 **Algorithm for Composed Compression Technique**

Require: input (MxN array), E (error bound), M(Rows), N (Columns)

1. While (Energy> 0 AND sensor-Detected= True)
2. Do
3. For each node ***i*** at each period ***p***
4. Do
5. Data (M x N)← collect data
6. Input (M x N)← store_video
7. Compress Video/ Data
8. Binary_output ← Compress video
9. Transmit_data (Binary output)
10. End for
11. End While

Figure 3.5: Algorithm for Proposed Compression Technique

recording process will start only if motion is being observed by the sensor. So, this is actually the data minimization technique as video capturing will start only if motion and energy is being observed by the sensor.

3.3 Proposed Strategy of Physical Layer Security Using Zero Knowledge Proof

3.3.1 Overview

The key point of contention is the use of an authentic source at the physical layer to provide secure connection. With this end aim in mind, a proposed strategy based on the RC6 Encryption/Decryption technique has been introduced, in which sender sends an encrypted message to receiver,which will be deciphered and decrypted. The decryption will bring back the original unique data that was originally sent for transfer, which receiver can decipher

right now. The fundamental contribution here is an encryption/decryption approach for creating encrypted messages for trustworthy communication. Finally, the legitimacy of the communication can be checked by decoding the encrypted message, which will return the sender's prior message.

Few methods will be used as encouragement for continuing to develop the author's way to keep the physical layer reliable, like the suggested scheme (Mohsin & Elmedany, 2021), which incorporated Internet of Health - care Things during COVID-19 by incorporating IoT and cognitive functionalities of diagnostic health coverage to obtain patient records in a truly secure manner. The SIMON lightweight blockcipher in VHDL is used in this method to preserve the secrecy of patients' private information and to maintain the required secrecy of particular activities (Alsaffar, Elmedany, & Ali, 2019). A further motivating scholarly paper addressed data transfer in intelligent transportation as well as how the RC5 Encryption/Decryption technique guarantees users' confidentiality in intelligent transportation. FPGA with Quartus Primelite Edition have been used to conduct this research. The approach was demonstrated to be effective in terms of intelligent mobility by presenting simulation that confirmed the RC5 algorithm's functioning. A further important research initiative (Sagheer, Searan, & Salih, 2018) is the formation of a new technique by merging RC4 and the S-Box of AES (Advanced Encryption Standard), as the RC4 algorithm has so many shortcomings, including such key bytes sliding between distinct values. Numerous attacks, such as the differentiating assault, are immune to the proposed framework, which would be implemented in a number of guidelines. The recommended technique for ensuring protection at the physical layer incorporates the author's key contributions to strengthening encryption at the physical layer for connected applications in IoT regime. It is additionally segmented into subcategories such as recommended protection architecture for cryptography at physical layer, framework of RC6 Encryption/Decryption Tech-

nique, and operating of RC6 at physical layer in Waveform enabling the improved explanation and clarity.

3.3.2 Proposed Zero Knowledge Proof Framework

If the sender wants to send the message to the receiver but the integrity or privacy of the sender's message should be kept secret and reveal only the part of the information while keeping the rest secure and private, this process is called Zero Knowledge Proof (ZKP). The verification of the identity is handled by the proposed ZKP. 'The flow of the information following the ZKP is mentioned in figure 3.6 given below:

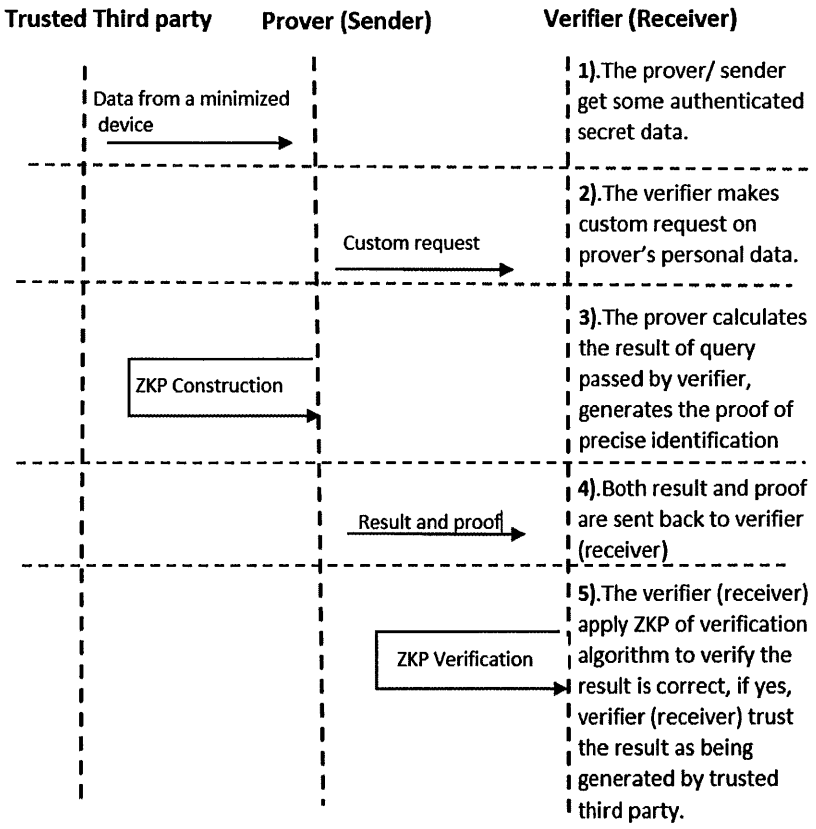


Figure 3.6: Proposed Zero Knowledge Proof Data Exchange Framework

The data is coming from minimised source, from a trusted third party

which can be a hospital or a bank, The prover/ sender get some authenticated secret data, the request is sent from prover (sender) to verifier (receiver) in a way that the verifier makes custom request on prover's personal data. Here, the ZKP is going to be constructed at prover (sender's) end, the prover calculates the result of query passed by verifier, generates the proof of precise identification. The result and proof send by the sender are sent back to verifier (receiver). The verified information is ZKP verification, if the result is correct, verifier (receiver) trust the result as being generated by trusted third party otherwise not.In order to get the shared information from prover to sender, the confidential information is being checked and verified and the result is received which is to be send to the receiver to get the result. this whole scenario is focused on the request of the information from receiver to sender, as a result the sender send the confidential information, the proof of that information is received at receiver which is checked in order to get the result. In case of our scenario, the purpose of ZKP is to detect only valid and actual motion detection, no unnecessary feed is not to be detected through this ZKP framework. Moreover , it will record only required information. ZKP is implemented on sensor and receive only that data which has motion and having real time motion detection.

3.3.3 Proposed Security Model for encryption at Physical Layer

The physical layer's fundamental task is to establish and terminated the integrity of a transaction amongst a transmitter and a receiver out across channel. As a result, electronic data is converted in the participant's devices in accordance to transmit signaling over a specified channels. Most of this implies preserving data confidentiality, authenticity, and accessibility (when appropriate) in the most economical, cost-effective, and secured approach

achievable.

To maintain protection in consideration, the author proposed a framework for confidentiality at the physical layer depending on the RC6 encryption/decryption methodology. The fundamental purpose is simple and clear: secure and secret communication between two endpoints. Figure 3.7 depicts the intended model for secure transmission using Error Detection Based Channel (EDBC). Apparently this model looks like a very simple one but involvement of Encryption/Decryption at conversion of signals and then decryption of signals again before modulation for decoding the message makes it unique in its form even in cryptographic strategies as well. The uniqueness in the model is that the proposed model provides a joint scheme of combination of encryption / decryption along with error detection in the channel. Error detection can be related to noise, eavesdropper in the channel. So, this scheme is the joint combination of encryption and error detection in physical layer. The privacy qualities of network encryption could be leveraged in this situation. As a result of the utilization of equipment, accuracy, performance, and cost savings are enhanced. It further provides adaptability in respect of structure and execution methodology. In terms of assaults, it's equally tough to develop lowest level detectors. When sender wants to send a message 'm' to receiver, through encryption using RC6 encryption, an encrypted message based on RC6 encryption technique, 'k' will be passed to EDBC to retrieve encoded cipher text as $k\prime_M$. With the help of key 'k', after retrieving $k\prime_M$,The receiver decodes and decrypts in one step utilizing EDBC, with the help of key 'k', to acquire m' for receiver. The decrypted message is then passed to decoder to be received by receiver. The proposed study integrates encryption and channel encoding into a single operation, potentially lowering hardware requirements. As power consuming reductions and space utilization are of highest priority in current wireless transmission, this could contribute to a lowering in hardware utilization,

which in response could play a role to an elevation in power savings. In contrast to two separate procedures, the EDBC does both encryption and error detection in a sequential manner. m (message) is converted to m' after demodulation of decrypted message. The decryption will return the same original message which was sent for transmission, and is ready to decode now to the receiver. Here, the main contribution is the encryption/ decryption technique for generating the cipher text for secure transmission. At the end, the validity of the message can be verified through decrypting the cipher text which will return the same original message which was sent by sender.

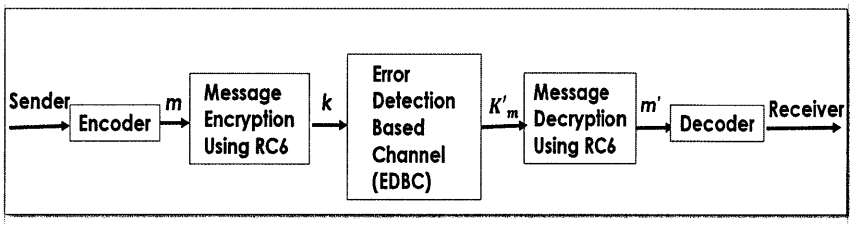


Figure 3.7: Proposed Model for Encryption/ Decryption at Physical Layer Using Rc6

3.4 Summary

This research study proposed a new secure IoT strategy for reducing data generation. With the help of this new method immense amount of data generation is minimized and secured at the same time. Moreover, the technique is implemented in virtual environment for performance evaluation. In order to further proceed with the new technique; an algorithm along with case studies and the implementation part is presented which verifies that by implementing this new technology, minimization and compression of data in IoT can be done with ease. According to proposed technique, the data is compressed and for the security of proposed compression technique,algorithm is verified through RC6 encryption technique in MATLAB

by using the video generated and converting the original video the encrypted video.

This research work creates a significant contribution to the security of the physical layer by employing the RC6 Encryption/Decryption mechanism, which would be widely appointed across several applications. The paper discussed IoT applications in various spheres of life, as well as the interaction between IoT and also the physical layer, as well as the key functions of the application and network layers. Various strategies for keeping the physical layer secure with IoT have been emphasized. The detailed analysis of all the proposed strategies have been highlighted with their methodologies to keep the physical layer secure. The techniques for keeping physical layer secure have been explained by different researchers in Section 2; including artificial noise, fountain coding, compressive sensing, channel based bit flipping, optimal quantization, secret key generation and anti-jamming. Furthermore the deep analysis of these techniques have been presented in Table 2.1 which critically overview each above describes proposed technique with advantages and disadvantages based on the work described in literature review. This analysis depicted that a secure and valid data transmission scheme is still in need which can transmit the data with security in an authenticated way at physical layer. By keeping this analysis under consideration, a novel technique of securing physical layer for IoT data is introduced in which security is maintained through encryption/ decryption process. The paper then provided a secure model to depict the work flow of the message from sender to receiver by applying encryption and decryption after the modulation and demodulation processes. The paper provides an EDBC which serves as the joint feature of error detection and encryption at physical layer. The practical implementation of the suggested technique was accomplished using MATLAB. As a result, this strategy appears to be a secure method for managing IoT data at the physical layer by encrypting

and decrypting the video using RC6 encryption/ decryption algorithm.

Chapter 4
Results and Discussion

4.1 Overview

4.2 RC6 Simulation Results Based on Video Encryption and Decryption

4.3 Experimental Setup

4.4 Limitations of Proposed Model

4.5 Discussion

4.6 Comparison of RC6 with other Algorithms

4.7 Summary

Chapter 4

Results and Discussion

4.1 Overview

Based on several investigations and research, RC6 has been established to be the most recent Advanced Encryption scheme in terms of security, convenience, compliance, and effectiveness.In order to secure the methodology, encryption/ decryption needed to be applied to check the performance. The techniques of RC6 in MATLAB has been used for this purpose. There is a dreadful need for integrity and confidentiality of information passed from one channel to another. RC6 have been used for encryption/ decryption technique. RC6 is a fast symmetric encryption algorithm that can be implemented in hardware or software (R. Yu, Yang, & Wang, 2020). RC6 is a symmetric a variable key cipher cryptographic key that is hardware and software compatible, adaptable to varied word lengths, and iterative in architecture (Verma & Singh, 2012). The reason of being fastest algorithm among all enforced to use as an encryption/decryption technique in proposed strategy. The RC6 algorithm is derived from the RC5 algorithm and organizes the bedrock for the RC6 method. The block size of RC6 can be 32, 64, or 128 bits, with a key length ranging from 0 to 2040 bits (Rivest, Robshaw, Sidney, & Yin, 1998).The results were recorded by using RC6 encryption/ decryption algorithm.

4.2 RC6 Simulation Results Based on Video Encryption and Decryption

Encryption and decryption were used to examine the functioning of the approach in addition to secure it. This was accomplished using RC6 algorithm in MATLAB. In the current research analysis, the sensors are embedded in the actual university campus so that the data achieved is the real life data in the form of video which shows the proper event occurrence and is stored accordingly. The main goal is now to convert this original video into encryptd video. But as it is already mentioned that ZKP is already implemented on sensor so that the data received in the form of video is not having any unnecessary feed in it.

Videos give exclusively spatially focused images data a dynamic attribute. A video is made up of individual frames that are sequentially organized in successive manner. An individual video frame can also be made up of many frames for various color streams or channels (RGB). So in this proposed strategy, a full RC6 algorithm is implemented with its three stages MATLAB. Then the algorithm is implemented with open source video encryption code (Raju, Umadevi, Srinathan, & Jawahar, 2008).

In a typical video encryption, a video is converted to frames, according to the frame rate of a video, certain number of frames are created. For example, if a video is of 5 seconds and frame rate is 30 frame per second,then 5*30=150 images (frames) will be created. When we read a certain image, there are three channels as video is colored, which are red, green and blue. there is a need to separate the channels and calculate length (x-axis) and height (y-axis) of each channel which is same for all channels. so, in this strategy, one pixel (picture element) is taken and process that through RC6. Let's consider that if 150 pixel is for height and 150 pixel is for length, then 150 * 150=22,500 pixel is for one channel. As there are three channels, so

each pixel needs to be taken and process through RC6, encrypt and encode it.

Keeping the above consideration under observation, the recorded video based on sensor implementation, frame rate is 30 frame per second, height and length is 720 and 1280 respectively. The number of pixel for one channel will be 921,600, similarly for second and third channel. So, each frame (image) is changed to pixel based on different coloured channels. This is how the encryption of each pixel is handled, if one of the pixel is left or not handled, encryption will not be done or handled.

In the proposed strategy, the source video can be separated into frames and audio during the encryption process. Then, from the video, the exact amount of frames are obtained. As the encryption procedure can only be completed in this amount of frames, those frames are transformed into images, which are then transferred to blocks and the block is encoded and encrypted using RC6 algorithm. After that, the frames and audio are turned back into video by merging the frames together again. The graphical structure can be well explained the proposed work done in Figure 4.1 for video encryption and figure 4.2 for video decryption method.

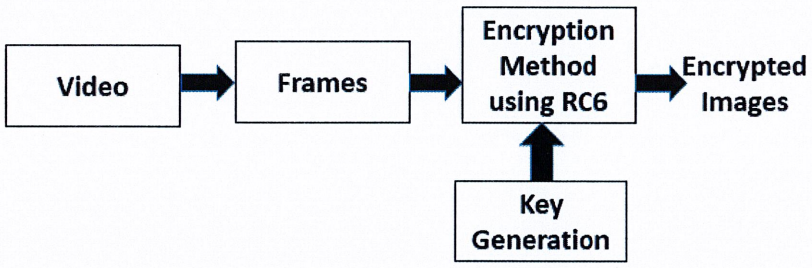


Figure 4.1: Video Encryption Method Using RC6

Now for the decryption method,the process will be reversed. As the encrypted images are received, decryption method using RC6 is applied, key will be generated which will merge all the frames to prepare the decrypted

video.The EDBC is there as well to perform the task of detecting the errors and providing encryption.

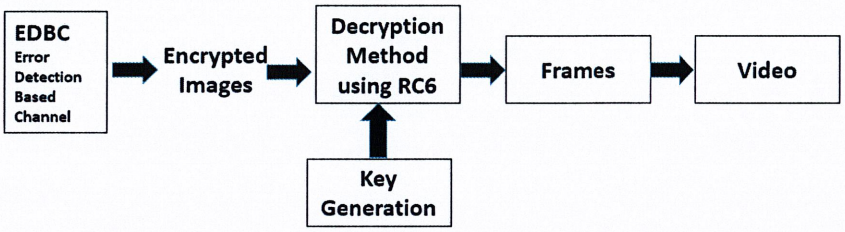


Figure 4.2: Video Decryption Method Using RC6

4.3 Experimental Setup

This section contains the information of the experimental setup which we have used to get the results. As we know while getting the results system specification matters a lot. We have used a system whose processor Intel(R) Core (TM) i7-7700K CPU @ 4.5GHz processor, using 16 GB memory, and 64-bit operating system. We have used MATLAB 2020b for the simulation purpose.

We captured data from camera installed in a college scenario and compressed using our proposed methodology before applying RC6 algorithm. We considered the following parameters as optimal values after trying several combinations:

Table 4.1: Parameters For Video Recording in RC6 Algorithm

Parameters	RC6 Algorithm
w (word size in bits)	32
r (No. of rounds)	20
b (Key length) in bytes	16
Block size (in bits)	32
No. of keys derived from key schedule	2r+4
Transformation Function f(x)	x(2x+1) mod 2w

The algorithms of encryption and decryption using RC6 are given below. These algorithms are implemented in MATLAB. The results of encryption and decryption on 5 seconds video of 1.10MB received after compressing it with the proposed methodology are shown in Figures 4.3 and 4.4. The original video recorded without compression algorithm takes 1GB on the storage disk. This shows the significance of the proposed compression algorithm over mainstream method without compression.

A digital image/frame comprises of three components, namely R, G, and B. If the three components are combined in a block, then the block will have data with 24 bits. However, the RC6 algorithm contains 32 bits registers. By default, shortage of bits in each block can be filled by the next bit of the pixel so that each block will have the appropriate size is 32 bits but this could result in faulty decryption. The problem that happens is if the number of pixels is not in accordance with the division, therefore we applied padding bit 0 in register block.

Algorithm (2):RC6 Encryption
Input: Plaintext stored in four w-bit input registers (A, B, C, D), r number of Rounds w-bit keys S [0, …, (2r+3)].
Output: Cipher text stored in (A, B, C, D).
$B = B + S[0]$
$D = D + S[1]$
$for\ i = 1\ to\ r\ do$
{
$t = \mathrm{B} * (2B + 1) \lll \log(w)$
$\mathrm{u} = \mathrm{D} * (2D + 1) \lll \log(w)$
$A = ((A \oplus t) \lll \mathrm{u}) + S[2i]$
$C = ((C \oplus u) \lll \mathrm{t}) + S[2i + 1]$
$(\mathrm{A}, \mathrm{B}, \mathrm{C}, \mathrm{D}) = (\mathrm{B}, \mathrm{C}, \mathrm{D}, \mathrm{A})$
}
$A = A + S[2r + 2]$
$C = C + S[2r + 3]$

Figure 4.3: RC6 Encryption Algorithm

Based on the above strategy, the practical implementation on real life video based on sensors implementation, a proper event detection is observed through those videos. Keeping under consideration about ZKP has also implemented on sensors as sensors only detect that data which has motion in it

Algorithm (3):RC6 Decryption
Input: Cipher text stored in four w-bit input registers (A, B, C, D), w-bit round keys S [0, …,(2r+3)], and r is number of rounds.
Output: Plaintext stored in (A, B, C, D).

$C = C - S[2r + 3]$
$A = A - S[2r + 2]$
$for i = r downto\ 1\ do$
{
(A, B, C, D) = (D, A, B, C)
u = D * (2D + 1) <<< log(w)
t = B * (2B + 1) <<< log(w)
$C = ((C - S[2i + 1]$ >>> t) $\oplus u$
$A = ((A - S[2i]$ >>> u) $\oplus t$
}
$D = D - S[1]$
$B = B - S[0]$

Figure 4.4: RC6 Decryption Algorithm

and no unnecessary feed is being detected. The video used for this test was 5 seconds. The total number of frames will be 150 (5 * 30 frame rate). The video encryption and decryption later on is observed on the video which was received after implementing sensors. Here is the pictorial representation after implementing RC6 Encryption/ Decryption Algorithm in MATLAB.

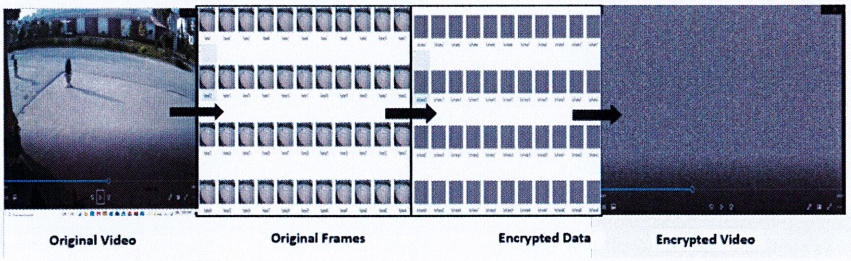


Figure 4.5: Proposed Video Encryption Process

The given Figure 4.5 represents complete RC6 encryption process based on implementation on MATLAB. The video utilized here was 5 seconds video , which resulted in 150 frames based on frame rate which was 30 frames per second. These original frames are converted to encrypted data and then encrypted video.

The figure 4.6 represents a complete RC6 decryption process which is based on decryption strategy and implemented. It depicts that encrypted video is then transferred to encrypted data and then to original frames which

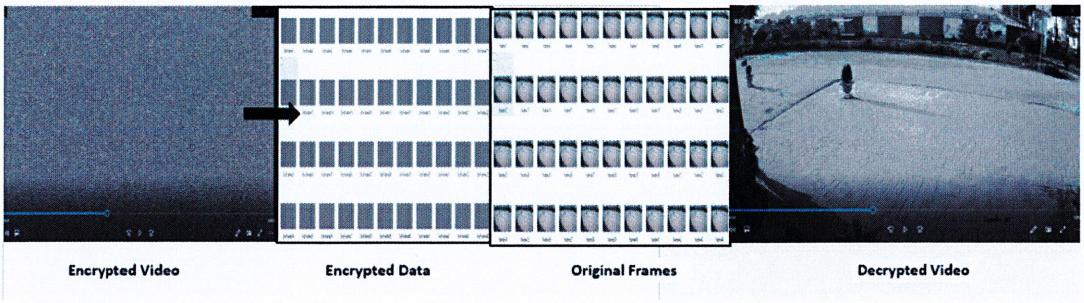


Figure 4.6: Proposed Video Decryption Process

ultimately return back to original video, which is a decrypted video.

The above mentioned scenario is a complete representation of a video encryption/ decryption based on real life data of a university campus. So, by keeping the PLS under consideration, this process will be followed for a complete message security based on RC6 encryption / Decryption technique and on a framework mentioned in figure 3.7

4.4 Limitations of Proposed Model

There can be few limitations given below:

1. The acquired data from the environment can be different at different places according to the situation, for example: if it is used for hospitals, as hospitals are most rushy places and motion detection is more so this methodology is not effective in those extreme rushy places, this research study needs more explanation on detection of particular motion that which specific motion needs to be detected.
2. Due to limitation of time, only focus of this study was on traffic minimization using sensors with ZKP, however after applying RC6 encryption, the generated data which is received afterwards, the focus was not on the volume of generated data, so further study should be done on how to reduce encrypted data using RC6.

4.5 Discussion

Nowadays, most concerned and challenging requirement in cryptography is to deliver accurate and fast results in a very less amount of time with minimum resources. Video encryption has been used since long time but the applications to implement this technique varies and that thing plays a vital role while talking about performance. Based on the privacy, integrity and confidentiality of data, The current research study is focused on implementation of RC6 on MATLAB which successfully presented the video encryption / decryption. The proposed strategy is implemented using RC6 which is lightweight and takes less time than heavy weight algorithms.

The length of a secret key can affect The RC6 Block Cipher. By running the RC6 code Using different key's size, results conclude that performance of RC6 is inversely proportional to key size, if key size will increase the performance will decrease and vice-versa (Paje, Sison, & Medina, 2018).

Of course there exist many more applications involving visual data requiring some sort of encryption support, to investigate the different requirements on privacy and confidentiality support and the desired properties of the corresponding cryptographic systems. Based on several investigations and research, RC6 has been established to be the most recent Advanced Encryption scheme in terms of security, convenience, compliance, and effectiveness. However, when it comes to the RC6 simulation technique, the methodology must've been faster than it is currently, as it will enhance the design's functionality while also increasing efficiency. The suggested symmetric encryption could be utilized to increase already completed work, leading to more efficient and secure solutions.

4.6 Comparison of RC6 with other Algorithms

The percentage of CPU use for each encryption algorithm is calculated.The time it takes to encrypt data is regarded as a significant parameter for determining how effective an encryption technique is.The throughput would be calculated using the following formula (Aggarwal, Saini, & Verma, 2013)

$$Throughput = c/t \tag{4.1}$$

where c denotes the encrypted plain text in bytes and t denotes the encryption time. To ensure consistency in the contrast, all encryption methods' input variables are specified. An average of ten repetitions for every algorithm's results to keep the results as efficient as possible. In order to select an effective encryption method, various variables must be considered, including speed, throughput, complexity, CPU use, security level, and so on.Simulations have proved different factors including key generation time in milliseconds, average encryption time in milliseconds, Average Decryption time (millisec), Throughput (MB/Sec) of encryption of different algorithms and Throughput of Decryption of Different Algorithms in MB/sec. Simulation results described by different research studies (Alenezi, Alabdulrazzaq, & Mohammad, 2020), (Aggarwal et al., 2013) have shown different behaviours regarrding different factors under observation at different times like throughput, encryption time, decryption time.

From the figure 4.7, it is obvious that minimum time is required for key generation for RC6 algorithm as compared to other algorithms. If minimum time is required for key generation , the encryption and decryption will fast. If encryption/ decryption is slow or key generation process is slow, it will affect the efficiency of algorithm. SO, if minimum time is required for key generation, the more fast the algorithm is.

The figure 4.8 represents Average Encryption Time. Average Encryp-

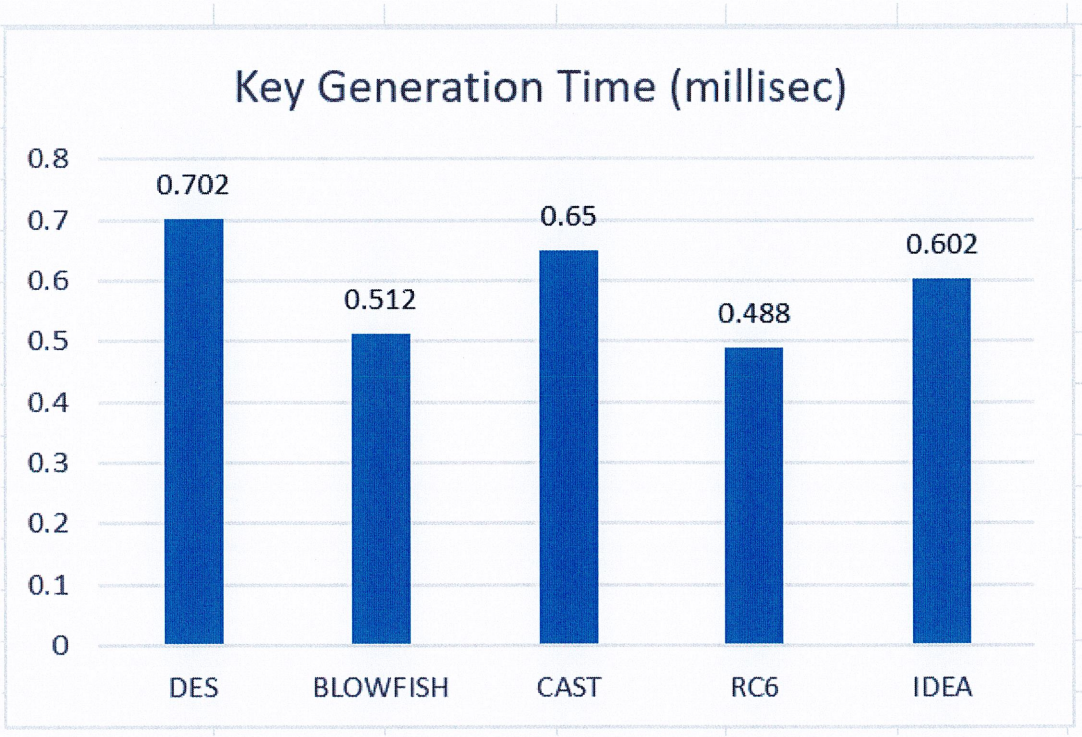


Figure 4.7: Key Generation time of different algorithms

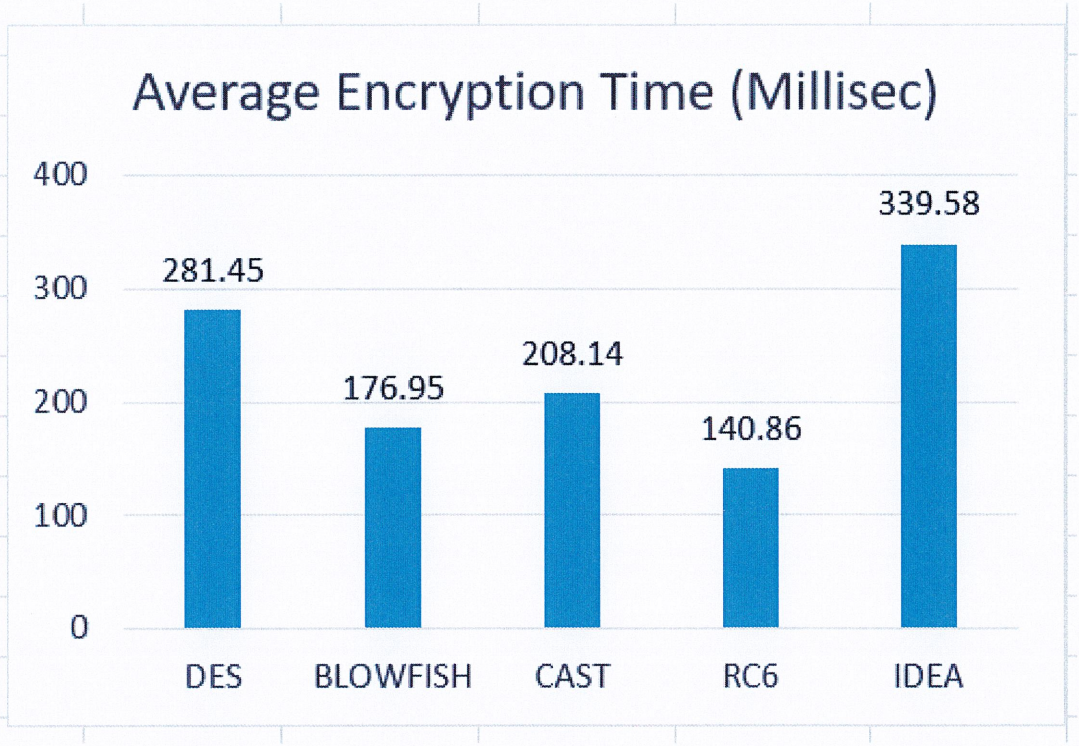


Figure 4.8: Encryption Time versus Different Algorithms of Encryption

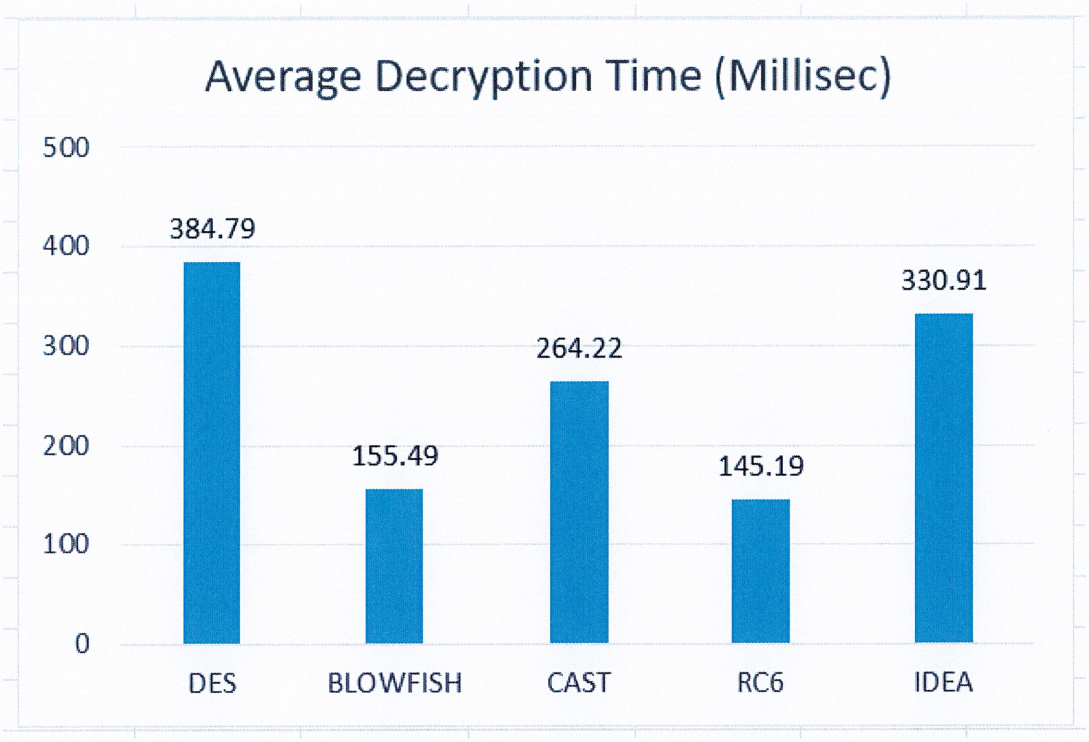


Figure 4.9: Decryption Time versus Different Algorithms of Dcryption

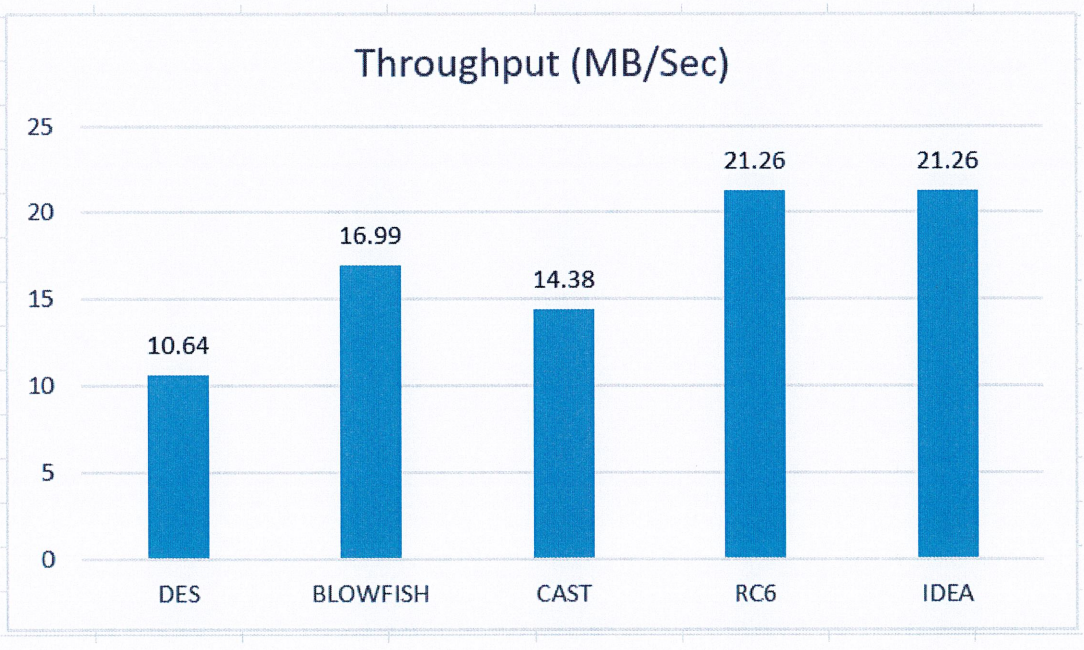


Figure 4.10: Plot between Throughput and Different Algorithms of Encryption

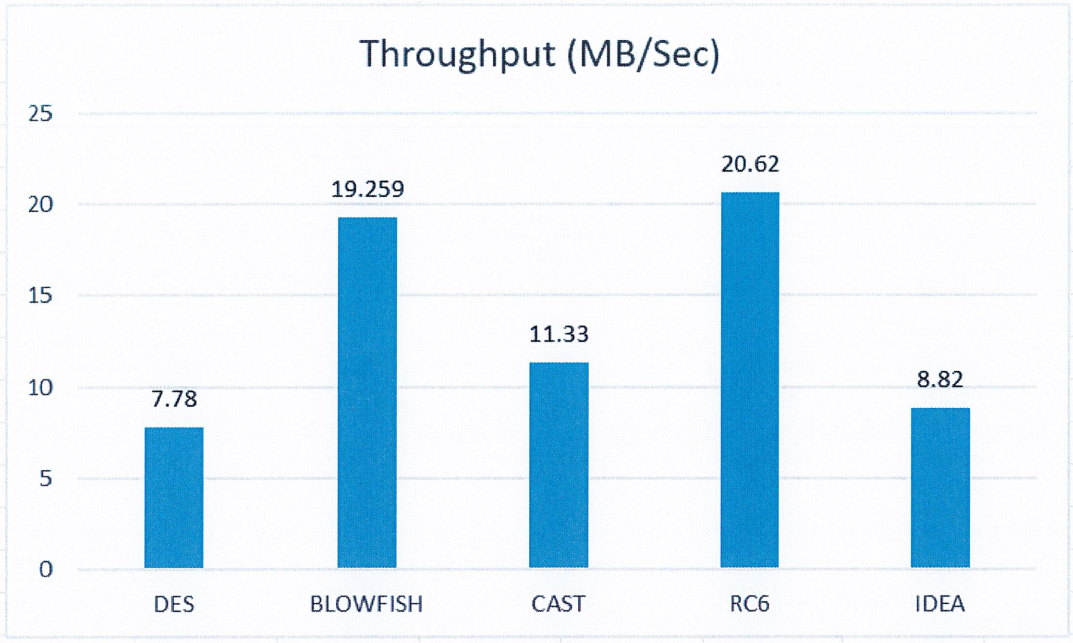


Figure 4.11: Plot between Throughput and Different Algorithms of Decryption

tion Time is not only one document's encryption time, and encryption time of each document vary from other, moreover; as we have done the encryption based on frames so the average encryption time of RC6 is minimum as compared to other algorithms.

Similarly, the average decryption time matters also in the same way as average encryption time. The Average Decryption Time discussed in figure 4.9 also depicts that as the document received at receiver's end, the receiver has to use it after decrypting it, if the decryption time is more or double than the transfer time or travelling time in the channel, the efficiency is reduced in this case and trust is lost. The less the decryption time, the more the algorithm is efficient and will definitely gain more trust. So, the figure 4.9 shows that the average decryption time is minimum as compared to other algorithms which obviously increase its efficiency and trust.

From the figures 4.10, 4.11 represents throughput of encryption of different and throughput of decryption of different algorithms represents

that RC6 has maximum throughput at encryption time and decryption time. As RC6 has maximum throughput, it clearly indicated that execution time of RC6 would be faster comparatively based on throughput.

4.7 Summary

The choice of RC6 for video encryption based on real life data proved to be an accurate approach which resulted in highly efficient results in form of encrypted video and decryption of the data to return original video.

Chapter 5
Conclusion and Recommendations

5.1 Overview

5.2 Conclusion

5.3 Recommendations and Future Work

Chapter 5

Conclusion and Recommendations

5.1 Overview

The research idea is resulted and conducted experiments and summarise our findings in this chapter. The research idea is resulted and conducted experiments and summarise our findings in this chapter.

5.2 Conclusion

The Internet of Things goal has evolved over the last few years from a conceptual framework to a main objective across various businesses. Organizations are seeking for new methods to use and manage and handle the data collected when they deploy IoT equipment into respective networked architectures.

The Internet of Things goal has evolved over the last few years from a conceptual framework to a main objective across various businesses. Organizations are seeking for new methods to use and manage and handle the data collected when they deploy IoT equipment into respective networked architectures.

The physical layer is vulnerable to a variety of threats, including malevolent insiders, malfunction or sabotage, degradation, overburden, natural

disasters, and so on. Even the most seemingly trivial component, such as a connector, can bring an entire system down if it is compromised or attacked. At the same time, the physical layer might serve as final line of defense. One could be the victim of a denial of service attack. In this instance, the only way to save the network is to provide measures to keep the physical layer secure.

We need to keep the data away from unauthorized user so that no one can access the data without having key. To keep the data secure and away from an authorized user, encryption is the necessary tool to be implemented. But the main question is, the way to provide an encryption technique through a way which is more secure, effective and fast among others. At investigative stage, Study Qualitative previous methods of data minimization, authentication, and encryption in IoT for finding related technique and solutions. The significance of the research focus on the security of the data in the terms that the encrypted code cannot be exploited by the third person. The security of the data should be accurate and privacy of the data should not be affected.

The choice of RC6 for video encryption based on real life data proved to be an accurate approach which resulted in highly efficient results in form of encrypted video and decryption of the data to return original video. This was done by implementing sensors in a university campus on the basis of algorithm figure 3.5. It was helpful in collecting real life data and ZKP was implemented on sensors to avoid any unnecessary feed in the data. Moreover, to keep the PLS under consideration , RC6 Encryption/Decryption technique is implemented with a complete encryption/ decryption based on real life data, which shows this research work's uniqueness from other research ideas.

Moreover, based on different studies, comparison of RC6 is discussed on the basis of throughput, encryption time and decryption time. This comparison based on simulation results depicts that RC6 is faster in through-

put comparatively with other algorithms. Different fields require encryption support like telemedicine (provide and protect the confidentiality of patient related medical image data when stored in databases and transmitted over networks of any kind), video conferencing (VC) has been around to serve such purposes for quite a while and is conducted on personal computers over computer networks, video telephony is a technology that has been emerging quite recently in the area of mobile cell phone technology.

5.3 Recommendations and Future Work

As the proposed strategy focused on placing sensors at different places for sensing and capturing the movement of an object for IoT data compression,So, by concluding, this technique seems to be an efficient and secure for handling IoT data at physical layer. It should be more refined to work in Defense Domain for data compression and sensing the movement of an object in order to keep our borders safe. Highly advanced and refined techniques will be more appreciated for IoT data Compression with reduction in storage hardware, communication bandwidth and transmission time, that will ultimately result in cost savings. The technique is needed to be faster than currently, as it will increase the performance of the design and saves the time as well. The proposed encryption technique can be focused more to extend the done work in order to get more efficient and secure results regarding real life data.

References

Abed, S., AlKandari, M., AlRasheedi, H., & Ahmad, I. (2020). Fpga implementation of enhanced jpeg algorithm for colored images. *International Journal of Computing and Digital Systems, 20*(1).

Achary, R. (2021). Internet of things (iot) security threats on physical layer security. In *Data science and security* (pp. 39–48). Springer.

Adhie, R. P., Hutama, Y., Ahmar, A. S., Setiawan, M., et al. (2018). Implementation cryptography data encryption standard (des) and triple data encryption standard (3des) method in communication system based near field communication (nfc). In *Journal of physics: Conference series* (Vol. 954, p. 012009).

Aggarwal, K., Saini, J. K., & Verma, H. K. (2013). Performance evaluation of rc6, blowfish, des, idea, cast-128 block ciphers. *International Journal of Computer Applications, 68*(25).

Ahanger, T. A. (2018). Defense scheme to protect iot from cyber attacks using ai principles. *International Journal of Computers Communications & Control, 13*(6), 915–926.

Akyildiz, I. F., Su, W., Sankarasubramaniam, Y., & Cayirci, E. (2002). Wireless sensor networks: a survey. *Computer networks, 38*(4), 393–422.

Al-Aswad, H., El-Medany, W. M., Balakrishna, C., Ababneh, N., & Curran, K. (2021). Bzkp: Blockchain-based zero-knowledge proof model for enhancing healthcare security in bahrain iot smart cities and covid-19

risk mitigation. *Arab Journal of Basic and Applied Sciences*, *28*(1), 154–171.

Alenezi, M. N., Alabdulrazzaq, H., & Mohammad, N. Q. (2020). Symmetric encryption algorithms: Review and evaluation study. *International Journal of Communication Networks and Information Security*, *12*(2), 256–272.

Ali, S. T., Sivaraman, V., & Ostry, D. (2013). Eliminating reconciliation cost in secret key generation for body-worn health monitoring devices. *IEEE Transactions on Mobile Computing*, *13*(12), 2763–2776.

Alsaffar, N., Elmedany, W., & Ali, H. (2019). Application of rc5 for iot devices in smart transportation system. In *2019 8th international conference on modeling simulation and applied optimization (icmsao)* (p. 1-4). doi: 10.1109/ICMSAO.2019.8880351

Anderson, R. (2020). *Security engineering: a guide to building dependable distributed systems*. John Wiley & Sons.

Balaji, S., Nathani, K., & Santhakumar, R. (2019). Iot technology, applications and challenges: a contemporary survey. *Wireless personal communications*, *108*(1), 363–388.

Bansal, M., Nanda, M., & Husain, M. N. (2021). Security and privacy aspects for internet of things (iot). In *2021 6th international conference on inventive computation technologies (icict)* (pp. 199–204).

Bashir, A., & Mir, A. H. (2018). Internet of things security issues, threats, attacks and counter measures. *International Journal of Computing and Digital Systems*, *7*(02), 111–120.

Bellandi, V., Ceravolo, P., Cristiano, A., Damiani, E., Sanna, A., & Trojaniello, D. (2021). A design methodology for matching smart health requirements. *Concurrency and Computation: Practice and Experience*, *33*(22), e6062.

Bennett, C. H., & Brassard, G. (2020a). Quantum cryptography: Public key

distribution and coin tossing. *arXiv preprint arXiv:2003.06557*.

Bennett, C. H., & Brassard, G. (2020b). Quantum cryptography: Public key distribution and coin tossing. *arXiv preprint arXiv:2003.06557*.

Cheng, L., Guo, S., Wang, Y., & Yang, Y. (2016). Lifting wavelet compression based data aggregation in big data wireless sensor networks. In *2016 ieee 22nd international conference on parallel and distributed systems (icpads)* (pp. 561–568).

Christidis, K., & Devetsikiotis, M. (2016). Blockchains and smart contracts for the internet of things. *Ieee Access*, *4*, 2292–2303.

Dunkels, A., Gronvall, B., & Voigt, T. (2004). Contiki - a lightweight and flexible operating system for tiny networked sensors. In *29th annual ieee international conference on local computer networks* (p. 455-462). doi: 10.1109/LCN.2004.38

Elrawy, M. F., Awad, A. I., & Hamed, H. F. (2018). Intrusion detection systems for iot-based smart environments: a survey. *Journal of Cloud Computing*, *7*(1), 1–20.

Enugu, S. R. (2008). Fpga implementation of rc6 algorithm for ipsec protocol..

Evangelos A, K., Nikolaos D, T., & Anthony C, B. (2011). Integrating rfids and smart objects into a unifiedinternet of things architecture. *Advances in Internet of Things*, *2011*.

Evans, D. (2011). The internet of things: How the next evolution of the internet is changing everything. *CISCO white paper*, *1*(2011), 1–11.

Faisal, Z., & Ameer, E. H. A. (2020). Encryption image by using rc6 and hybrid chaotic map. *Webology*, *17*(2), 189–199.

Fang, C., Yao, H., Wang, Z., Wu, W., Jin, X., & Yu, F. R. (2018). A survey of mobile information-centric networking: Research issues and challenges. *IEEE Communications Surveys & Tutorials*, *20*(3), 2353–2371.

Faragallah, O. S., Afifi, A., El-Shafai, W., El-Sayed, H. S., Alzain, M. A., Al-Amri, J. F., & El-Samie, F. E. A. (2020a). Efficiently encrypting color images with few details based on rc6 and different operation modes for cybersecurity applications. *IEEE Access*, *8*, 103200-103218. doi: 10.1109/ACCESS.2020.2994583

Faragallah, O. S., Afifi, A., El-Shafai, W., El-Sayed, H. S., Alzain, M. A., Al-Amri, J. F., & Abd El-Samie, F. E. (2020b). Efficiently encrypting color images with few details based on rc6 and different operation modes for cybersecurity applications. *IEEE Access*, *8*, 103200–103218.

Gaeta, M., Loia, V., & Tomasiello, S. (2015). Multisignal 1-d compression by f-transform for wireless sensor networks applications. *Applied Soft Computing*, *30*, 329–340.

Geraldo Filho, P., Villas, L. A., Gonçalves, V. P., Pessin, G., Loureiro, A. A., & Ueyama, J. (2019). Energy-efficient smart home systems: Infrastructure and decision-making process. *Internet of Things*, *5*, 153–167.

Gokhale, P., Bhat, O., & Bhat, S. (2018). Introduction to iot. *International Advanced Research Journal in Science, Engineering and Technology*, *5*(1), 41–44.

Goldwasser, S., Micali, S., & Rackoff, C. (1989). The knowledge complexity of interactive proof systems. *SIAM Journal on computing*, *18*(1), 186–208.

Groth, J. (2010). Short pairing-based non-interactive zero-knowledge arguments. In *International conference on the theory and application of cryptology and information security* (pp. 321–340).

Huo, Y., Tian, Y., Ma, L., Cheng, X., & Jing, T. (2017). Jamming strategies for physical layer security. *IEEE Wireless Communications*, *25*(1), 148–153.

Hussain, A. M., Abualsaud, K., Yaacoub, E., Khattab, T., Gehani, A., &

Guizani, M. (2021). A testbed for implementing lightweight physical layer security in an iot-based health monitoring system. In *2021 international wireless communications and mobile computing (iwcmc)* (pp. 486–491).

Hussein, W., Abdullah, J., & Alduais, N. (2020). Data aggregation algorithms with multiple sensors in clustered-based wsn/iot. *International Journal of Computing and Digital Systems*, *9*(03).

Iqbal, A., Suryani, M. A., Saleem, R., & Suryani, M. A. (2016). Internet of things (iot): On-going security challenges and risks. *International Journal of Computer Science and Information Security*, *14*(11), 671.

Jing, Q., Vasilakos, A. V., & Wan, J. (2014). Jingwei, and dechao qiu,"security of the internet of things: Perspective and challenges,". *Wireless Networks (Springer Link)*, *20*(8), 2481–2501.

Kabulov, A., & Normatov, I. (2019). About problems of decoding and searching for the maximum upper zero of discrete monotone functions. In *Journal of physics: Conference series* (Vol. 1260, p. 102006).

Kabulov, A., Normatov, I., & Ashurov, A. (2019). Computational methods of minimization of multiple functions. In *Journal of physics: Conference series* (Vol. 1260, p. 102007).

Kabulov, A., Normatov, I., Boltaev, S., & Saymanov, I. (2020). Logic method of classification of objects with non-joining classes. *Advances in Mathematics: Scientific Journal*, *9*(10), 8635–8646.

Kabulov, A., Urunbaev, E., Normatov, I., & Ashurov, A. (2020). Synthesis methods of optimal discrete corrective functions. *Advances in Mathematics: Scientific Journal*, *9*(9), 6467–6482.

Kabulov, A., Urunbayev, E., & Ashurov, A. (2019). Logical method for constructing the optimal corrector of fuzzy heuristic algorithms. In *2019 international conference on information science and communications*

technologies (icisct) (pp. 1–4).

Kabulov, A., Yarashov, I., & Vasiyeva, D. (2021). Security threats and challenges in iot technologies. *Science and Education*, *2*(1).

Kim, D.-Y., Min, S. D., & Kim, S. (2019). A dpn (delegated proof of node) mechanism for secure data transmission in iot services. *CMC Comput. Mater. Cont*, *60*, 1–14.

Klus, L., Klus, R., Lohan, E. S., Granell, C., Talvitie, J., Valkama, M., & Nurmi, J. (2021). Direct lightweight temporal compression for wearable sensor data. *IEEE Sensors Letters*, *5*(2), 1–4.

Krishna, A., Le Pallec, M., Mateescu, R., Noirie, L., & Salaün, G. (2019). Iot composer: Composition and deployment of iot applications. In *2019 ieee/acm 41st international conference on software engineering: Companion proceedings (icse-companion)* (pp. 19–22).

Kshetri, N. (2017). The economics of the internet of things in the global south. *Third World Quarterly*, *38*(2), 311–339.

Kwon, D., Hodkiewicz, M. R., Fan, J., Shibutani, T., & Pecht, M. G. (2016). Iot-based prognostics and systems health management for industrial applications. *IEEE Access*, *4*, 3659–3670.

Letafati, M., Kuhestani, A., Ng, D. W. K., & Beshkani, M. R. A. (2020). Physical layer secrecy and transmission resiliency of device-to-device communications. In *Globecom 2020-2020 ieee global communications conference* (pp. 1–6).

Li, L., Liu, J., Cheng, L., Qiu, S., Wang, W., Zhang, X., & Zhang, Z. (2018). Creditcoin: A privacy-preserving blockchain-based incentive announcement network for communications of smart vehicles. *IEEE Transactions on Intelligent Transportation Systems*, *19*(7), 2204–2220.

Li, S., Da Xu, L., & Zhao, S. (2015). The internet of things: a survey. *Information Systems Frontiers*, *17*(2), 243–259.

Liu, J., Hu, Q., Sun, R., Du, X., & Guizani, M. (2020). A physical layer security scheme with compressed sensing in ofdm-based iot systems. *ICC 2020 - 2020 IEEE International Conference on Communications (ICC)*, 1-6.

Madakam, S., & Date, H. (2016). Security mechanisms for connectivity of smart devices in the internet of things. In *Connectivity frameworks for smart devices* (pp. 23–41). Springer.

Madrahimova, D., & Yarashov, I. (2020). Limited in solving problems of computational mathematics the use of elements. *Science and Education*, *1*(6).

Maiorescu, I., Bucur, M., Georgescu, B., Moise, D., Strat, V. A., & Zgură, I. D. (2020). Social media and iot wearables in developing marketing strategies. do smes differ from large enterprises? *Sustainability*, *12*(18), 7292.

Major, W., Buchanan, W. J., & Ahmad, J. (2020). An authentication protocol based on chaos and zero knowledge proof. *Nonlinear Dynamics*, *99*(4), 3065–3087.

Margelis, G., Fafoutis, X., Oikonomou, G., Piechocki, R., Tryfonas, T., & Thomas, P. (2017). Physical layer secret-key generation with discreet cosine transform for the internet of things. In *2017 ieee international conference on communications (icc)* (pp. 1–6).

Mohsin, F., & Elmedany, W. (2021). A secure internet of healthcare things for tackling covid-19. In *2021 international conference on innovation and intelligence for informatics, computing, and technologies (3ict)* (p. 98-104). doi: 10.1109/3ICT53449.2021.9581819

Morais, E., Koens, T., Van Wijk, C., & Koren, A. (2019). A survey on zero knowledge range proofs and applications. *SN Applied Sciences*, *1*(8), 1–17.

Nemati, H. R., & Yang, L. (2010). *Applied cryptography for cyber secu-*

rity and defense: Information encryption and cyphering: Information encryption and cyphering. IGI Global.

Oddershede, A. M., Macuada, C. J., Quezada, L. E., & Montt, C. A. (2020). Automation factors influencing the operation of iot in health institutions: A decision support methodology. *INTERNATIONAL JOURNAL OF COMPUTERS COMMUNICATIONS & CONTROL, 15*(4).

Pachghare, V. (2019). *Cryptography and information security*. PHI Learning Pvt. Ltd.

Paje, R. E. J., Sison, A. M., & Medina, R. P. (2018). 1024bit key fortification of rc6 for video encryption. In *Proceedings of the 4th international conference on industrial and business engineering* (pp. 250–255).

Paje, R. E. J., Sison, A. M., & Medina, R. P. (2019). Multidimensional key rc6 algorithm. In *Proceedings of the 3rd international conference on cryptography, security and privacy* (pp. 33–38).

Pang, Z. (2013). *Technologies and architectures of the internet-of-things (iot) for health and well-being* (Unpublished doctoral dissertation). KTH Royal Institute of Technology.

Parizi, R. M., Dehghantanha, A., et al. (2018). Smart contract programming languages on blockchains: An empirical evaluation of usability and security. In *International conference on blockchain* (pp. 75–91).

Pechetti, S. V., Jindal, A., & Bose, R. (2018). Exploiting mapping diversity for enhancing security at physical layer in the internet of things. *IEEE Internet of Things Journal, 6*(1), 532–544.

Pecorella, T., Brilli, L., & Mucchi, L. (2016a). The role of physical layer security in iot: A novel perspective. *Information, 7*(3), 49.

Pecorella, T., Brilli, L., & Mucchi, L. (2016b). The role of physical layer security in iot: A novel perspective. *Information, 7*(3), 49.

Porkodi, R., & Bhuvaneswari, V. (2014). The internet of things (iot) applications and communication enabling technology standards: An

overview. In *2014 international conference on intelligent computing applications* (pp. 324–329).

Quora. (2013, Jan). *How many things are currently connected to the "internet of things" (iot)?* Forbes Magazine. Retrieved from https://www.forbes.com/sites/quora/2013/01/07/how-many-things-are-currently-connected-to-the-internet-of-things-iot/

Raju, C. N., Umadevi, G., Srinathan, K., & Jawahar, C. (2008). Fast and secure real-time video encryption. In *2008 sixth indian conference on computer vision, graphics image processing* (p. 257-264). doi: 10.1109/ICVGIP.2008.100

Reyes-Campos, J., Alor-Hernández, G., Machorro-Cano, I., Olmedo-Aguirre, J. O., Sánchez-Cervantes, J. L., & Rodríguez-Mazahua, L. (2021). Discovery of resident behavior patterns using machine learning techniques and iot paradigm. *Mathematics*, *9*(3), 219.

Rivest, R. L., Robshaw, M. J., Sidney, R., & Yin, Y. L. (1998). The rc6tm block cipher. In *First advanced encryption standard (aes) conference* (p. 16).

Rodrigues, J. J., Segundo, D. B. D. R., Junqueira, H. A., Sabino, M. H., Prince, R. M., Al-Muhtadi, J., & De Albuquerque, V. H. C. (2018). Enabling technologies for the internet of health things. *Ieee Access*, *6*, 13129–13141.

Sadeeq, M. A., Zeebaree, S. R., Qashi, R., Ahmed, S. H., & Jacksi, K. (2018). Internet of things security: a survey. In *2018 international conference on advanced science and engineering (icoase)* (pp. 162–166).

Sagheer, A. M., Searan, S. M., & Salih, S. S. (2018). Developing rc4 algorithm using s-box of advanced encryption standard cipher. *International Journal of Computing and Digital Systems*, *07*, 207-214.

Sánchez, D. C. (2019). Zero-knowledge proof-of-identity: Sybil-resistant,

anonymous authentication on permissionless blockchains and incentive compatible, strictly dominant cryptocurrencies. *arXiv preprint arXiv:1905.09093*.

Sanchez, L., Muñoz, L., Galache, J. A., Sotres, P., Santana, J. R., Gutierrez, V., ... others (2014). Smartsantander: Iot experimentation over a smart city testbed. *Computer Networks*, *61*, 217–238.

Sicari, S., Rizzardi, A., Grieco, L., & Coen-PorisiniSecurity, A. (2014). privacy and trust in internet of things: the road ahead comput. *Networks*, *76*, 146–164.

Soni, A., Upadhyay, R., & Kumar, A. (2019). Wireless physical layer key generation with improved bit disagreement for the internet of things using moving window averaging. *Physical Communication*, *33*, 249–258.

Staudemeyer, R. C., Pöhls, H. C., & Watson, B. W. (2017). Security and privacy for the internet of things communication in the smartcity. In *Designing, developing, and facilitating smart cities* (pp. 109–137). Springer.

Šulyová, D., & Koman, G. (2020). The significance of iot technology in improving logistical processes and enhancing competitiveness: A case study on the world's and slovakia's wood-processing enterprises. *Sustainability*, *12*(18), 7804.

Sun, L., & Du, Q. (2018a). A review of physical layer security techniques for internet of things: Challenges and solutions. *Entropy*, *20*(10), 730.

Sun, L., & Du, Q. (2018b). A review of physical layer security techniques for internet of things: Challenges and solutions. *Entropy*, *20*(10), 730.

Sun, L., Ren, P., Du, Q., & Wang, Y. (2016). Fountain-coding aided strategy for secure cooperative transmission in industrial wireless sensor net-

works. *IEEE Transactions on Industrial Informatics*, *12*(1), 291-300. doi: 10.1109/TII.2015.2509442

Sun, L., & Xu, H. (2018). Fountain-coding-based secure communications exploiting outage prediction and limited feedback. *IEEE Transactions on Vehicular Technology*, *68*(1), 740–753.

Sundaravadivel, P., Kougianos, E., Mohanty, S. P., & Ganapathiraju, M. K. (2017). Everything you wanted to know about smart health care: Evaluating the different technologies and components of the internet of things for better health. *IEEE Consumer Electronics Magazine*, *7*(1), 18–28.

Swamy, S. N., Jadhav, D., & Kulkarni, N. (2017). Security threats in the application layer in iot applications. In *2017 international conference on i-smac (iot in social, mobile, analytics and cloud)(i-smac)* (pp. 477–480).

Tang, J., Xu, A., Jiang, Y., Zhang, Y., Wen, H., & Zhang, T. (2020). Secret key attaches in mimo iot communications by using self-injection artificial noise. In *2020 ieee international conference on artificial intelligence and information systems (icaiis)* (pp. 225–229).

Uriarte, R. B., & DeNicola, R. (2018). Blockchain-based decentralized cloud/fog solutions: Challenges, opportunities, and standards. *IEEE Communications Standards Magazine*, *2*(3), 22–28.

Valanarasu, M. R. (2019). Smart and secure iot and ai integration framework for hospital environment. *Journal of ISMAC*, *1*(03), 172–179.

Verma, H. K., & Singh, R. K. (2012). Performance analysis of rc6, twofish and rijndael block cipher algorithms. *International Journal of Computer Applications*, *42*(16), 1–7.

Vimal Jerald, A., Rabara, S., & Bai, T. (2015). Internet of things (iot) based smart environment integrating various business applications. *International Journal of Computer Applications*, *128*(8), 32–37.

Voulgaris, S., Fotiou, N., Siris, V. A., Polyzos, G. C., Jaatinen, M., & Oikonomidis, Y. (2019). Blockchain technology for intelligent environments. *Future Internet*, *11*(10), 213.

Wang, X., & Liu, F. (2020). Data-driven relay selection for physical-layer security: A decision tree approach. *IEEE Access*, *8*, 12105–12116.

Yan, Q., Zeng, H., Jiang, T., Li, M., Lou, W., & Hou, Y. T. (2016). Jamming resilient communication using mimo interference cancellation. *IEEE Transactions on Information Forensics and Security*, *11*(7), 1486–1499.

Yan, Z., Zhang, P., & Vasilakos, A. V. (2014). A survey on trust management for internet of things. *Journal of network and computer applications*, *42*, 120–134.

Yang, Y., Wu, L., Yin, G., Li, L., & Zhao, H. (2017). A survey on security and privacy issues in internet-of-things. *IEEE Internet of Things Journal*, *4*(5), 1250–1258.

Yao, J., Jing, Y., et al. (2018). Event-based anomaly detection for non-public industrial communication protocols in sdn-based control systems.

Ye T, P. Q., & ZH, R. (2012). Iot's perception layer, network layer and application layer security analysis.

Yim, J., Yoo, H.-K., Kwak, J.-y., & Kim, S.-M. (2018). Blockchain and consensus algorithm. *Electronics and telecommunications trends*, *33*(1), 45–56.

Yoo, H., Han, S., & Chung, K. (2020). A frequency pattern mining model based on deep neural network for real-time classification of heart conditions. In *Healthcare* (Vol. 8, p. 234).

Yu, K., Arifuzzaman, M., Wen, Z., Zhang, D., & Sato, T. (2015). A key management scheme for secure communications of information centric advanced metering infrastructure in smart grid. *IEEE transactions on instrumentation and measurement*, *64*(8), 2072–2085.

Yu, R., Yang, W., & Wang, S. (2020). Performance evaluation of lossy quality compression algorithms for rna-seq data. *BMC bioinformatics*, *21*(1), 1–15.

Yu, X.-Y., & Guo, X.-H. (2020). Data anomaly detection and data fusion based on incremental principal component analysis in fog computing. *KSII Transactions on Internet and Information Systems (TIIS)*, *14*(10), 3989–4006.

Zanella, A., Bui, N., Castellani, A., Vangelista, L., & Zorzi, M. (2014). Internet of things for smart cities. *IEEE Internet of Things journal*, *1*(1), 22–32.

Zhao, K., & Ge, L. (2013). A survey on the internet of things security. In *2013 ninth international conference on computational intelligence and security* (pp. 663–667).

Zulkipli, N. H. N., & Wills, G. B. (2017). An event-based access control for iot. In *Proceedings of the second international conference on internet of things, data and cloud computing* (pp. 1–4).

ملخص الدراسة

حاليًا ، يتمثل التحدي الرئيسي في أجهزة إنترنت الأشياء في تقليل حجم البيانات وتوفير البيانات المصادقة وتشفير البيانات. من خلال وضع هذا الرأي في الاعتبار ، فإن البحث الحالي يركز الفكرة على تقليل توليد البيانات باستخدام منهجية قائمة على الحدث. كحدث تقنية مستخدمة لتوليد البيانات وتقليلها بحيث يتم تصغير البيانات في بداية المرحلة باستخدام مستشعر كشف الحركة. لغرض المصادقة ، أشهر هاسيتم استخدام تقنية إثبات المعرفة الصفرية. أجهزة إنترنت الأشياء بها الكثير من مشكلات الأمان مثل إمكانية الوصول غير الموثوق بها ، والوصول غير المصرح به ، وفشل التشفير. للتغلب على مشاكل أمن إنترنت الأشياء، يتم معالجة تشفير البيانات ؛ استنادًا إلى تقنية التشفير RC6 (Rivest cipher 6).

اقترحت هذه الدراسة البحثية دراسات حالات مختلفة تتعلق بمجالات الحياة اليومية مثل المتعلقة بالحرم الجامعي من خلال تطبيق اجهزة الاستشعار في أماكن مختلفة من الجامعة ،سيتم تنفيذ ذلك باستخدام طريقة إدخال الأحداث ، والتي تكون فيها الأجهزة فقط يتم تنشيطها لتسجيل البيانات عند وقوع حدث ما. للتعامل مع القضايا الأمنية ، إثبات المعرفة الصفري هو منهجية يمكن من خلالها لمستخدم أن يثبت للآخر أن البيانات صالحة دون تقديم أي معلومات إضافية حول البيانات. بمساعدة RC6 في MATLAB ، لن يتمكن المستخدمون غير المصرح لهم من فك تشفير البيانات. علاوة على ذلك ، يتم فحص فكرة البحث المقترحة في بيئة محاكاة للتقييم. تمت مقارنة الطريقة المقترحة مع طرق آخرى في الادبيات بناءً على معدل النقل ووقت إنشاء المفتاح ومتوسط وقت التشفير وفك التفشير مما أظهر أن الطريقة المقترحة تفوق الطرق الأخرى.

University of Bahrain
Deanship of scientific Research

جامعة البحرين
عمادة البحث العلمي

(استمارة ايداع البحث)

اسم الباحث: عافية مراد أشرف

عنوان البحث: اطار عمل آمن لتقليل حركة بيانات انترنت الاشياء باستخدام إثبات المعرفة الصفري وتشفيرRC6

سنة النشر: 2022م

الكلية: تقنية المعلومات

البريد الالكتروني: 202000120@stu.uob.edu.bh

القسم: نظم المعلومات

رقم الاتصال:35387762

إقرار الباحث بالموافقة على الشروط التالية :

بحق لجامعة البحرين إتاحة وتوفير الرسالة أو الأطروحة المذكورة أعلاه في مكتبة الجامعة أو من خلال موقع الحاوية العلمية للجامعة أو على نطاق أوسع في الخارج ، كما ويمكن اعادة طباعة الرسالة اذا اقتضت الحاجة لذلك او رقمنتها مع اتاحتها على شبكة الانترنت وذلك حسب تقدير ادارة الجامعة

تنطبق هذه الشروط على جميع النسخ بما في ذلك النسخ الإلكترونية

تعتبر هذه الرسالة أو الأطروحة من المواد المحمية والتي تخضع إلى حقوق النشر والتأليف، ولا يجوز نشر أي اقتباس من الرسالة بدون توثيق المصدر

توقيع الباحث: _____ التاريخ: 04/08/2022

جامعة البحرين

كلية تقنية المعلومات



إطار عمل آمن لتقليل حركة بيانات إنترنت الأشياء باستخدام إثبات المعرفة الصفرية وتشفير RC6

اطروحة مقدمة كجزء من متطلبات الحصول على
درجة الة الماجستير في الأمن الإلكتروني

أعداد
عافية مراد أشرف
٢٠٢٠٠٠١٢٠

إشراف
د. وائل محمد المدني

(أستاذ مشارك)

جامعة البحرين

مملكة البحرين
يوليو ٢٠٢٢