

Design of Lightweight schemes to ensure security of the Internet of Things

A Thesis Submitted to the
Delhi Technological University
For the Award of Doctor of Philosophy
In
Computer Science and Engineering

Submitted By:
IRFAN ALAM
(2K19/PhDCO/04)



Under the Supervision of
Dr. Manoj Kumar
Professor

**DEPARTMENT OF COMPUTER SCIENCE AND
ENGINEERING**

DELHI TECHNOLOGICAL UNIVERSITY

(Formerly Delhi College of Engineering)

DELHI-110042, INDIA

2024

CERTIFICATE

This is to certify that the thesis entitled “**Design of Lightweight schemes to ensure security of the Internet of Things**” being submitted by Mr. Irfan Alam for the award of degree of Doctor of Philosophy to the Delhi Technological University is based on the original research work carried out by him. He has worked under my supervision and has fulfilled the requirements that to our knowledge have reached the requisite standard for the submission of this thesis. It is further certified that the work embodied in this thesis has neither partially nor fully submitted to any other university or institution for the award of any degree or diploma.

(Prof. Manoj Kumar)

Supervisor

Department of Computer Science and Engineering

Delhi Technological University

Delhi, India

DECLARATION

I, IRFAN ALAM, Department of Computer Science and Engineering, Delhi Technological University, certify that the work embodied in this Ph.D. thesis is my own bonafide work carried out by me under the supervision of Prof. Manoj Kumar at Delhi Technological University. The matter embodied in this Ph.D. thesis has not been submitted for the award of any other degree. I declare that I have faithfully acknowledged, given credit to, and referred to the researchers wherever their works have been cited in the text and the body of the thesis. I further certify that I have not willfully lifted up some other person's work (para, text, data, result, etc. reported in journals, books, magazines, reports, dissertations, thesis, etc. and included them in this Ph.D. thesis and cited them as my own work.

Place: Delhi

(Irfan Alam)

Date:

ACKNOWLEDGEMENT

I am profoundly thankful to the Almighty for His guidance and unwavering blessings during my doctoral journey. Through His benevolence, I received timely assistance from the right individuals, who played a crucial role in my success.

First and foremost, I am profoundly grateful to Professor Manoj Kumar, my mentor and supervisor, whose unwavering support throughout my Ph.D. study and research has left me deeply indebted. I express my sincere appreciation for his patience, motivation, and vast knowledge. His guidance, both in formal and informal discussions, as well as his constructive criticism, has constantly pushed me to enhance and refine my research efforts at every stage of my doctoral journey.

I am also thankful to Prof. Vinod Kumar, the chairman of the Department of Computer Science and Engineering, for providing me with all the necessary facilities. I can never forget the motherly treatment I received from Prof. Rajni Jindal, the DRC chairperson.

I extend my sincere appreciation to Mr. Saquib Mohtashim, Dr. Mohammad Misbahuddin, Associate Director CDAC, Bangalore, Dr. Abdul Basit, Dr. Zeeshan Ansari, Dr. Izharuddin, Dr. Tufail, Dr. Muzakkir, Dr. Zubair Ashraf, Dr. Tauseef, and Dr. Hamza for their unwavering presence as guiding figures throughout my Ph.D. journey. Their valuable scientific insights, personal assistance, and friendly demeanor have consistently provided me with a sense of comfort and ease. I have always been able to rely on their support whenever I needed it the most, and their guiding hands have been a constant source of strength.

I extend my sincere and heartfelt gratitude to all my colleagues and Professional-Sathi, especially Mr. Nadeem Ahmad, Mr. Mansha, Mr. Sharique, and Mr. Azeem, for their eternal and moral support, and counseling me to undertake proper steps when and wherever necessary. I greatly appreciate the help of and thank Dr. Mohammad Bilal for the invaluable time that he helped me in numerous ways during all the stages.

The personalities who inspired and influenced me to pursue research for the welfare of humanity are (Late) Prof. Nadir Ali Khan, Prof. Sanaullah Khan, and Dr. Sagheeruddin. Their expertise, guidance, and dedication have been instrumental in shaping my research and academic journey. I owe a debt of gratitude to each of them for their significant contributions to my work and for being a constant source of inspiration throughout the thesis process. Their legacy and effect on my academic pursuits will forever be cherished.

I am profoundly grateful to my family, and words cannot adequately convey my appreciation. Both my mother and father have made countless sacrifices on my behalf, and their prayers have been the source of my strength thus far. I also want to express my sincere gratitude to my respected Bhaijaan, Mr. Rizwan Alam, for his unwavering patience and

endless moral support throughout this journey. Your support in every aspect of my life has been invaluable, and your encouragement has been a constant driving force. To my beloved Wife, I extend my heartfelt thanks for being an exceptional partner and always keeping me stress-free. I am deeply obliged to my brothers, sisters, and all family members for their selfless support, and I cherish the bonds we share. Last but certainly not least, I wholeheartedly dedicate this work to an endless list of awesome individuals, including but not limited to: Mr. Farman, Dr. Pawan Sing Mehra, Mr. Imran, Mr. Vijendra, Mr. Rajat, and countless others. Their invaluable feedback and blessings have served as a constant source of inspiration throughout the completion of this work.

“O Almighty, there is no ease except what You make easy, and You make the difficult easy if You wish”

ABSTRACT

The Internet of Things (IoT) is one of the core and essence of the infrastructure of the modern world. Almost all facets of human endeavor now have applications for the IoT, making it one of the most revolutionary technological advancements. IoT provides seamless communication and data exchange by linking common objects and gadgets to the internet, resulting in unmatched efficiency, convenience, and innovation. IoT promotes a more connected, intelligent, and sustainable society through smart homes that allow automated management over appliances and energy use and intelligent healthcare systems that monitor patients remotely. IoT also facilitates predictive maintenance in industrial environments and increases efficiency by optimizing processes. Accepting the immense potential of IoT not only improves decision-making and streamlines operations, but it also paves the way for a time when technology enables us to live safer, healthier, and more connected lives.

IoT devices constantly generate, analyze, and exchange substantial volumes of security-critical and privacy-sensitive data, making them ideal targets for attacks and vulnerabilities. IoT security focuses on defending networks, devices, and data against potential threats and security flaws. A breach might have serious repercussions because there are numerous linked devices gathering and transmitting sensitive information. To strengthen IoT security, strong authentication, encryption, and regular software updates are essential. It is crucial to prioritize and invest in comprehensive security measures as the IoT ecosystem continues to grow.

In the case of the IoT, security measures vary from application to application. Authentication is mandatory for almost all applications related to the IoT infrastructure. It is a fundamental security measure that must be used by all IoT-based services to keep out intruders and illegal access. IoT authentication is important for ensuring that only authorized people and devices have access to networked systems. Strong authentication procedures, such as strong cryptographic algorithms and distinctive IDs, build confidence and stop unauthorized parties from altering or tampering with sensitive data. IoT networks can guard against potential intrusions, protect user privacy, and uphold the general integrity of the interconnected ecosystem by putting strong authentication methods in place. Therefore, we emphasized significant assaults and technical approaches against the IoT authentication system.

One of the primary challenges is choosing the optimised security protocol because of limitations such as dynamic resources and limited storage. Before being used in real-world applications, authentication systems must endure thorough crypt-analysis. We also covered current security verification methods and IoT authentication evaluation strategies. We have tried to prove that our proposed schemes are resilient to various numbers of attacks in

formal analysis sections of each chapter.

First, this thesis encompasses all the necessary stuff for understanding all about IoT systems, such as definition, basic architecture and its application, IoT security, the critical status of IoT security, and the importance of authentication in the introduction chapter. A literature review has been performed in an organized way on the basis of recent manuscripts from top-rated journals.

Second, this thesis proposes a novel scheme for efficient authentication in cloud based IoT devices. Third, this thesis proposes a novel authentication scheme for group-based authentication.

Fourth, this thesis proposes a novel authentication protocol to ensure confidentiality among the Internet of Medical Things (IoMT). Fifth, this thesis discusses the performance evaluation of the discussed protocols and schemes in a resource-constrained IoT network.

Finally, our work presents security concerns, unresolved issues, and prospective future IoT authentication applications in order to assist future researchers, along with a conclusion.

Contents

CERTIFICATE	I
DECLARATION	II
ACKNOWLEDGEMENTS	III
ABSTRACT	V
LIST OF FIGURES	IX
LIST OF TABLES	XI
KEY TO ABBREVIATIONS	XII
1 INTRODUCTION	1
1.1 Background	2
1.2 Motivations	7
1.3 Contributions	10
1.4 Outline of thesis	12
2 STATE OF THE ART: THE LITERATURE REVIEW	14
2.1 Need for literature review	15
2.2 Literature review	15
2.2.1 Review on details of authentication protocols for cloud based IoT devices	16
2.2.2 Review on group based authentication.	17
2.2.3 Review on authentication schemes for Medical Internet of Things to ensure confidentiality.	19
2.2.4 Review on performance evaluation	20
2.3 Knowledge gap analysis	21
2.4 Problem formulation	21
3 AUTHENTICATION SCHEME IN CLOUD BASED IoT DEVICES	23
3.1 Introduction	24
3.2 Preliminaries	26
3.2.1 Elliptic curve discrete logarithm problem (ECDLP)	26
3.2.2 One-way cryptographic hash function	26

3.2.3	System model	26
3.2.4	Adversary model	27
3.3	Proposed protocol	27
3.3.1	Pre-deployment phase	28
3.3.2	Registration of cloud server	28
3.3.3	User registration phase	29
3.3.4	Login phase	31
3.3.5	Authentication phase	31
3.4	Security Analysis	34
3.4.1	BAN logic (a formal approach of security analysis)	34
3.4.2	AVISPA: A simulator for authentication protocols	38
3.4.3	Informal analysis of attacks	40
3.5	Summary	44
4	A GROUP BASED SCHEME FOR IoT ORIENTED INFRASTRUCTURE	45
4.1	Introduction	46
4.2	Related works	48
4.3	Preliminaries	50
4.3.1	The (t, n) Threshold Scheme of Shamir	50
4.3.2	Group Based Authentication	52
4.3.3	One-way Cryptographic Hash Function	54
4.3.4	System Model	55
4.3.5	Adversary model	55
4.4	Proposed Scheme	57
4.4.1	Pre-deployment phase	57
4.4.2	Registration phase	58
4.4.3	Authentication phase	58
4.5	Security Analysis	60
4.5.1	Formal Analysis	60
4.5.2	Informal analysis	62
4.6	Summary	64
5	AUTHENTICATION SCHEME TO ENSURE CONFIDENTIALITY AMONG IoMT	66
5.1	Introduction	67
5.2	Related work	69
5.3	Preliminaries	70
5.3.1	Bilinear pairing	70
5.3.2	Timestamp	71
5.3.3	Hash function	72
5.4	Modular structure of the system	72
5.4.1	Network model	73
5.4.2	Adversary model	74

5.5	Proposed Scheme	75
5.5.1	Pre-deployment phase	76
5.5.2	User Registration	76
5.5.3	Doctor Registration	76
5.5.4	Authentication	77
5.5.5	Confidentiality	78
5.6	Security Analysis	79
5.6.1	Formal security analysis using BAN logic	79
5.6.2	Protocol validation and verification using SCYTHER	81
5.7	Summary	88
6	PERFORMANCE EVALUATION	89
6.1	Introduction	89
6.2	Preliminaries	90
6.2.1	Informal analysis	90
6.2.2	Formal analysis	93
6.3	Performance analysis	96
6.3.1	Performance evaluation of discussed schemes	97
6.3.2	Performance evaluation of Scheme of chapter-4	99
6.3.3	Comparison with existing schemes	100
6.3.4	Performance evaluation of Scheme of chapter-5	101
6.3.5	Performance Analysis	101
6.4	Summary	103
7	CONCLUSION AND FUTURE WORK	104
7.1	Conclusion	104
7.2	Limitations	105
7.3	Future Work	105
	LIST OF PUBLICATION	107
	BIBLIOGRAPHY	109
	ANNEXURE	127

List of Figures

1.1	IoT Device architecture	3
1.2	Service-Oriented Architecture	4
1.3	Importance of IoT security	8
3.1	Cloud-based IoT environment authentication model	27
3.2	Cloud-Server Registration	30
3.3	User Registration	30
3.4	Pre-verification of user	31
3.5	TA Authentication	32
3.6	TA Authentication	34
3.7	Constraint-Logic-based Attack Searcher (CL-AtSe)	40
3.8	On-the-fly Model-Checker (OFMC)	41
4.1	mart City and IoT World	48
4.2	Total time taken in secret sharing scheme	52
4.3	Informal authentication process.	53
4.4	Group-based membership authentication process.	54

4.5	Group-based membership authentication process.	56
4.6	Constraint-Logic-based Attack Searcher (CL-AtSe)	58
4.7	On-the-fly Model-Checker (OFMC)	59
5.1	General hospital setup and IoMT	68
5.2	Proposed Network Model	73
5.3	User Registration	75
5.4	Doctors Registration	77
5.5	Authentication in IoMT	78
5.6	Scyther results for authentication between User and Trusted Authority	82
5.7	Scyther results for authentication between Doctor and Trusted Authority	83
5.8	Scyther results for authentication between User and Doctor	84
6.1	Attacks on IoT Authentication	91
6.2	Performance Comparison of scheme of Chapter-III	99
6.3	Comparison of Schemes of Chapter-IV	101
6.4	Communication cost comparison of the proposed and conventional protocols (Scheme of Chapter-V)	103

List of Tables

1.1	Summary of IoT Applications core security Requirements	9
3.1	Notations of cloud based scheme	29
3.2	Attack resilient comparison with existing schemes	38
4.1	Notations used in Group Based Authentication (GBA)	57
4.2	Comparison of group authentication schemes in terms of attack resilient	61
5.1	Notations in scheme-III	74
5.2	Attack resilient comparison with existing schemes	87
6.1	Computational overhead with related schemes of chapter-III	98
6.2	Communication Overhead of scheme of Chapter - V	102

Key Abbreviations

IoT Internet of Things

SoA Service-oriented architecture

IIoT Industrial Internet of Things

GBA Group Based Authentication

GAS Group Authentication Scheme

IoMT Internet of Medical Things

PSSS Protected secret sharing scheme

AVISPA Automated Validation of Internet Security Protocols and Applications

PIA Privileged Insider Attacks

OPG Offline Password Guessing

UA User Anonymity

SSC Stolen Smart Card

PFS Perfect Forward Secrecy

ECC Elliptic curve cryptography

RSA Rivest-Shamir-Adleman

ITS Intelligent transportation system

WMSN Wireless Medical Sensor Networks

WBAN Wireless body area networks

ECDLP Elliptic Curve Discrete Logarithm Problem

VMs Virtual Machines

DoS Denial of Services

HLPSL High-Level Protocol Specification Language

mMTC Massive Machine-type Communication

SSS Secret Sharing Scheme

DLP Discrete logarithm problem

CDHP Computational Diffie - Hellman problem

BDHP Bilinear Diffie - Hellman problem

IBC Identity based Cryptography

PS Proposed scheme

OFMC On-the-fly Model-Checker

CL-AtSe Constraint-Logic-based Attack Searcher

SATMC SAT-based Model-Checker

TA4SP Tree Automata based on Automatic Approximations for the Analysis of Security Protocols

SPDL Security Protocol Descriptive Language

GUI Graphical User Interface

Chapter 1

INTRODUCTION

The IoT has emerged as one of the most revolutionary technological innovations, with the proliferation of applications within almost all fields of the human race. The Internet of Things is present everywhere, from industry to healthcare. Smart city infrastructures, telemedicine, and the industrial revolution are not possible without inclusion of IoT. At every stage of the product life cycle and value chain, the IoT also generates numerous new and possibly more deadly, security vulnerabilities that must be actively and consistently addressed. Imagine a remote attacker turning on your home's air conditioning in the dead of winter or forcing your coffee maker to overheat and catch fire. And if that weren't enough to destroy your day, in the middle of a busy intersection, your car suddenly accelerates and the steering wheel locks. Imagine waking up to a home that is already heated to a comfortable level and coffee that is prepared based on your actual wake-up time rather than a fixed schedule. You are reminded by your refrigerator to stop at the store on your way home to get milk and eggs. And when a problem is about to arise, your car automatically contacts the closest dealer to check on the availability of replacement components and sets up a drop-off time.

IoT devices are ideal targets for attacks and weaknesses because they continuously produce, analyze, and communicate large volumes of data that is privacy- and security-sensitive. There is a higher requirement for enhanced secrecy, integrity, availability of services, and automated process flow in critical infrastructure, physical security, transportation, telecommunications, government applications, surveillance, and networked alert techniques. Due to resource limitations including low-energy devices, low latency, and a lack of standards and interoperability, IoT device security is different from typical network security. Design strategies that, given these limitations, offer the highest level of security are required for hours. Such research and innovation will result in the safe and intelligent application of IoT in the present world.

1.1 Background

The Internet of Things (IoT) refers to the interconnected network of everyday objects and devices, ranging from household appliances and vehicles to industrial machinery and wearable technology. Through embedded sensors, these objects can collect and exchange data, enabling them to communicate and cooperate in ways that enhance efficiency, convenience, and automation. IoT has the potential to revolutionize industries and daily life by enabling smart systems that provide real-time insights, streamline processes, and improve decision-making. However, it also raises issues with data security, privacy, and the moral use of the enormous amounts of data produced by these connected devices.

Before moving further, we must be aware about the basic definition, importance and application of Internet of Things. This would lead reader towards the thorough study of present work. Here first we focus on some popular definitions of IoT followed by architecture of IoT systems based on device and services.

Defining the IoT

The global user community does not now have a single definition of Internet of Things IoT that is accepted. In reality, the phrase has been defined by a wide range of groups, including academicians, researchers, practitioners, innovators, developers, and business individuals, however its initial use has been credited to Kevin Ashton, a specialist in digital innovation [1] . The idea that the first version of the Internet was about data created by people, whereas the current version is about data created by objects, is something that all of the definitions share in common. The proper definition would be:

The IoT is defined the network of physical objects “things” that are embedded with sensors, software, and other technologies for the purpose of connecting and exchanging data with other devices and systems over the internet.

Or

“An open and comprehensive network of intelligent objects that have the capacity to auto-organize, share information, data and resources, reacting and acting in face of situations and changes in the environment”

Or

“The Internet of Things integrates everyday ‘things’ with the internet.”

Basic architecture of Internet of Things.

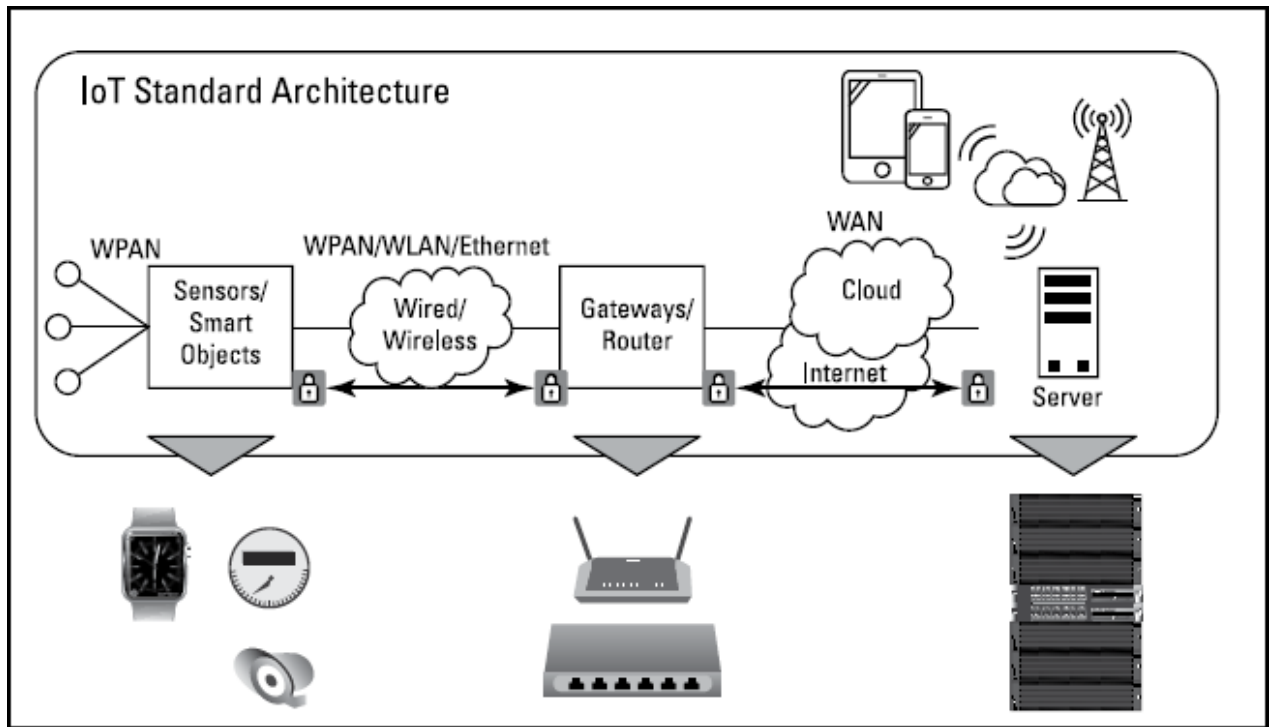


Figure 1.1: IoT Device architecture

IoT system architecture can be understood in two ways, one is of device - based architecture, and the other is service-oriented architecture. In device based architecture, we understand the hardware components and their interconnections, while in service-oriented architecture, we deal with how it provides services. The device based architecture consists of following components as shown in the figure 1.1.

- **Sensors/Smart Objects (Interface):** Theses devices observe the surroundings and collects the data.
- **Power Management Unit(PMU):** ON/OFF Switches to save power
- **Host processor:** The brain of the devices.
- **Memory:** It is highly desirable in IoT applications requiring storage of critical data and code.
- **Display:** For providing interface to users(Man-Machine interface).
- **Connectivity:** Communication link to connect to the other devices using WI-FI, Ethernet, and Bluetooth etc.

Service-oriented architecture (SoA):

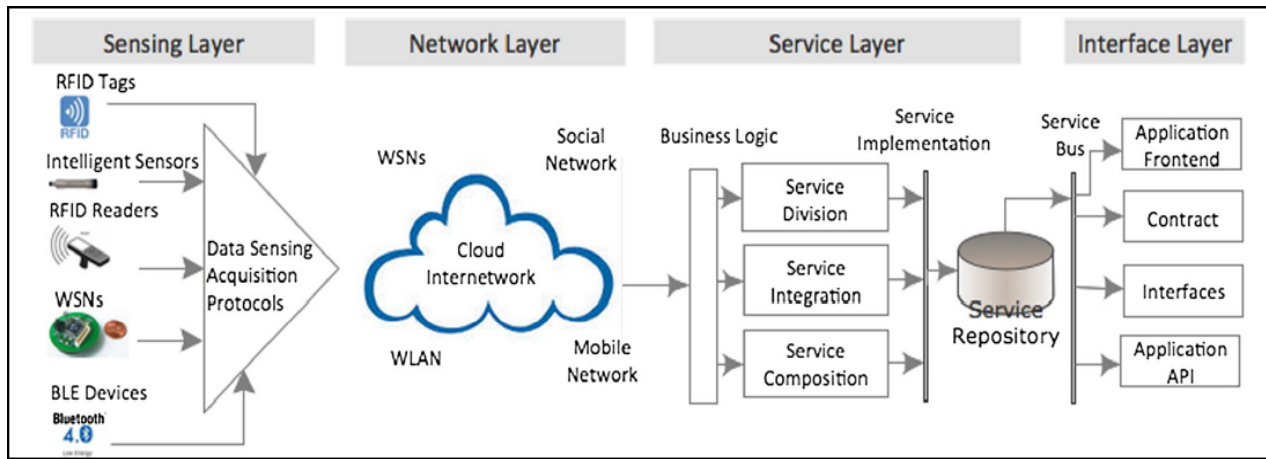


Figure 1.2: **Service-Oriented Architecture**

Service-oriented architecture (SoA) ensures that heterogeneous devices can communicate with other in multiple ways. A typical SoA is shown in Figure 1.2, which has four layers with their functionalities [2].

- **Sensing Layer:** The sensing layer is integrated with the hardware items currently in use to sense the status of things.
- **Network layer:** The infrastructure that supports wireless or wired communications, among other things, is called the network layer;
- **Service Layer:** Services needed by users or applications are created and managed at the service layer.
- **Interfaces Layer:** The user or application interaction techniques are included in the interfaces layer.

Application of IoT

Internet of Things are considered as one of the best invention of this century. Almost all walk of life is decorated with the connected things named as Internet of Things. Following are the some very famous area which are almost completely on the setup of internet of Things.

- **Smart Home and Office:** Smart offices and homes have undergone a revolution owing to the Internet of Things (IoT), which has increased their functionality and comfort. Smart thermostats, lighting controls, and security cameras are examples of Internet of Things (IoT) devices that give homeowners remote access to their environment, allowing them to save energy and increase security. Additionally, virtual assistants and

connected appliances allow for seamless automation and individualized experiences. Similar to this, IoT has improved workplace management in smart offices by automating processes like scheduling, climate control, and lighting, promoting a more comfortable and productive work environment for employees. Our interactions with our living and working places have changed as a result of the integration of IoT in both contexts, paving the way for a more connected and intelligent future. It includes Smart Door access control system, Smart lighting for home and office, Automated Gate and garage, Smart thermostats and humidity controllers.

- **Wearable Devices:** With Internet of Things, Wearable technology now has more uses than just reading texts, showing notifications from other apps, tracking location, keeping track of workout progress, setting reminders, and continuously monitoring health issues. Future wearable technology will be able to identify ailments early and initiate therapy when they are still treatable. Sensitive nano-sensors will be able to identify substances in our bodily fluids (sweat, tears, and saliva) and alert us to specific physical abnormalities that may later lead to more severe disease.
- **Healthcare:** The Internet of Things (IoT), which offers several advantages in patient care, monitoring, and data management, has completely transformed the healthcare sector. IoT in healthcare refers to a network of sensors and medical devices that continuously gather, transmit, and analyze patient data. These gadgets may include implantable gadgets, smart medical equipment, wearable health monitors, and tools for remote monitoring. Medical personnel can track chronic illnesses, monitor patients' vital parameters, and proactively spot potential health risks by incorporating IoT technologies into healthcare. A faster and more accurate diagnosis, individualized treatment strategies, and better patient outcomes are all made possible by real-time data. Additionally, IoT in healthcare improves efficiency and streamlines administrative work in healthcare facilities, thereby raising the overall standard of healthcare services. In addition to improving the effectiveness and cost-effectiveness of healthcare systems,

IoT increases patient pleasure. The use of IoT in healthcare will improve the whole hospital experience.

- **Autonomous Driving and Smart farming:** With the application of artificial intelligence and sophisticated sensor technology in the Internet of Things, autonomous driving has been developing. Drivers will receive assistance from earlier generations of autonomous vehicles (partial automation) to help them drive safely, avoid crashes, and issue warnings about the state of the road and the vehicle. To produce more foods and vegetables to feed the growing world population, agriculture and farming face several difficulties. The Internet of Things can help farmers and academics in this field discover more efficient and affordable ways to boost production.

- **Industrial Internet of Things (IIoT):** One of the first sectors to embrace the Internet of Things, which completely altered numerous stages of the product development cycle, was the manufacturing sectors.

Industrial IoT will advance several stages of product creation, including supply chain monitoring, inventory management, and product development optimization. Automate mass production procedures, enhance product quality, enhances packaging and management, uses data from a large number of sensor networks to optimize processes, and provides a cost-effective method for managing factories as a whole.

- **Disaster management:** Engineers may create a more effective emergency response system for industries, schools, hospitals, airports, and other public gathering places. Thanks to the Internet of Things and its extensive spectrum of smart sensors. Sensors will be used to automatically detect any emergency scenarios, such as a fire outbreak or floods, and this information will be immediately shared with the appropriate task groups.
- **Big Data Analytics:** Data is one of the fundamental elements of big data analytics, many businesses view data as their most important asset for expanding their business plans. Data sources include machines, the natural World, humans, plants, and even animals. The Internet of Things

uses many sensors to collect data from various applications. Big data analytics can use vast amounts of data from millions of smart sensors to enhance its machine learning and artificial intelligence based decision-making algorithm.

- **Smart Grids and energy management:** A “smart grid” aims to improve current electrical grids by installing sensors in each customer outlet and along transmission lines. These sensors allow us to detect any malfunctions or irregularities in the line and comprehend the nature of usage and changing activity patterns.
- **Logistic and fleet management:** Since the commodities must be handled with more outstanding care and effectiveness, smart logistics is a challenging endeavor. Service providers must ensure that items are transported in pristine condition in addition to moving them from one place to another.

1.2 Motivations

The motivation behind research in IoT security is to address the growing concerns and vulnerabilities associated with the rapid proliferation of interconnected devices. IoT devices encompass a wide range of objects, such as smart home appliances, industrial sensors, medical devices, and autonomous vehicles, which are all connected to the internet and each other. While IoT offers numerous benefits, it also introduces significant security risks. IoT security is of paramount importance due to the widespread adoption and integration of IoT devices in various aspects of our lives. IoT security plays a crucial role in safeguarding sensitive data, protecting against cyber threats, ensuring network integrity, promoting user trust, and complying with legal requirements. By addressing security challenges, we can unleash the full potential of IoT while minimizing risks and maximizing the benefits of this transformative technology.

Today, every connected firm faces a significant issue regarding data protection and privacy. The media frequently reports on the widespread theft of people’s financial and health records from institutions in the public and commercial sectors. However, threats from more sensitive and private

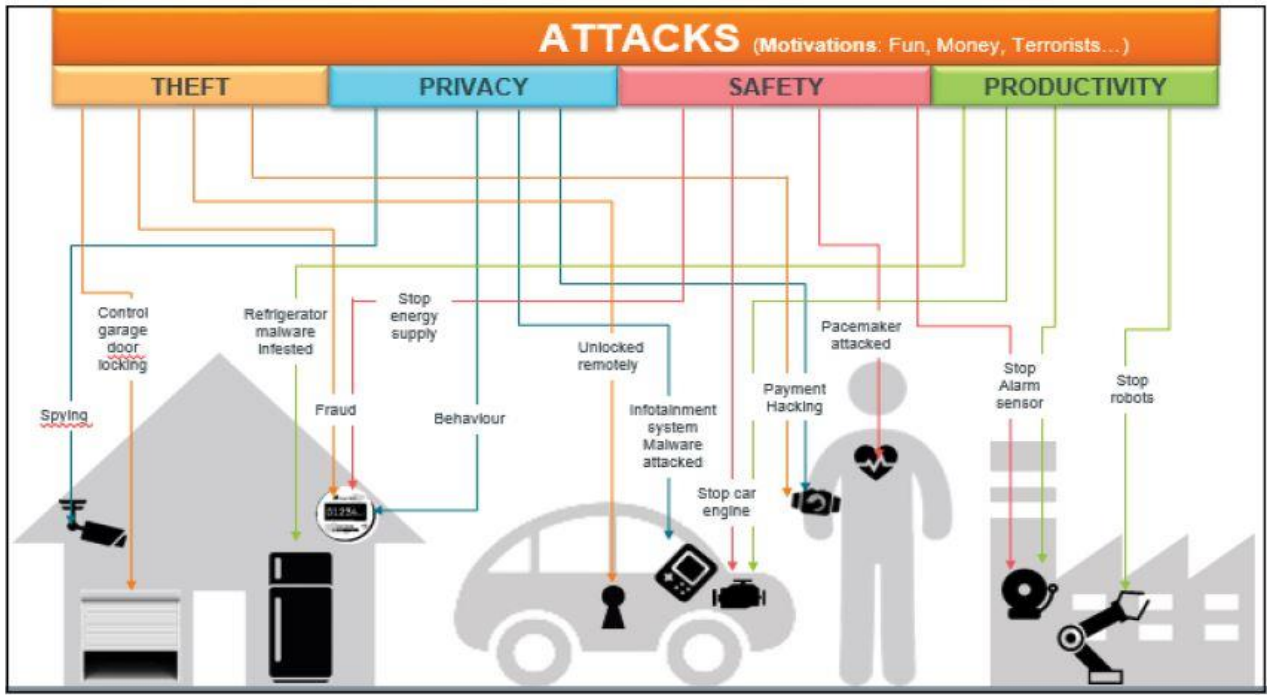


Figure 1.3: **Importance of IoT security**

data that IoT devices collect pose a considerably more significant threat. Attackers can have four main consequences on victims. From Figure 1.8., we can easily conclude “IoT is pressing necessity in today’s world and an indispensable requirement for the future.”

IoT devices mostly operate on low power, limited memory, computing power, and storage area. On the other hand, the traditional network is made up of overflowing resource devices, Therefore, a balance is required between security levels and computational resources in IoT systems, which calls for lightweight security schemes. In lightweight security, we need to focus on lightweight cryptographic techniques such as ECC, Hash functions, XOR, linear pairing .

In the process to decide the lightweight techniques, first step is to choose the security requirements of different IoT based systems or application. In 2020, Iqbal et al. comes with in depth analysis of security requirements of different systems [3]. In Table 1.1., we can see that among all security requirements such as Confidentiality, Integrity , Availability (CIA), Privacy, Non-Repudiation and Authentication, Authentication is common for almost all application of IoT. Confidentiality takes second place. Verifying the

Table 1.1: **Summary of IoT Applications core security Requirements**

IoT Applications	Confidentiality	Integrity	Privacy	Authentication
Smart Grids	✓	✓	✓	✓
Healthcare	×	×	×	✓
Transportation System	×	×	×	✓
Smart Cities	×	×	×	✓
Smart Manufacturing	×	×	×	✓
Smart Homes	×	×	×	✓
Smart Wearable	×	×	×	✓
Smart farming	✓	✓	✓	✓
Smart Supply Chain	×	×	✓	✓
Smart Security System	×	×	×	✓

identity of a user, device, or other entity trying to access a system or resource is commonly referred to as authentication in the realm of security. It is a key security mechanism that makes certain that only authorized people or organizations have access to confidential data, programs, or services while guarding against unauthorized access or potential security breaches. Presenting credentials, such as usernames, passwords, biometrics, smart cards, or digital certificates, is a common part of the authentication process. The system subsequently checks the credentials against stored data or an authentication server. Access is allowed to the person or device if the provided credentials match those on file; otherwise, access is denied. Strong authentication systems are essential for data security, preventing illegal access, and preserving the secrecy, integrity, and accessibility of sensitive data and resources.

In literature, Researchers have done tremendous efforts to propose the various schemes to provide efficient solutions for the IoT authentication. Due to rapid development in technologies, new ways of attacking the IoT device also came into existence. Every day, the technology landscape is constantly evolving and introducing new innovations. With each new technology, unique challenges arise, and the Internet of Things (IoT) is no exception. IoT, with its vast array of interconnected devices, presents a multitude of complexities that demand innovative solutions for authentication.

Overall, Scale and Diversity, Resource Constraints, Privacy Protection, Interoperability, Evolving Technology and User Experience are major reasons for new schemes for IoT Authentication. As a result of the dynamic nature of technology and the particular difficulties faced by the IoT ecosystem, new and creative authentication schemes must be designed. These schemes need to consider the diverse range and dimensions of IoT gadgets, work within resource constraints, highlight the importance of safeguarding privacy, facilitate seamless interaction, adjust to evolving technology, and present a user-friendly system. Unless these challenges are directly confronted, IoT authentication cannot achieve dependability, security, or the ability to support the growing IoT environment.

1.3 Contributions

The major contributions of this work are summarized below, along with the relevant publications.

1. A novel scheme for efficient authentication in cloud-based IoT devices is proposed by the use of discrete logarithmic properties of ECC. The proposed scheme is computationally very light and successfully resists attacks that are not covered by the currently existing scheme.
 - (a) Alam Irfan and Manoj Kumar. “A novel scheme for efficient authentication in cloud-based IoT devices.” *Multimedia Tools and Applications* (2022), SCIE-Indexed (I.F: 3.75) [4]
2. A novel authentication scheme has been proposed to ensure confidentiality of Internet of Medical Things (IoMT). This scheme is best suit for COVID-19 and future pandemic situations . The use bilinear pairing with hash and XOR function makes this scheme resilient to most common attacks in healthcare industries.
 - (a) Alam Irfan and Manoj Kumar. “A novel authentication protocol to ensure confidentiality among the Internet of Medical Things in covid-19 and future pandemic scenario.” *Internet of Things* (2023), SCIE-Indexed (I.F.:5.9). [5]
3. Group-based Authentication (GBA) has been extensively studied, and a

novel scheme has been introduced to enhance GBA's application in smart cities. In this scheme, the binomial polynomial is utilized in a secret sharing scheme, ensuring robust security against potential threats. By employing this approach, the proposed GBA scheme demonstrates improved resilience and effectiveness in safeguarding smart city infrastructures and services.

- (a) Alam Irfan, and Manoj Kumar. "A novel authentication scheme for group based communication for IoT oriented infrastructure in smart cities." (2022).

Under review in *IEEE transaction on information forensics and security*. (SCIE-Indexed with I.F.:7.211) [6]

4. Various aspects of performance evaluation are considered, encompassing both formal and informal analyses. The performance evaluation helps identify any bottlenecks, vulnerabilities, or potential inefficiencies in the proposed scheme. It aids in fine-tuning the scheme design and ensuring that it aligns with the resource constraints of IoT devices, allowing for seamless integration and operation within the IoT ecosystem.

- (a) Alam Irfan, and Manoj Kumar. "Various Elements of Analysis of Authentication Schemes for IoT devices: A Brief Overview". *International Conference on Recent Advances in Computer Science and Engineering (ICRACSE-2022)*, Scopus Indexed

5. Existing work in IoT Authentication is studied discussing its main concepts, challenges, evaluation metrics. The security of IoT devices is a constantly evolving field, and researchers and security experts have indeed made significant strides in studying various aspects of attacks targeting IoT devices. After thorough study, we came into the comprehensive literature survey for IoT authentication.

- (a) Alam Irfan, and Manoj Kumar. "An overview of Secure Communication in Smart Cities: Issues and Cryptographic Solution." 2022 International Conference on Data Analytics for Business and Industry (ICDABI). IEEE, 2022. [7]

- (b) Alam Irfan, and Manoj Kumar. "A Critical Authentication Analysis

and Future Research Directions for the Security of Internet of Things: A Comprehensive Review” is communicated in *Internet of Things, Science Direct*

1.4 Outline of thesis

This thesis contains seven chapters. Flow of thesis are following:

- Chapter 1 presents an overview of IoT devices, such as the definition of IoT the basic architecture, the application of IoT, and IoT Security .
- Chapter 2 delves into the state of the art with a comprehensive literature review. It begins by addressing the importance of conducting such a review. Following this, chapters 3, 4, and 5 are reviewed in detail. The analysis identifies knowledge gaps through a thorough examination of existing literature, and subsequently, the problem is formulated.
- Chapter 3 first discusses the crucial role of IoT devices in our daily life and the advantages of using cloud computing on IoT devices and authentication requirements in such an environment. Efficient authentication is the need for the hours for IoT devices. The proposed scheme is computationally very light and successfully resists attacks that are not covered by the currently existing scheme. Elliptic curve discrete logarithm problem (ECDLP) is used with a one-way hash function and the XOR operator. Use of ECDLP makes the proposed schemes are hard to break. The use of a one-way hash function and the XOR operator maintains the efficiency of authentication along with secrecy.
- Chapter 4, IoT devices performance in group-based communication is discussed, so the proposed scheme deals with group-based membership authentication. It provides recent compulsory security features and has lower communication, storage, and computation costs than existing schemes.
- Chapter 5, we have proposed a novel authentication scheme that can provide confidentiality also. Its applicability in the Medical Internet of

Things (MIoT) with the special consideration of COVID-19 is discussed in detail. Bilinear pairing is used as the core concept behind this protocol.

- Chapter 6, explores methods for the performance evaluation of different schemes for resource-constrained IoT network. The schemes discussed in Chapters 3, 4, and 5 are evaluated in detail by using Automated Validation of Internet Security Protocols and Applications (AVISPA) and SCYTHER. The proposed schemes are verified using BAN logic and simulated using High-Level Protocol Specification Language (HLPSL) language for the AVISPA tool. We have included crucial techniques for manipulating BAN logic and utilizing the AVISPA tool in any endeavors involving the secure utilization of IoT devices.
- Finally, Chapter 7 concludes the present thesis with prospective research work.

Chapter 2

STATE OF THE ART: THE LITERATURE REVIEW

After the necessary knowledge about IoT and its security in Chapter 1, this chapter presents the details of existing literature and techniques that are the basis of the present work.

We have started with the need for a literature review in Section 2.1. Section 2.2 has been divided into subsections to demonstrate the literature reviews of IoT Security in different areas based on the applications and the technology used. Subsection 2.2.1 is about the authentication scheme for cloud-based IoT devices. Group-based authentication has been discussed in 2.2.2. Subsection 2.2.3 explains the literature regarding the authentication of the Internet of Medical Things (IoMT) and its application in COVID-19 and future pandemics. Methods of performance evaluation of the schemes in resource-constrained IoT networks have been discussed in Subsection 2.2.4. Based on these reviews, the knowledge gap has been concluded in Section 2.3. The objectives of the research work have been described in Section 2.4.

This Chapter presents a thorough evaluation of the literature reviewing pertinent papers from four major academic databases (IEEE Xplore, Web of Science, ACM Digital Library, and ScienceDirect) to better understand the cyber-security threats and vulnerabilities in the IoT systems .

2.1 Need for literature review

Any academic or research study needs a solid foundation, and a literature review provides that. It is a succinct analysis and summary of prior research and expertise on a particular subject or research question. Researchers can uncover knowledge gaps, evaluate the advantages and disadvantages of earlier studies, and obtain a detailed understanding of the historical background of their topic by performing a thorough literature review. They can build on previous research, cut out duplication of effort, and create more focused and pertinent study objectives thanks to this method. Furthermore, by displaying a thorough understanding of the subject and situating their research within the larger academic environment, a well-done literature review strengthens the credibility of their work.

2.2 Literature review

IoT has a significant impact on people's everyday lives, which draws researchers to expand their research so that it can benefit people. As a result, many researchers labored on the IoT survey to provide information about the IoT system and its specifics. A few pieces of work have been done to give an overview of IoT security security issues. A few pieces of work have been done to give an overview of IoT security issues. The potential threats are reviewed in [8–11]. Various attack types were covered in these papers. The security flaws in Bluetooth are shown in article [12], along with potential Bluetooth-based IoT threats. The challenges of IoT are presented by others, and a few of them are [13–15], etc. The article [14] also presented security guidelines and the impact of 5G on IoT systems was discussed in [16]. IoT architecture and layers were focused on and different protocols are discussed in [11, 17, 18]. Various applications of IoT were discussed in different papers, such as [19] showing the impact of smart logistics in the industry. As the IoT is a resource-constrained device, efficient and lightweight operations are required. To cover these things, refs. [20–22] showed how edge computing can help process IoT services, like smart agriculture, smart logistics, etc. Concerning the aforementioned type of

research, it becomes imperative to guarantee secure data transmission and provide protection against various security attacks. The authentication framework has been formulated with careful consideration of these factors.

2.2.1 Review on details of authentication protocols for cloud based IoT devices

In general, Confidentiality, Integrity, and Availability (CIA) are the main features to be taken care of in the case of traditional security. In contrast, in the case of the IoT, security measures vary from application to application. In 2020, Iqbal et al. [3] assessed IoT security requirements, challenges, and remedies in depth. From there, it is clear that authentication is mandatory for almost all applications related to cloud-based IoT infrastructure. In their survey paper, Nandy et al. [23] reviewed all aspects of IoT authentication. It also explains the taxonomy of all possible attacks on IoT authentication, factors involved in choosing the authentication technique, and the tools for simulation of authentication protocols for IoT devices. Authentication protocols are usually based on three parameters: biometric features of users, credentials, and smart cards.

In 1981, Lamport [24] proposed a password-based authentication protocol for untrusted networks. However, a stolen-verifier attack was found in password table-based protocols at the server end. After that, numerous protocols have been proposed using a single or combination of the techniques such as Smart card, Password, and Biometrics. In 1985, Victor Saul Miller [25] and Neal I. Koblitz [26] came up with the elliptic curve in cryptography. Elliptic curve cryptography (ECC) algorithms have been used since 2004 widely due to their small size and low computational requirements with the same security level as Rivest-Shamir-Adleman (RSA) [3, 27]. In [28–31], authors have worked with the Computational hardness of ECC for IoT devices. In [32], Kim et al. have done cryptanalysis of the hash function. Protocols like [33–35], have used hashed-based algorithms, which are helpful to ensure the integrity of the messages and verify the sender as well.

In 2015, Li et al. [36] proposed a mutually authenticated protocol based on a smart card in cloud computing. Their protocol does not persist against physical attack, forging attack, and masquerade attack [37]. Furthermore, Sun et al. [38] proposed a novel remote user authentication and key agreement protocol for the mobile client-server Environment. Still, it does not provide a pleasant process of password update and biometric change [37].

After that, in 2016, an efficient authentication protocol was proposed for IoT-enabled devices in a distributed cloud environment by Amin et al. [39]. In this work, different attacks has been discussed, such as user anonymity, insider attack. In 2018, Challa et al. [40] analyzed that Amin et al. protocol [39] does not resist masquerade attacks such as Privileged Insider Attacks (PIA) and impersonation attacks. In 2018, Wu et al. [41] explained that Irshad et al. [33] and Amin et al. [39] are vulnerable to PIA and Offline Password Guessing (OPG) attacks, respectively. They both do not guarantee User AnonymityUser Anonymity (UA). Recently, Wu et al. [35] analyzed Xu et al. protocol [41]. They concluded that Xu et al., protocol could not resist Privileged Insider (PI) and Stolen Smart Card (SSC) attacks and did not provide pre-verification and Perfect Forward Secrecy (PFS).

2.2.2 Review on group based authentication.

Authentication is critical for IoT devices to avoid severe damage and mass destruction. Due to limitations in resources such as heterogeneity and low power supplies, an authentication mechanism must be lightweight. Researchers have used many lightweight techniques such as ECC, blockchain, hash, and XOR functions instead of heavy cryptographic algorithms [42–44].

In the context of vaious IoT based systems such as smart city, several devices constitute a group. Secure group communication and membership authentication is needed for hours. Recently, [45–47] have used group-based authentication in fog computing, drones network and Intelligent transportation system Intelligent transportation system (ITS), respectively.

Studies on group authentication are mostly based on secret sharing schemes. The secret sharing scheme was first introduced by Shamir in 1979 [48]. In 2013, Shamir's secret sharing scheme was exploited by Harn [49] for efficient group authentication, Harn proposed an idea of group authentication whose complexity ($O(n)$) is very much less than the conventional approach of authentication ($O(n^2)$) [50]. Three different Group Authentication Scheme (GAS) were put forth by Harn. If group users share their private keys simultaneously, his first scheme offers a solution. The other two schemes that Harn has suggested are made for asynchronous key sharing. Chien [51] demonstrates in his paper that Harn's techniques are insecure and that an attacker may recover the security parameters. He proposes a brand-new system based on bilinear mapping and elliptic curve cryptography (ECC). Chien also compares communication costs between his proposal and Harn's approach. Although the tokens are disclosed using an arbitrary point on an elliptic curve determined before each group authentication session, redistribution is required when all points are distributed and used. In addition, between-node synchronization is required using a previously disclosed value when an internal group node does not participate in group authentication. Furthermore, the Harn and Chien schemes broadcast tokens to nodes participating in group authentication during authentication. This process (resembling an IoT environment) is hierarchical and does not ensure secure communication in an environment where communications are connected, and a group leader manages devices. We solve this problem by devising a Group authentication scheme (GAS) that operates safely in IoT communication environments but employs reusable authentication.

In group-based authentication, an adversary can pretend to be a legitimate member, or a legitimate member may act as an internal adversary. To prevent such types of attacks membership authentication has been used by several authors [52, 53] and [54]. In the case of membership authentication, there is a need for a secure network to exchange tokens among other members to prevent attacks such as man-in-the-middle attacks and reply attacks. Setting up a secure network separately for each interchange of tokens will lead to an inefficient and uneconomical Infrastructure of IoT

devices that will never suit smart cities. In present work, Protected secret sharing scheme (PSSS) has been used to propose a novel scheme in which one part of the token is used to encrypt another.

In 2017, Harn proposed PSSS [55]. In PSSS, a bivariate polynomial instead of a single variable polynomial is used to avoid extra channels, variables and keys for the exchange of secrets to members of the group. Harn used PSSS for group authentication with multiple trials and multiple authentication [56]. Their scheme, however, does not integrate the new feature. Their analysis is poor and fails to consider a wise insider attack. Furthermore, their scheme's parameters are also unreasonable. [57].

2.2.3 Review on authentication schemes for Medical Internet of Things to ensure confidentiality.

By 2025, IoT would have a favorable economic impact of 3-6 trillion per year, with IoMT services accounting for 1-2.5 trillion of that total [58]. Several researchers developed IoT authentication mechanisms with ample applications in almost all areas of the human race, such as agriculture [59]- [60] and Smart Grid [61]- [62]. A lightweight scheme was proposed by Zhang et al. [63], a process by which users and drones mutually authenticate each other. Jiang et al. [64] also introduced a cloud-centric key agreement and three-factor authentication approach to ensure secure access to cloud servers and autonomous vehicles . Adil et al. [65] and Kumar et al. [66] have recently concentrated on authentication for healthcare systems. For Wireless Medical Sensor Networks (WMSN), Wu et al. [67] created a lightweight authentication system that offers the attribute of user untraceability . For intra- and inter Wireless body area networks (WBAN), Yuan et al. presented a health-critical index utilised to guarantee the transmission privilege of emergency data [68]. A strong ECC-based authentication and key generation technique for healthcare applications was proposed by Ostad-Sharif et al. [69]. However, Kumari et al. [70], emphasised that due to key compromise, their protocol cannot withstand impersonation assaults and password guessing attacks . Even though the abovementioned schemes are focused on IoT in healthcare. However, we

require an IoMT capable of handling conditions that may arise during a pandemic, such as AI-based patient health monitoring and quick responses for both patients and hospital administrators. After covid-19, researchers also worked towards the area of authentication in IoMT, such as Rehman et al. [71] have focused on the attacks on the deep learning-based solution to IoMT in covid-19 but do not provide its remedies. Masud et al. [72] tried to overcome many attacks but did not provide a check for correctness.

2.2.4 Review on performance evaluation

The significant aspects of conventional security to be concerned with are confidentiality, Integrity, and Availability (CIA). In contrast, IoT security protocols vary from application to application. Iqbal et al. [73] conducted a thorough assessment of IoT security requirements, difficulties, and solutions in 2020. It follows that practically all applications connected to cloud-based IoT infrastructure must require authentication. Authentication is the process of verifying the identity of a user or information. There are lots of literature on authentication for IoT devices. Some of the recent works are [74–78].

A particular authentication scheme must pass through a solid analysis before its implementation in any application. Cryptanalysis and Performance analysis are the two main elements of analysis for IoT devices [79–81]. Cryptanalysis is the study of methods for decrypting data that has been encrypted without having access to the secret information often required. The usual requirements include finding a secret key and understanding how the system works. Another name for cryptanalysis is codebreaking or cracking the code. When choosing or constructing schemes for IoT devices, performance analysis is one of the centric factors to care very minutely. In performance analysis, we concentrate on various factors, such as computational cost, communication cost, and storage capacity. There are various survey papers focusing on IoT device security in different areas. Ashraf et al. [82], have focused on the maritime industry . Yang et al. [83], described the physical security of IoT devices but lacked all possible attacks. Similarly, Serror et al. [84], have focused on Industrial IoT , but it lacks a description of the simulation tools for the security analysis of various

schemes. On the other hand, Alam et.al [4], described cloud-assisted IoT infrastructure . Various informal and formal proof of security and analysis are discussed in these manuscripts. Some extra features must be added to make it universally accepted.

2.3 Knowledge gap analysis

The following are the key research areas where some gaps are identified. These gaps are as follows:

- Above discussed schemes fail to resist various attacks such as a stolen verifier attack, activity tracking attack, data manipulation attack, sensor capture attack, desynchronization attack, sensor forgery attack, known session-specific attack, routing attack.
- Most of the literature covers only one aspect of security. Very few existing schemes assure Confidentiality and Integrity alongwith authentication, while, in Iqbal et al. [3], we have already seen that confidentiality is also very important in most of the IoT oriented applications.
- In IoT devices, we must consider the parameters such as communication cost, storage overhead, and energy consumption. Very few of the recent literature explained all types of conditions to make schemes efficient and compatible with real world.
- Schemes are not robust to both dynamic environmental conditions and flexible user behavior.
- Very few schemes are designed for general purpose that fits all types of IoT applications. They are application-specific and vary from application to application.

2.4 Problem formulation

Based on the research gaps, the following main objectives are proposed:

- To design a novel scheme for efficient Authentication in cloud-based IoT devices that covers most of the attacks.

- To design an authentication scheme to ensure secure Group based communication among IoT devices that suites for dynamic environmental conditions of IoT devices.
- Design a scheme to ensure Authentication and Confidentiality of messages exchanged with consideration of resource-constraint IoT networks.
- Discuss the performance evaluation of above discussed schemes in resource -constrained IoT network.

Chapter 3

AUTHENTICATION SCHEME IN CLOUD BASED IoT DEVICES

The Internet of Things (IoT) has emerged as one of the most revolutionary technological innovations with the proliferation of applications within almost all fields of the human race. A cloud environment is the main component of IoT infrastructure to make IoT devices efficient, safe, reliable, usable, and autonomous. Reduction in infrastructure cost and demand accessibility of shared resources are essential parts of cloud-based IoT (CIoT) infrastructure. Information leakage in cloud-based IoT devices may invite dangerous activities and phenomena. Various cloud-based systems store IoT sensor data and later on access it accordingly. Some of them are public, and some of them are private. Private cloud services must be secured from external as well as internal adversaries. Hence, there must be a robust mechanism to prevent unauthorized access to the devices. This paper proposes a novel and efficient protocol based on the Elliptic Curve property known as Elliptic Curve Discrete Logarithm Problem (ECDLP) with hash and XOR functions for the authentication in cloud based IoT devices. In comparison to the existing protocols, the proposed protocol is resistant to attacks and other security vulnerabilities. The one-way hash function and XOR function effectively ensure a reduction in computation cost. AVISPA and BAN logic have been used for formal analysis of the proposed protocol. As per the performance analysis results, it is clear that the proposed protocol is efficiently suitable for cloud-based IoT devices.

3.1 Introduction

The Internet of Things (IoT) is a setup of different entities like objects, people, and animals capable of transferring data over networks without head-to-head or head-to-computer connection. IoT is an acronym for Any time, Anything, Any place connections. In recent years, the Internet of Things (IoT) has risen to prominence as a critical technological component for overcoming interoperability, heterogeneity, and Internet-aware resistances. The deployment of IoT devices has increased exponentially, resulting in a large amount of data handling and analysis [85]. There is a need for a standard platform to manage heterogeneous gadgets and data. Cloud-based infrastructures are well suited to this need. Ray, in his survey paper, describes applications for the IoT cloud platforms [86]. In general, cloud services are of two types: public cloud services and private cloud services. A person or organization owns private cloud services that make cloud security essential [87]. Analysis of the cloud-based IoT (CIoT) device mechanism [88–91] shows that most applications carry essential information, and leakage of such information may lead to a significant loss and several attacks. Also, the nature of attacks changes from time to time. Computing resources are employed on-demand via a network in the Cloud services. It consumes a significant amount of energy, which can not be measured easily with computational resources. Pete et al. [92] proposed an experimental energy-efficient model for Virtual Machines Virtual Machines (VMs) scheduling over the cloud. Furthermore, Kumar et al. [93], illustrate an economically efficient model for virtualization over the Cloud using a docker container. Authentication is a primary security mechanism for all network-based services that prevent unauthorized users or adversaries from gaining access [27]. It is compulsory to ensure that only authenticated users should access the resources. For information exchange through an unsecured network such as the Internet, IoT authentication can ensure the trust of IoT devices. A robust IoT authentication model is needed to protect unauthorized users and devices. Traditional public-key cryptosystems are commonly used in authentication procedures. Traditional public-key cryptosystems, such as RSA, have large key sizes and use a lot of computing

resources [94] . As a result, most standard authentication systems are incompatible with the limited computational power of IoT devices. Recently, several research papers addressed IoT authentication and the possibility of attacks [33, 35, 36, 39, 41, 95]. However, many attacks are still unresolved, such as packet analysis, gateway forgery, and sybil attacks. Choosing an appropriate protocol to address recent attacks is a tough task, due to unavoidable resource constraints, such as low power support, small storage, low computational support, and low latency support. The proposed protocol is a solution for above said challenges. The significant contributions of this paper have been listed as follows: A novel protocol has been proposed for the IoT infrastructure based on a cloud environment. The proposed novel authentication protocol prevents adversaries from common attacks such as man - in - the - middle, masquerade, denial of services, forging, guessing, and physical attacks. It can provide robust and secure authentication using the Elliptic Curve Discrete Logarithm Problem (ECDLP) property of ECC with hash and XOR functions. NP-hard complexity of ECDLP makes the protocol resistant to attacks such as Forging, guessing, and Man in the middle, and the inclusion of XOR and hash keeps it lightweight. The proposed protocol has been compared with the existing protocols to explore its ability to resist attacks, reduce computation power and storage requirements, etc. Its computational cost is very low (0.2 s) and resists more than fifteen modern attacks. It also shows its usefulness more than other existing protocols. and The modular structure of protocols varies from application to application. We have tried to modal the proposed protocol in such a way so that it suits ninety percent of IoT infrastructures. In Chapter 4, Simulation of the proposed protocol using AVISPA [96] and BAN logic [37, 38] proves its power against active adversaries. Description of BAN logic and AVISPA in the present article would allow readers to understand and apply these tools for other protocols easily.

3.2 Preliminaries

3.2.1 Elliptic curve discrete logarithm problem (ECDLP)

For two points, P and Q , of an elliptic curve $E_p(a, b)$. The ECDLP is to find an integer $K \in [1, n - 1]$ such that $Q = k.P$.

ECDLP is more complicated than most discrete logarithm and factorization problems in cryptography. There are several attempts to break this problem; however, it is still unbreakable.

3.2.2 One-way cryptographic hash function

Here we describe the brief properties of the hash function, which are as follows:

- This function is deterministic $h : \{0, 1\}^* \rightarrow \{0, 1\}^n$
- h is the hash function, where output produces $y = h(x)$ (hash digest), $y \in \{0, 1\}^n$.
- Any small modification to the input string potentially leads to an entirely different hash value (message digest).

3.2.3 System model

The modular architecture of IoT-based systems may vary from application to application. We have tried to consider the most common approach suited for 90% of IoT infrastructure. As shown in Fig. 3.1, the main components of the proposed system are User (U), Cloud Server (S_m) directly associated with IoT devices, and Trusted Authority (TA) sometimes called a control server.

Both user (U) and cloud server (S_m) must register with (TA) before (U) can access (S_m) data via a secure channel. Necessary credentials for (U) and (S_m) are generated by a Trusted Authority (TA) and stored in their memory. A session key is established (After mutual authentication between (U) and cloud server(S_m)) for future independent communication.

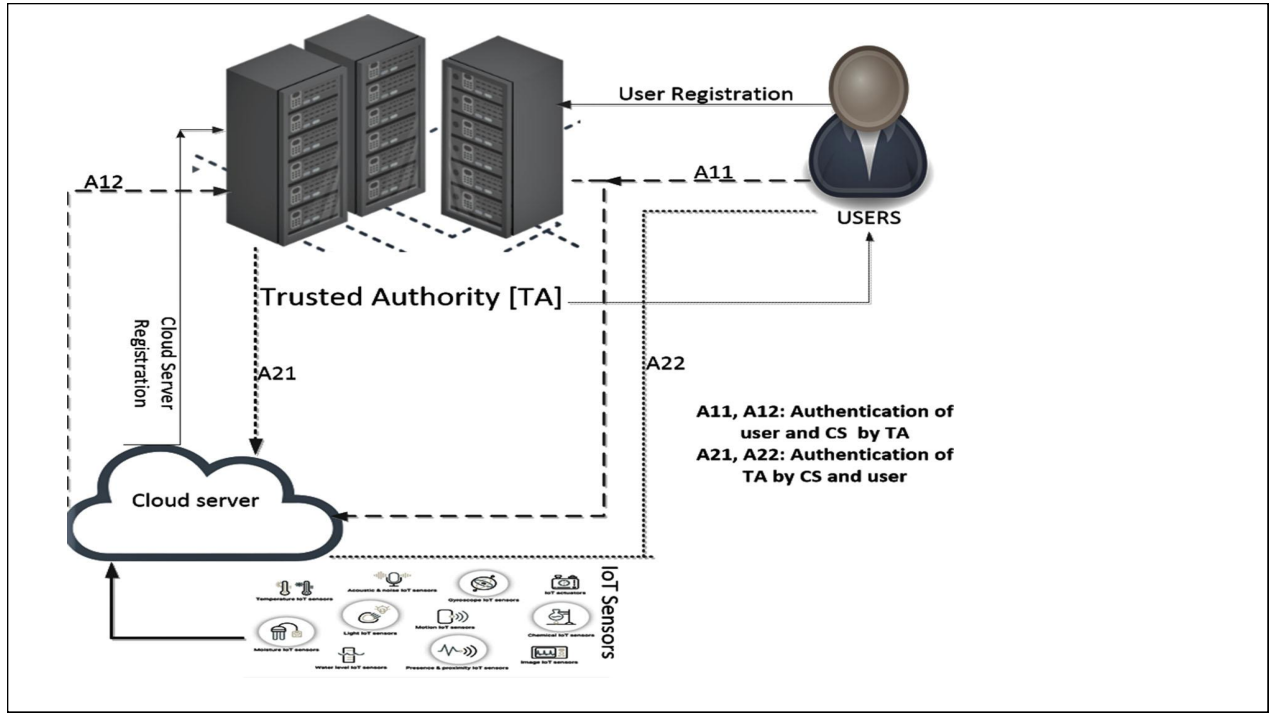


Figure 3.1: **Cloud-based IoT environment authentication model**

3.2.4 Adversary model

If there is a protocol for some security purpose, there must be some adversary model against which the protocol is safe. A fundamental and most common adversary model was proposed by Dolev and Yao [97] in 1983. It is a broadly accepted model. According to this model, an adversary can read, alter and perform decryption (if got right keys) on messages. Adversaries are unable to carry out any statistical or cryptanalytic assaults. Due to rapid transformation in technologies, adversaries are now more advanced and have extraordinary capacities. Along with the Dolev and Yao model, we have considered that adversaries would know critical information from smart cards (if lost/stolen) using power analysis of smart cards [98,99]. An adversary would also extract data from network flow using a network analyzer and AI techniques [100,101].

3.3 Proposed protocol

This section presents an ECC-based protocol designed mainly to ensure that the devices are accessible in a secure manner on public channels. Cloud involvement in all entities and clock synchronization is our assumption for

the proposed protocol. In Table 1, we listed necessary and frequent notations with their explanation for the proposed protocol. The proposed protocol comprises different phases, viz., pre-deployment, registration, login, and authentication. In the pre-deployment phase, the setup of the elliptic curve is discussed with the declaration of public and private keys. Registration of cloud server and user have been described in subsections 3.3.2 and 3.3.3, respectively. After successful registration, verification of the user is done in the login phase via smart card by a trusted authority. In section 3.3.5, firstly, user authentication proceeded by cloud server authentication is done by a trusted authority. Later, trusted authority is authenticated by both user and cloud server consecutively. At the same time, a session key is established for further communications between the user and the cloud server

3.3.1 Pre-deployment phase

An elliptic curve $E_P(b_1, b_2)$ of non-singular nature over a finite field Z_P is selected by TA, where P is a large prime and $4b_1^3 + 27b_2^2 \neq 0 \pmod{P}$. At the same time, a base point P of order n over $E_P(b_1, b_2)$ where TA also chooses $n.P = O$, and a private key $d_{TA} \in Z_P$. Then TA computes the public key $Q_{TA} = d_{TA}.P$ corresponding to d_{TA} . TA chooses the one-way cryptographic hash function. In the same way, cloud servers and the user also compute private keys and public keys using ECC properties.

3.3.2 Registration of cloud server

- Cloud server S_m chooses identity $(sid_m), d_{cs} \in Z_{cs}$ and $Q_{cs} \doteq d_{cs}.P$ after that sends $(sid_m), d_{cs}$, and Q_{cs} securely to TA as shown in Fig. 3.2.
- TA computes $psid_m = h(sid_m || d_{cs})$.
- TA also computes $B_{sm} = h(psid_m || Q_{TA})$.
- TA sends B_{sm} to S_m , which saves B_{sm} and d_{cs} in the server memory

Table 3.1: Notations of cloud based scheme

S.No	Symbol	Explanation
1.	$E_P(b_1, b_2)$	An elliptic curve
2.	S_m	Cloud Server
3.	U_i	Identity of the i^{th} User
4.	TA	Trusted authority
5.	P_u	Password of user
6.	CR	Card Reader
7.	$Z_p = \{0, 1, \dots, p-1\}$	a prime finite field Z_p
8.	ΔT	Transmission delay
9.	TS_m, TS_u, T_{TA}	Timestamps of CS, User and TA, respectively
10.	$\{Q_{TA}, d_{TA}\}$	Pair of public key, private key of TA
11.	\parallel	Concatenation operation
12.	$H(.)$	Hash functions
13.	SK	Session key
14.	\oplus	XOR function

3.3.3 User registration phase

- User chooses identity (U_i), password (P_u), $d_u \in Z_P$ and $Q_u = du.P$ as shown in Fig. 3.3.
- User calculate $A_u = h(p_u \parallel d_u)$, $PID_u = h(U_i \parallel Q_u)$ and $bb_u = Q_u \oplus A_u$
- Then user send A_u and PID_u to a TA .
- After receiving A_u and PID_u , TA calculates $h(A_u \parallel PID_u)$, $D_u = h(PID_u \parallel d_{TA})$ and $E_u = D_u \oplus A_u$.
- After step 4, TA send $[C_u, E_u]$ to the user
- User again calculate $DP_u = h(U_i \parallel P_u) \oplus d_u$.
- User saves $[C_u, E_u, DP_u]$ in the smart card.

Finally, a smart card holds $[C_u, E_u, DP_u, \text{ECC parameters}]$.

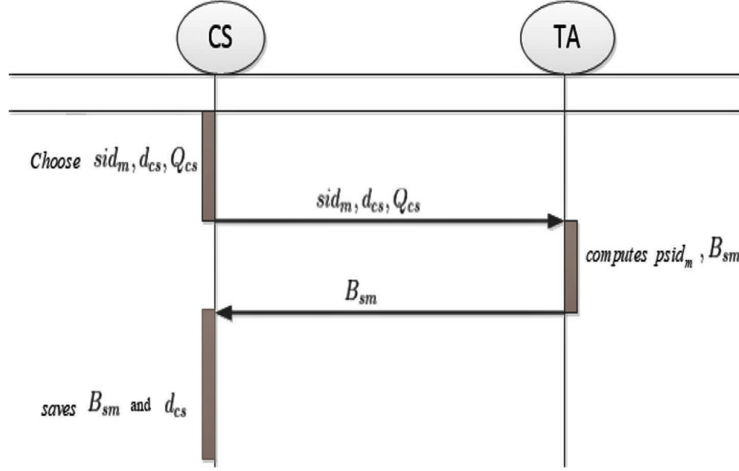


Figure 3.2: Cloud-Server Registration

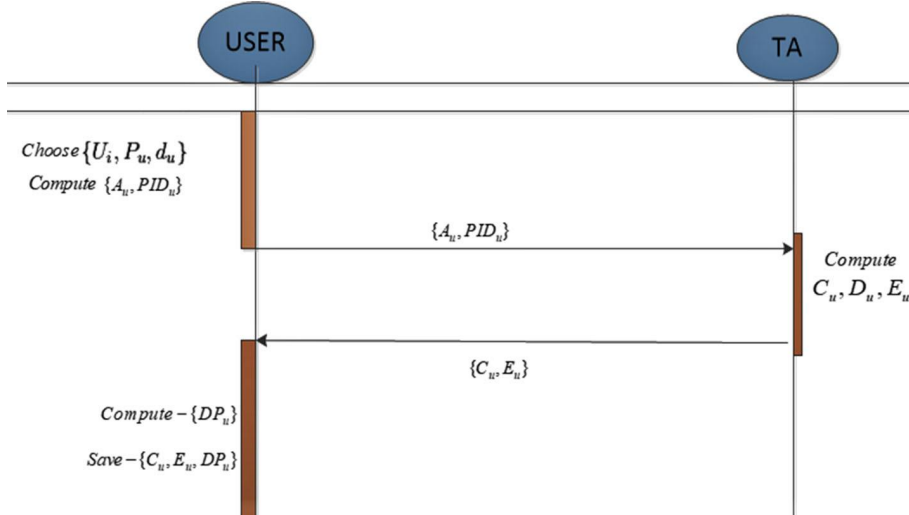


Figure 3.3: User Registration

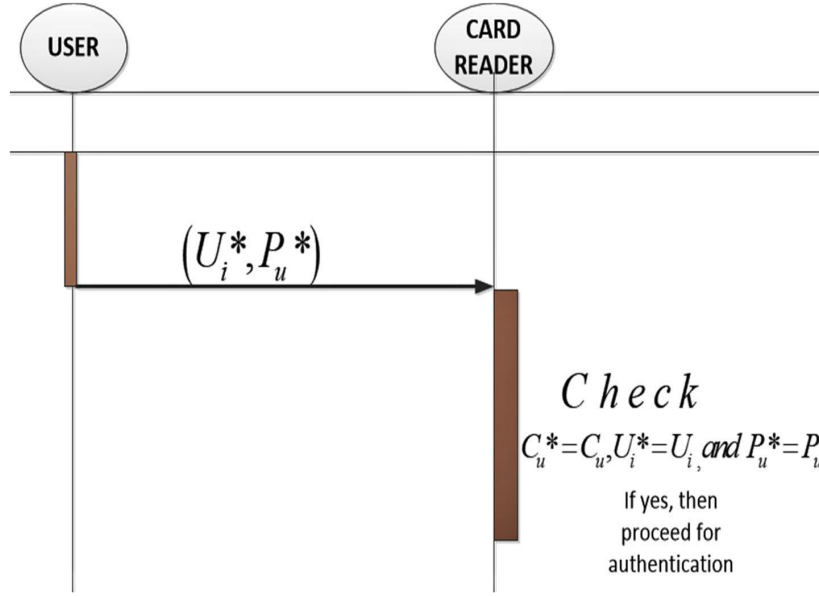


Figure 3.4: **Pre-verification of user**

3.3.4 Login phase

- Firstly, a smart card is punched into the card reader by the legal user for accessing server resources, and then the user provides Id and password $(U_i^*P_u^*)$ in the card reader terminal, as shown in Fig. 3.4.
- After first step card reader calculates the following:
 1. $d_u^* = DP_u \oplus h(U_i^*||P_u)$ and $A_u^* = h(p_u^*||d_u^*)$.
 2. $Qu^* = (bb_u^* \oplus A_u^*)$
 3. $PID_u^* = h(U_i^*||Qu^*)$
 4. $C_u^* = h(A_u^*||PID_u^*)$

Card reader checks the conditions $C_u^* = C_u$, $U_i^* = U_i$, and $P_u^* = P_u$, if satisfied, then it proceeds for an authentication phase.

3.3.5 Authentication phase

- After the login phase, the smart card produces a nonce N_u , Calculate $D_u = E_u \oplus A_u$, $F_u = D_u \oplus N_u$, and $Z_u = SID_m \oplus h(D_u||N_u)$ and send

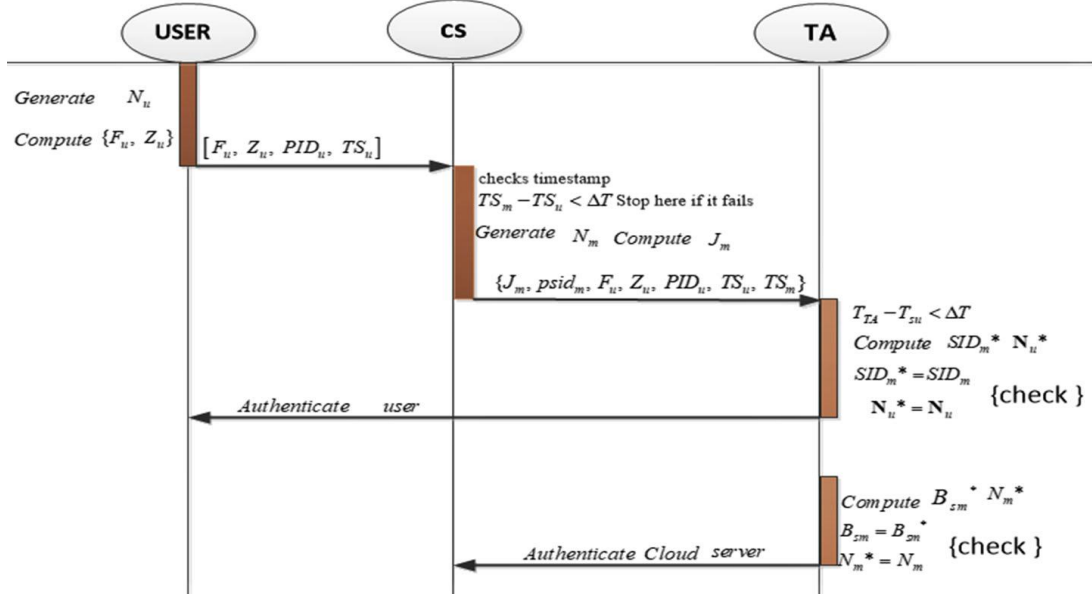


Figure 3.5: **TA Authentication**

$[F_u, Z_u, PID_u, TS_u]$, to the S_m , here (SID_m) is the cloud server identity chosen by the user and TS_u is the user's timestamp.

- The following steps are done on the Cloud server-side, as shown in Fig. 3.5.
 1. At the cloud server, it checks timestamp $TS_m - TS_u < \Delta T$ (Stop here if it fails, where TS_m is a current timestamp and ΔT is the time interval to be expected during message transmission, respectively)
 2. Cloud server produces 128 bits nonce N_m .
 3. Calculates $J_m = B_{sm} \oplus N_m$,
 4. Sends $[J_m, psid_m, F_u]$ and $[Z_u, PID_u, TS_u, TS_m]$ to TA.
- After receiving the above keys, TA confirms the validity of timestamp ($T_{TA} - T_{su} < \Delta T$) and calculates $N_u^* = F_u \oplus D_u$, $SID_m^* = Z_u \oplus D_u$ and check $SID_m^* = SID_m$ and $N_u^* = N_u$. If this is ok then TA authenticates the user as the legal user.
- After authenticating user, TA computes $B_{sm} = h(psid_m || Q_{TA})$ and $N_m^* = B_{sm}^* \oplus J_m$
TA checks $B_{sm}^* = B_{sm}$ and $N_m^* = N_m$ if it is ok, TA authenticates the Cloud server.

- After Authenticated User and Cloud server, TA chooses a 128-bit nonce N_{TA} and computes the following:
 1. $P_{TA} = N_m \oplus N_{TA} \oplus h(N_u || D_u)$.
 2. $SK_{TA} = h(N_u \oplus N_m \oplus N_{TA})$.
 3. $R_{TA} = N_u \oplus N_{TA} \oplus h(B_{sm}^* || N_m^*)$.
 4. $R_{TA} = N_u \oplus N_{TA} \oplus h(B_{sm}^* || N_m^*)$.
 5. $Z_{TA} = h(N_m \oplus N_{TA}) || SK_{TA}$.
 6. $V_{TA} = h(N_u || N_{TA}) || SK_{TA}$.
 7. Finally SK_{TA} is the secret session key.
 8. TA sends $[P_{TA}, R_{TA}, Z_{TA}, V_{TA}]$ to the S_m through public communication.
- After receiving $[P_{TA}, R_{TA}, Z_{TA}, V_{TA}]$ from TA, the S_m computes following:
 1. $W_m = h(B_{sm} || N_m)$,
 2. $N_u \oplus N_{TA} = R_{TA} \oplus W_m$,
 3. $SK_m = h(N_u \oplus N_{TA} \oplus N_m)$ and
 4. $V_{TA}^* = h(N_u || N_{TA}) || SK_{TA}$
- Then, S_m check the condition, $(V_{TA}^* = V_{TA})$.
- If yes, then proceed and send $[P_{TA}, Z_{TA}]$ it to the user publicly.
- On obtaining $[P_{TA}, Z_{TA}]$ from S_m , the user calculates the following:
 1. $L_u = h(N_u || D_u)$, $SK_U = h(N_m \oplus N_{TA} \oplus N_u)$ and $Z_{TA}^* = h((N_m \oplus N_{TA}) || SK_U)$.
 2. A user checks the condition $(Z_{TA}^* = Z_{TA})$ and $N_m \oplus N_{TA} = P_{TA} \oplus L_u$, and an affirmative answer proves that S_m and TA are authentic .

Finally, Mutual authentication is achieved among users S_m and TA.

- Session key $SK_m = SK_u$ are established for future communication as shown in Figure. 3.6.

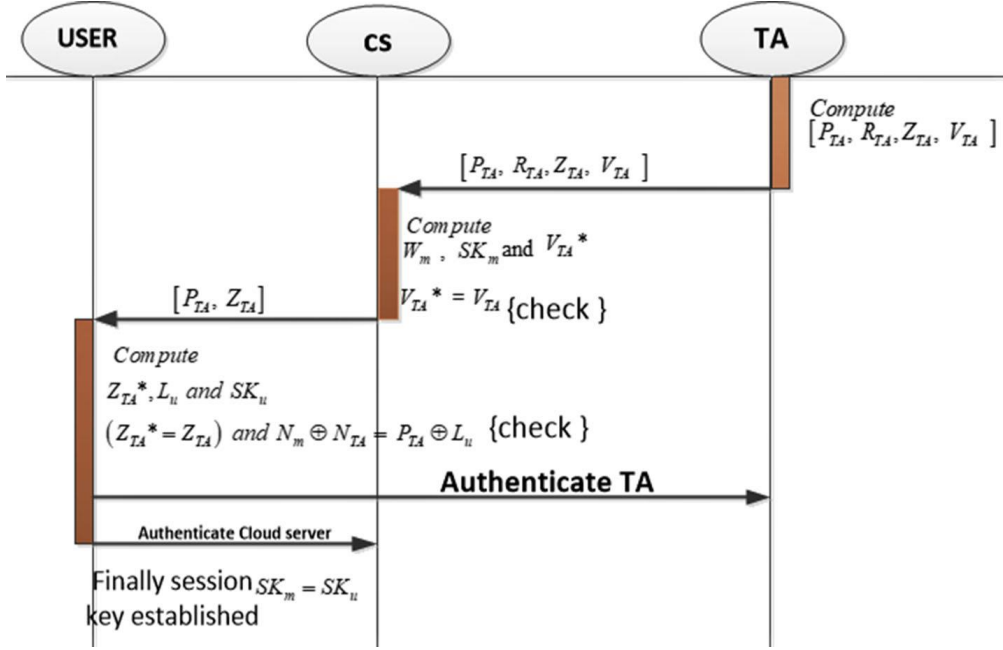


Figure 3.6: **TA Authentication**

3.4 Security Analysis

To demonstrate and validate the security and correctness of our proposed protocol, we use BAN logic [37, 38, 102–105], followed by Automated Validation of Internet Security Protocols and Applications (AVISPA) [106–108]. Furthermore, an informal discussion has also been done in the latter part of this section.

3.4.1 BAN logic (a formal approach of security analysis)

It is very much essential to ensure the correctness of the authentication protocol. Michael Burrows, Martin Abadi, and Roger Needham developed BAN Logic in February 1990 to logically verify the correctness, efficiency, and applicability of an authentication protocol. Although detailed descriptions are illustrated by M. Burrows et al. [103] and more such as [37, 38, 102, 104, 105], we have tried to summarize BAN logic to understand the main concepts of BAN logic. By using BAN logic, we can get the following important information about an authentication protocol:

1. The purpose of each protocol (Goal).
2. The cryptosystem that was used.
3. Whether secrets are used or not (other than the key).

4. Is there a guarantee that messages will arrive on time?
5. Whether protocol establishes each party's presence.
6. To remove redundancy.

The main goal of our protocol is that a user (U), Cloud server (Sm), and Trusted authority (TA) must authenticate one another. A session key (SK) is established for further communication between the server and the user. Following are the steps used in the proposed protocol. Sentences with bold letters are common in all authentication protocols.

The main goal of our protocol is that a user (U), Cloud server (S_m), and Trusted authority (TA) must authenticate one another. A session key (SK) is established for further communication between the server and the user. Following are the steps used in the proposed protocol. Sentences with bold letters are common in all authentication protocols.

- Goals are written

1. G1: U believes $U \xleftrightarrow{SK} S_m$
2. G2: U believes S_m believes $U \xleftrightarrow{SK} S_m$
3. G3: S_m believes $U \xleftrightarrow{SK} S_m$.
4. G4: S_m believes U believes $U \xleftrightarrow{SK} S_m$.
5. G5: S_m believes $S_m \xleftrightarrow{SK} TA$
6. G6: S_m believes TA believes $S_m \xleftrightarrow{SK} TA$
7. G7: TA believes $S_m \xleftrightarrow{SK} TA$
8. G8: TA believes S_m believes $S_m \xleftrightarrow{SK} TA$

- The proposed protocols are idealized and written in the form of language of formal logic.

1. M1 (Message 1):

$$U \rightarrow S_m : pid_u, TS_u, A_u, E_u : \langle A \rangle_{D_u}, F_u : \langle N_u \rangle_{D_u}, Z_u : \langle SID_m \rangle_{D_u || N_u}$$

2. M2 (Message 2): $S_m \rightarrow TA : M1, psid_m, J_u : \langle N_m \rangle_{(b_{sm})}$

3. M3(Message3):

$$TA : \rightarrow S_m : P_{TA} : \langle N_m \oplus N_{TA} \rangle_{h(N_u || D_u)}, V_{TA} : \langle N_u \oplus N_{TA} \rangle_{SK_{TA}}$$

4. M4(Message4): $S_m \rightarrow U : P_{TA} : \langle N_m \oplus N_{TA} \rangle_{h(N_u || D_u)}$

- We identify the assumptions which show the initial state of the proposed protocol.

1. A1 (First assumption): $U | \equiv \#(N_u)[U \text{ believes fresh}(N_u)]$.
2. A2: $S_m | \equiv \#(N_u)$.
3. A3: $TA | \equiv \#(N_u)$.
4. A4: $S_m | \equiv \#(N_m)$.
5. A5: $U | \equiv \#(N_m)$.
6. A6: $TA | \equiv \#(N_m)$.
7. A7: $TA | \equiv \#(N_{TA})$.
8. A8: $U | \equiv \#(N_m \oplus N_{TA})$.
9. A9: $U | \equiv \#(N_u \oplus N_{TA})$.
10. A10: $U | \equiv \#(U \xleftrightarrow{D_u} S_m)$.
11. A11: $S_m | \equiv \#(U \xleftrightarrow{SK} S_m)$,
12. A12: $S_m | \equiv \#(S_m \xleftrightarrow{B_{sm}} TA)$.
13. A13: $TA | \equiv \#(U \xleftrightarrow{SK} S_m)$.

Many other assumptions can be added in the initial assumption, such as $S_m | \equiv \text{controls}(N_u)$, $TA | \equiv S_m \text{ controls}(N_m)$, but they are already evident, so we do not expand that.

- For proof, the idealized forms (M1, M2 , ..., Mn) of the proposed protocol are analyzed. The basis of the analysis is based on the assumptions and BAN logic rules such as Message Meaning (MM), Freshness Conjunction (FC), Belief (BL), Nonce -Verification (NV), Jurisdiction (JR), Session keys (SK). Based on the analysis in the fourth step, we reach the goals.

1. Using $TS_u, A_u, E_u : \langle A \rangle_{D_u}, F_u : \langle N_u \rangle_{D_u}, Z_u : \langle SID_m \rangle_{D_u || N_u}$
with Message-1: $U \rightarrow S_m : pid_u$ and seeing rule we get.
 - $S_m \triangleleft pid_u, TS_u, A_u, E_u : \langle A_u \rangle_{D_u}$.
 - $S1 : F_u : \langle N_u \rangle_{D_u}$.
 - $Z_u : \langle SID_m \rangle_{h(D_u || N_u)}$.

2. Applying MM rule with S1, A11 results in S2: $S_m| \equiv N_u| \equiv N_m$.
3. Applying FC and NV rules A2, S2, results in S3: $S_m| \equiv U| \equiv N_u$
(here N_u is a required parameter of the proposed protocol's session key.)
4. Applying JR rule with A14, S3 results in S4: $S_m| \equiv N_u$.
5. Applying SK rule with A2, S3 results in S5: $S_m| \equiv U \xleftrightarrow{SK} S_m$ (G3).
6. Applying the NV rule with A2, S3 results in S6: $S_m| \equiv U| \equiv U \xleftrightarrow{SK} S_m$ (G4).
7. Applying seeing rule on M2: $S_m \rightarrow TA: M1, psid_m, J_u : \langle N_m \rangle_{B_{sm}}$. and results S7: $TA \triangleleft M1, psid_m, J_u : \langle N_m \rangle_{B_{sm}}$
8. Applying MM rule with A13, S7, and results in S8: $TA| \equiv S_m| \equiv N_m$
9. Applying A6, S7, MM, and NV rule results S9: $TA| \equiv S_m| \equiv N_m$.
Where N_m is a required parameter of the proposed protocol's session key.))
10. Applying JR rule with A15, S9 results in S10: $TA| \equiv N_m$.
11. Applying SK rule with A6, S10 results in S11: $TA| \equiv S_m \xleftrightarrow{SK} TA$ (G7).
12. Applying NV rule with A6, S11 results in S12: $TA| \equiv S_m| \equiv S_m \xleftrightarrow{SK} TA$ (G8).
13. Applying seeing rule with M3 results S13: $S_m \triangleleft P_{TA}, V_{TA}$. Results S14: $S_m| \equiv TA| \equiv (N_u \oplus N_{TA})$.
14. Applying FC and NV rule with A12, S14 results in S15: $S_m| \equiv TA| \equiv (N_u \oplus N_{TA})$
15. Applying SK rule with A9, S15 results in S16: $S_m| \equiv S_m \xleftrightarrow{SK} TA$ (G5).
16. Applying NV rule with A9, S16 results in S17: $S_m| \equiv |TA| \equiv S_m \xleftrightarrow{SK} TA$ (G6).
17. Applying seeing rule with M4: $S_m \rightarrow U : P_{TA} : \langle N_m \oplus N_{TA} \rangle_{(h(N_u||D_u))}$. results in S18: $U \triangleleft P_{TA}$.
18. Applying MM rule with S18, A8 results in S19: $U| \equiv S_m| \equiv (N_m \oplus N_{TA})$.

19. Applying FC and NV rule with S19, A10 results in S20: $U| \equiv S_m| \equiv (N_m \oplus N_{TA})$.
20. Applying SK rule with A10, S20 results in S21: $U| \equiv U \xleftrightarrow{SK} S_m(G1)$.
21. Applying NV rule with A8, S21 results in S22: $U| \equiv S_m| \equiv U \xleftrightarrow{SK} S_m(G2)$.

Thus, the above steps are used in BAN logic to verify the authentication protocols.

Table 3.2: **Attack resilient comparison with existing schemes**

Security Features	[41]	[35]	[109]	[39]	[34]	[28]	Proposed
1. User anonymity and untraceable	✓	✓	✓	✓	✓	✓	✓
2. Offline guessing attack	×	×	×	×	×	×	✓
3. Perfect forward secrecy	×	✓	×	×	×	×	✓
4. Sybil attack	×	×	×	×	×	×	✓
5. Known session-specific temporary information	×	×	×	×	×	✓	✓
6. Stolen smart card attack	×	✓	×	×	×	×	✓
7. Privileged insider attack	×	✓	✓	×	×	×	✓
8. User impersonation attack	✓	✓	✓	✓	✓	✓	✓
9. Cloud server impersonation attack	×	×	✓	×	✓	✓	✓
10. Trusted authority (TA) impersonation attack	×	×	×	×	×	✓	✓
11. Pre-verification in smart card	×	×	×	✓	×	×	✓
12. Pre-verification in the smart card	×	✓	×	×	×	✓	✓
13. Known-key attack	×	✓	×	✓	✓	×	✓
14. Replay attack	✓	✓	✓	✓	✓	✓	✓

3.4.2 AVISPA: A simulator for authentication protocols

It is vital to have tools that support the rigorous analysis of security protocols to speed up the next generation of security protocols and improve their security. For that, it detects weaknesses and establishes their correctness. In 2005, Armando et al. [106], came with a push-button tool for

the automated validation of Internet security-sensitive protocols and applications named AVISPA. The tool is used by a protocol designer who describes a security problem in the HLPSL [108] . Moreover, detailed studies of AVISPA and its execution are available in [106, 107]. In addition to this, some essential tricks to write the protocols in HLPSL language are reported in our work, followed by screenshots of our protocol result.

- First and foremost, the role of each participant is written, which contains the role name, declaration of local as well as constant variables, and transition.
- When the Roles of participants are defined, Roles are combined in a session.
- Define the Environment in which protocol is analyzed that contains prior knowledge about the intruder, the scenario to be executed, and the session instances to be run in parallel.
- Finally, we declare security properties of protocol to be executed.

As shown in figure 3.7 and 3.8, We have passed our protocol with utilities provided by AVISPA tools that are following:

1. On-the-fly Model-Checker (OFMC): Performs protocol falsification and bounded verification.
2. Constraint-Logic-based Attack Searcher (CL-AtSe): It can identify type flaws and manage message concatenation associativity.
3. SAT-based Model-Checker (SATMC): constructs a propositional formula encoding a bounded unrolling of the IF's specified transition relation, the initial state, and the set of conditions denoting a breach of the security properties.
4. Tree Automata based on Automatic Approximations for the Analysis of Security Protocols (TA4SP): Here regular tree languages and rewriting are used to approximate attacker knowledge.

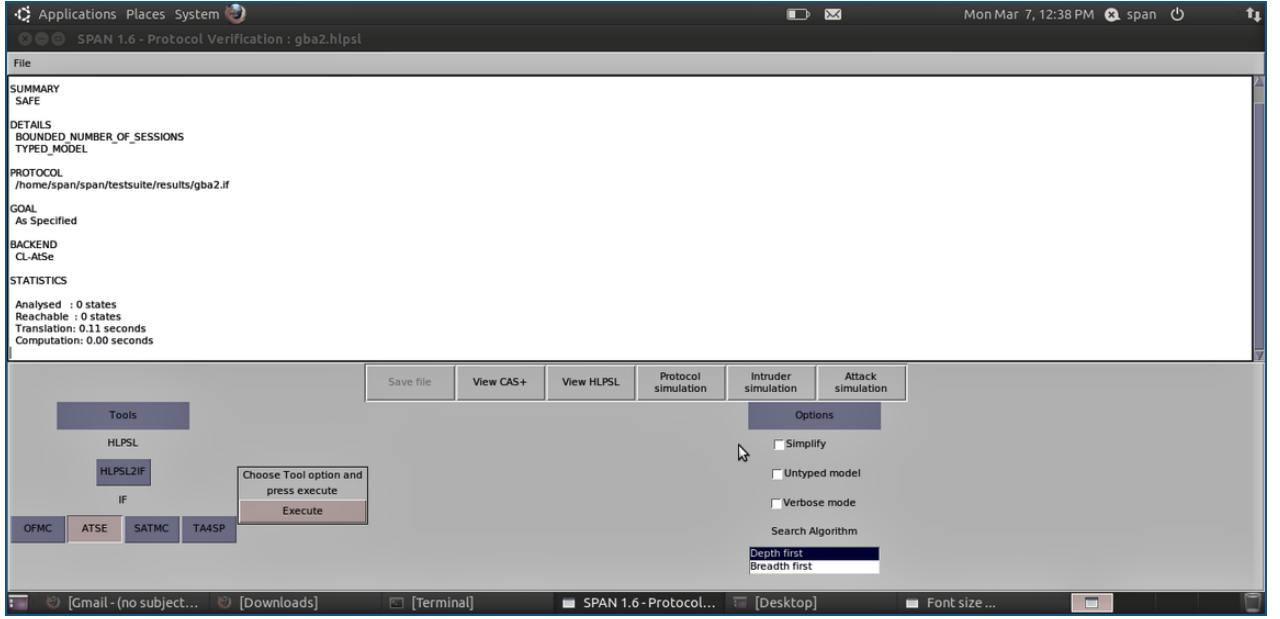


Figure 3.7: Constraint-Logic-based Attack Searcher (CL-AtSe)

3.4.3 Informal analysis of attacks

In this subsection that follow, we do a preliminary study to show the secrecy of the proposed protocol against a wide range of threats.

- **User anonymity and un-traceability** : The identity of user must not be revealed during the exchange of keys among the user, cloud server, and trusted authority. User, cloud server, and trusted authority are generated for each fresh session nonce, respectively. At the same time, different timestamps (T_{TA} , T_{su} and T_{sm}) validate the session. User identity is concatenated with Q_u and hashed that , results into PID_u : ($PID_u = h(U_i || Q_u)$). It is passed to the trusted authority. Hence, it is obvious that extracting information about the user's identity (U_i) is impossible by a third party. So, the proposed protocol preserves user anonymity and the un-traceability of the user's identity
- **Offline Guessing Attacks (OGA)**: The adversary can know various information saved in smart cards using power analysis or differential power analysis attacks [25, 101]. In the proposed protocol, the smart card holds C_u , E_u , DP_u . Concatenation and XOR operation on user identity and password preceded by hashing results above parameters. One-way collision resistance property of hash function and uniqueness of ECC makes too hard to get knowledge about user identity and password. Wu et al. [41] and Tsu et al. [35] are also using almost the

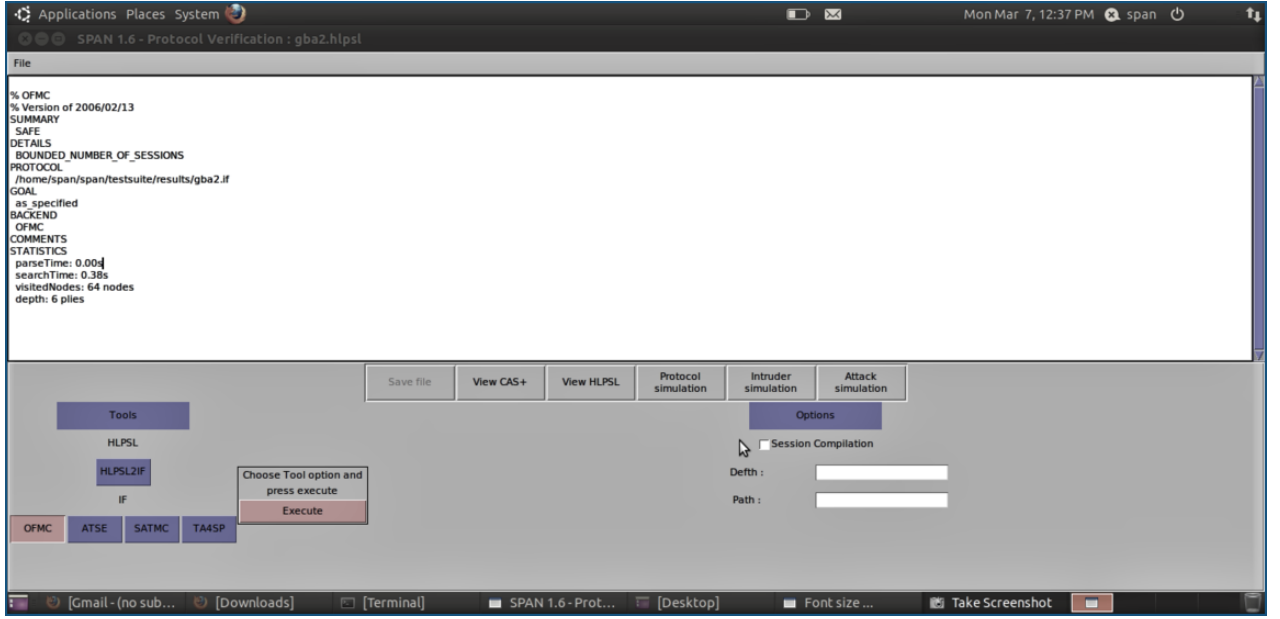


Figure 3.8: **On-the-fly Model-Checker (OFMC)**

same parameters as Amin’s protocol [39]. Possibilities of the same attacks are there in these two protocols. In the proposed protocol, parameters such as user id (U_i), password, and server identity are concatenated with the private key generated on ECC. Then it is hashed with one-way hash function functions. So these consecutive steps eliminate the chance of power analysis attacks.

- **Perfect Forward Secrecy (PFS)** Some keys and parameters are readily available to adversaries. PFS ensures that session keys among users, cloud servers, and trusted authorities are unknown to adversaries at any cost. Here in the proposed protocol, assume an adversary wants to compute $SK_u = SK_m = h(N_m \oplus N_{TA} \oplus N_u)$. These three parameters N_m, N_{TA} and N_u are not available to the adversary because these parameters are always used in hashed conditions and concatenated with elliptic curve points. It is very tough to get a polynomial-time solution to this problem. Hence, the proposed protocol can provide PFS.
- **Sybil Attack (SA)** In a Sybil attack, multiple accounts/nodes are created by an adversary to take over the network. In the proposed protocol, TA’s elliptic curve Q_{TA} is involved in the registration and first phase of authentication. Thus ECDLP property of ECC eliminates the chance of private computing key from known parameters. So the

uniqueness of private keys disaffects the harm of multiple accounts.

- **Known Session-Specific Temporary Information (KSTIA)** In KSTIA attack, session ephemeral secrets are exposed to the adversary, an adversary would be able to get the session keys. In the proposed protocol, almost all information is hashed and concatenated with the private key. It is very tough to extract information from temporary information. Some researcher explains this attack with the name of Ephemeral Secret Leakage (ESL) Attack.
- **Stolen Smart Card Attack (SSCA)** At the worst, there may be the situation that information C_u, E_u, DP_u are known to intruder A due to the loss or steal of a smart card. But due to $h(.)$ protection secret entities of U, viz., C_u, E_u and DP_u , are not known to A. Therefore, our protocol is secure against this attack.
- **Privileged Insider Attack (PIA)** There is always the possibility of two types of adversaries in a system, outside adversaries and inside adversaries. An inside adversary may have privileged access to TA. In this case an adversary can get information such as A_u and PID_u while user is registering to TA, but $A_u = h(P_u || d_u)$, $PID_u = h(U_i || Q_u)$ and d_u, Q_u are the points on elliptic curve, so to reveal P_u and U_i from A_u and PID_u is almost impossible. Furthermore, if the intruder fetches the information C_u, E_u and DP_u from the smart card directly by smart card attack [37, 38], in this case also getting P_u and U_i is very difficult as discussed in stolen smart card attack.
- **User Impersonation Attack (UIA)** An adversary may put P_u and U_i in authentication phase, to impersonate a user U, but to complete authentication by TA, there is need of SID_m and N_u . Getting SID_m and N_u is not possible because $N_u = F_u \epsilon D_u$ and $D_u = E_u \epsilon A_u$, for A_u, P_u is concatenated with d_u (point of elliptic curve) and transferred to TA in hashed form. Therefore getting N_u is too tough, similar is the condition with SID_m .
- **Cloud Server Impersonation Attack (CSIA)** An adversary may get the identity of a cloud server (sid_m) to impersonate the cloud server, but

to be authenticated from trusted authority (TA), $B_{sm} = h(psid_m || Q_{TA})$ should be known where $psid_m = h(sid_m || d_{cs})$. Here, in this case Q_{TA} and d_{cs} are the points of two different elliptic curves. Hence, by using the ECDLP property of ECC, we conclude that our protocol is safe from Cloud server Impersonation attacks.

- **Trusted Authority (TA) Impersonation Attack (TA-IA)** To impersonate TA, an adversary may attempt to get the key $P_{TA}, R_{TA}, Z_{TA}, V_{TA}$ but at cloud server-end $V_{TA} = h((N_u || N_{TA}) || SK_m)$ and at user-end $Z_{TA} = h((N_m || N_{TA}) || SK_u)$ are used for authentication, getting nonces N_u, N_{TA} and N_m in correct form is tough, also collision resistance property of hash function makes almost impossible to get the correct keys. Thus, this protocol is safe from TA impersonation attack.
- **Pre-verification in the smart card:** In the login phase several protocols such as [30, 110, 111] does not support smart card to verify the identity and password of user. It puts an extra burden on the server. While in the proposed protocol the smart card checks $C_{u^*} = C_u, U_{i^*} = U_i$, and $P_{u^*} = P_u$ in the login phase. If it is found valid, the proposed protocol proceeds for the authentication phase. Otherwise, the session will be deferred until the right password and identity have been submitted. This means that the proposed protocol saves computational and communication expenses whether there is inaccurate input or an unlawful user. As a result, the proposed protocol successfully provides pre-verification.
- **Known-Key Attack (KKA)** If one session key is compromised, it does not necessarily mean that all other session keys would be as well. The accepted session key in the proposed protocol is based on three random ephemeral secrets N_u, N_{TA} and N_m , which are different for each session. Due to the difficulty of the ECDLP problem, the adversary may not be able to derive all of these at the same time. As a result, revealing one session key does not allow the adversary to learn about additional session keys. Sometimes researchers call it “No key control property”.
- **Replay Attack (RA)** In the authentication phase, we have used

timestamps TS_u, TS_m, TS_{TA} , and accepted delay (δ) is sufficiently tiny, which makes replaying of old messages useless. Hence, our protocol is secure against replay attacks.

In Table 3.2, the summary of the security features of recently published protocols and proposed protocols is given.

3.5 Summary

This chapter first discusses crucial role of IoT devices in our daily lives, the advantages of using cloud computing in IoT devices, and authentication requirements in such an environment. Efficient authentication is the need for the hours for IoT devices. The proposed protocol is computationally very light and successfully resists attacks that are not covered by the currently existing protocol. Elliptic curve discrete logarithm problem (ECDLP) is used with one way hash function and XOR operator. ECDLP property makes the proposed protocols hard to break. The use of one way hash function and XOR operator maintains the efficiency of authentication as well as secrecy. The proposed protocol is verified using BAN logic and simulated using HLPSL language for the AVISPA tool. We have added essential tricks to play with BAN logic and the AVISPA tool for any protocols related to the secure use of IoT devices. The generalized approach of the system model makes the proposed protocol implementable for the different scenarios of IoT devices such as Medical IoT, Industrial IoT, and cyber-physical systems. The proposed protocol can be extended for healthcare IoT devices and Industrial IoT by incorporating novel biometric, homomorphic encryption, and iterative learning techniques

Chapter 4

A GROUP BASED SCHEME FOR IoT ORIENTED INFRASTRUCTURE

Group-oriented communication, such as data gathering and area monitoring, is critical in the IoT World. It enables the users to manage various IoT devices simultaneously. Conventional one-to-one authentication techniques do not consider the resource constraints of IoT devices in grouped communication. They also do not solve the issue of Massive Machine-type Communication (mMTC) scalability. Many to Many (M2M) authentication approach of group authentication makes group oriented communication and mMTC very secure. The lower time complexity of Group-based authentication (GBA) makes these protocols very popular for efficient and secured communication. This Chapter uses a polynomial-based group authentication scheme and membership verification to ensure efficient and threat-free communication among IoT devices. Bi-variate polynomials have been used instead of single variable functions in the proposed scheme. The protected nature of the bi-variate polynomial makes the proposed scheme very secure and reliable. Furthermore, establishing the session key makes the proposed scheme effective and efficient. Security analysis of the proposed work shows its efficiency over existing schemes. In this chapter we have also included some study about smart cities and usefulness of GBA in smart city.

4.1 Introduction

Without a broadly agreed-upon definition, the smart city sector is still in the “I’ll know it when I see it phase”. According to the Smart Cities Council (The Smart Cities Council works globally across sector divides to make the world safer, more activated, beautiful, sustainable, equitable and resilient for everyone), a smart city is one where digital technology is incorporated throughout all city functions [112]. Almost all smart city sectors use the Internet of Things (IoT) as an easy and efficient tool for Intra and inter-functionalities. From Fig. 4.1., we can easily conclude that Smart cities are the super application domain of IoT. Fernandez-Anezan [113] analyzes the various descriptions of a smart city. Luong et al. [114] analyze the economical pricing policies and their relationships in communication and data collecting for IoT. In contrast, Arasteh et al. discuss the smart city and IoT relationship [115, 116]. From industrial automation to health care, IoT devices have become an integral part of almost all activities of smart cities. Security is needed at every user hierarchy level, such as secure booting, access control, update, and patching. To assure security, authentication is mandatory for all sectors of IoT-enabled smart cities [3]. Several research papers have recently been published that deal with traditional IoT authentication [33, 35, 39, 41]. Traditional authentication mechanisms are not scalable for densely deployed IoT networks containing millions of nodes expected to be operational. To assure security, authentication is mandatory for all sectors of IoT-enabled smart cities [3]. Several research papers have recently been published that deal with traditional IoT authentication [33, 35, 39, 41]. Traditional authentication methods that follow the establishment of the session key are not scalable for densely deployed IoT networks, where millions of nodes are expected to be operational.

The uses of IoT devices are increasing day by day leads to the exponential growth of data and devices. Security is needed at every user hierarchy level, such as secure booting, access control, update, and patching. Due to the massive data interchange, the proliferation of IoT devices in smart cities has resulted in several performance concerns, including excessive latency and network congestion. Many applications such as supply chain management,

smart energy grids, area monitoring, flood sensing, fire alarm, and many more are based on Group-oriented communication [117]. Authentication in IoT systems, in particular, is critical for smart cities and must be accessible, secure, and quick. Harn et al. [49] proposed Group Based Authentication (GBA) to authenticate members in group-based communication. GBA is one of the authentication solutions, such as massive authentication requests to the authentication server and congestion control. GBA1 is for synchronous, and GBA2 is for asynchronous communication. Su et al. [50] compared the existing schemes and conclude that Communication complexity is reduced in GBA. Group-based authentication plays a vital role in the case of a large number of nodes. In 1979, Adi Shamir [48] came up with the idea of the Secret Sharing Scheme (SSS). In SSS, a secret key is distributed among the members of a group in the form of a unique shadow (token) such that in a later stage, a certain number of members can reconstruct the secret using their tokens without the involvement of an authentication server. However, tokens are disposable after participating in secret regeneration in the case of GBA1. Similarly, an adversary can recollect the tokens from the network and later can perform attacks such as spoofing attacks [51]. Chien et al. [51] have used the Elliptic curve discrete logarithmic (ECDLP) to solve the problem of GBA2. Furthermore, resembling the IoT environment makes Chien's scheme insecure [118]. However, only as a pre-processing of user authentication can group authentication be used. Because it cannot identify non-members. To identify non-members, additional one-to-one user authentications are required known as membership authentication [52, 53, 119].

In group based membership communication, one of the most critical aspects of the communication between the trusted authority and the participants is using private channels. A private channel multiplies the latency and is prone to several attacks, such as man-in-the-middle attacks and spoofing attacks. Insider adversary is also one of the problems in the attack-free implementation of group-based membership authentication. Primary contributions of this chapter are mentioned below in light of these challenges:

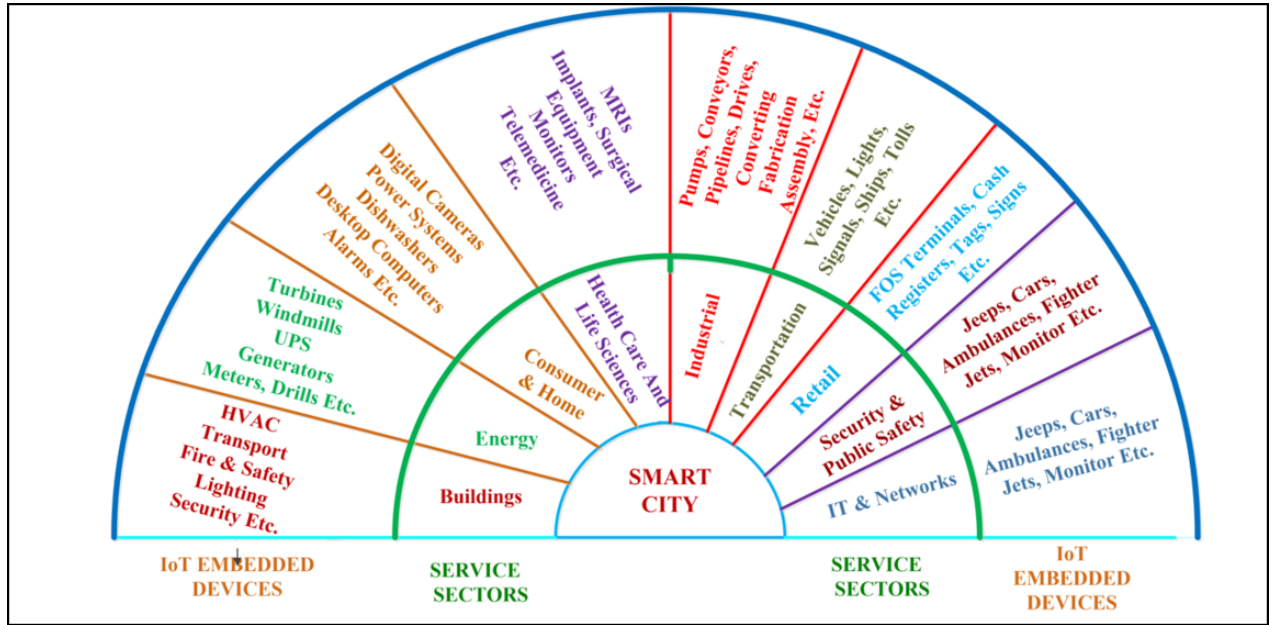


Figure 4.1: smart City and IoT World

- Proposed scheme (PS) is a scalable, lightweight authentication scheme that can be deployed in centralized or distributed group authentication scenarios to overcome possible pitfalls in group authentication.
- This scheme provides authentication among the members and generates a session key for uninterrupted communication.
- Due to resource - constrained nodes in IoT scenarios, lightweight schemes are mandatory, and it is tried to keep the proposed scheme simple, more flexible, and lightweight than the existing schemes.
- one unique property of the proposed scheme is that shares generated by Trusted Authority can serve two purposes that are: 1. To reconstruct the secrets 2. To establish secret communication keys for shareholders.
- Proposed scheme uses bi-variate polynomial as in [55, 56, 120], which makes this schemes very light as compared to others because it eliminates the requirement of extra key generation for the exchange of tokens among the nodes.

4.2 Related works

Authentication is critical for IoT devices to avoid severe damage and mass destruction. Due to limitations of resources such as heterogeneity and low

power supply, an authentication mechanism must be lightweight. Researchers have used many lightweight techniques such as ECC, blockchain, hash, and XOR functions instead of heavy cryptographic algorithms [42–44]. In the context of a smart city, several devices constitute a group. Secure group communication and membership authentication is needed for hours. Recently, [45–47] have used group-based authentication in fog computing, drones network and Intelligent transportation system (ITS). Studies on group authentication are mostly based on secret sharing schemes. The secret sharing scheme was first introduced by Shamir in 1979 [48]. In 2013, Shamir’s secret sharing scheme was exploited by Harn [49] for efficient group authentication, harn proposed an idea of group authentication whose complexity ($O(n)$) is very much less than the conventional approach of authentication ($O(n^2)$) [50]. Three different group authentication schemes were put forth by Harn. If group users share their private keys simultaneously, his first scheme offers a solution. The other two schemes that Harn has suggested are made for asynchronous key sharing. Chien [51] demonstrates in his paper that Harn’s techniques are insecure and that an attacker may recover the security parameters. He proposes a brand-new system based on bilinear mapping and elliptic curve cryptography (ECC). Chien also compares communication costs between his proposal and Harn’s approach. In addition, between-node synchronization is required using a previously disclosed value when an internal group node does not participate in group authentication. Furthermore, the Harn and Chien schemes broadcast tokens to nodes participating in group authentication during authentication. This process (resembling an IoT environment) is hierarchical and does not ensure secure communication in an environment where communications are connected, and a group leader manages devices. We solve this problem by devising a group authentication scheme that operates safely in IoT communication environments but employs reusable authentication.

In group-based authentication, an adversary can pretend to be a legitimate member, or a legitimate member may act as an internal adversary. To prevent such types of attacks membership authentication has been used by several authors [52, 53] and [54]. In the case of membership authentication,

there is a need for a secure network to exchange tokens among other members to prevent attacks such as man-in-the-middle attacks and reply attacks. Setting up a secure network separately for each interchange of tokens/tokens will lead to an inefficient and uneconomical Infrastructure of IoT devices that will never suit smart cities. In present work, protected secret sharing scheme (PSSS) has been used to propose a novel scheme in which one part of the token is used to encrypt another.

In 2017, Harn proposed protected secret sharing scheme (PSSS) [55]. In PSSS, a bivariate polynomial instead of a single variable polynomial is used to avoid extra channels, variables and keys for the exchange of secrets to members of the group. Harn used PSSS for group authentication with multiple trials and multiple authentication [56]. Their scheme, however, does not integrate the new feature. Their analysis is poor and fails to consider an intelligent insider attack. Furthermore, their scheme's parameters are also unreasonable. [57]. The proposed scheme is proposed to overcome the above-discussed outcomes and match the constraints specification of the IoT devices in grouped communication. The use of hash and XOR functions with timestamps makes the proposed scheme realistic for grouped authentication. Furthermore, establishing the session key enhances its usability compared to other group-based authentication schemes.

To complete the authorization process, this article designs an authentication scheme that authenticates the group's other members and then agrees upon a common secret session key for secure communication.

4.3 Preliminaries

4.3.1 The (t, n) Threshold Scheme of Shamir

There is one secret in the Shamir Secret Sharing Scheme (SSS). Let's say it's C . C 's shadows (tokens), designated as F_1, F_2, \dots, F_n , are allocated to n stakeholders (members). A minimum k number of shadows is essential during the reconstruction phase to regenerate the secret. The scheme is known as the (t, n) threshold scheme. t is a threshold value in this scheme.

The mathematical concept behind SSS is Lagrange interpolation. Generally, Modular arithmetic is used in place of real arithmetic in secret sharing schemes to make the scheme more secure. Flow of SSS can be summarized the in the following steps:

- A prime no. M is selected, which is prime, such that $M \geq C, n$.
- A function $g(x) = a_0 + a_1x + a_2x^2 + \dots + a_{k-1}x^{k-1} \text{ mod } M$ is taken where $a_0 = C$ is the secret.
- Pair $(i, g(i))$ is generated by using $g(x)$, where $i = 1, 2, \dots, n$.
- These points $(i, g(i))$ are allocated among n participants/ members in secure manner.
- A minimum of t token holders collaborate in the reconstruction and exchange of tokens through a secure channel.

$$g(x) = \sum_{i=1}^n L_i q_i \quad (4.1)$$

where $L_i = \prod_{j=1, j \neq i}^n \frac{x - x_j}{x_i - x_j}$. From (4.1), we get

$$g(x) = a_0 + a_1x + a_2x^2 + \dots + a_{k-1}x^{k-1} \text{ mod } M$$

Therefore $a_0 = C$ is the secret. Using a secret sharing scheme in authentication would result in great time savings. Time taken by general authentication methods for large no devices is much greater than the use of secret sharing. As in Fig 4.2, for the whole process of the secret sharing scheme time taken for 16 devices is 0.006 seconds. While in case of general authentication methods total time = $16 * 0.012 = 0.092 \text{ sec}$ [39]. Although Shamir's scheme is based on future works, there exist several shortcomings, some of which are following drawbacks of Shamir secret sharing scheme.

- It works for a single secret and cannot deal with multi-secrets.
- Recreation of the token is mandatory once used.
- No communication between dealer and participants without private channel

```

Using 16 shares and a threshold of 4
Secret: I love IoT
===Shares===
bXktawQAAAAAAAAAAAAAAAAAAEAASBdU90BLZzgmxFEg==
bXktawQAAAAAAAAAAAAAAAAAAEAASCoeEE67qFYI/Mxw==
bXktawQAAAAAAAAAAAAAAAAAAEAASDouLGXLF08MwqDQ==
bXktawQAAAAAAAAAAAAAAAAAAEAASE1fSNHbfgPNVHCw==
bXktawQAAAAAAAAAAAAAAAAAAEAASFa+h/iPu574mYSA==
bXktawQAAAAAAAAAAAAAAAAAAEAASG3nhvI3l5aEzi1A==
bXktawQAAAAAAAAAAAAAAAAAAEAASHXwhHav7sIXXrww==
bXktawQAAAAAAAAAAAAAAAAAAEAASIPi8Xn9Q5mi5miQ==
bXktawQAAAAAAAAAAAAAAAAAAEAASJwDzPFBMVuVOE3Q==
bXktawQAAAAAAAAAAAAAAAAAAEAASKq1tuqhTU1w38Mg==
bXktawQAAAAAAAAAAAAAAAAAAEAASLayRs1Rgfbh9I6g==
bXktawQAAAAAAAAAAAAAAAAAAEAASM+6XKSgVZESwStg==
bXktawQAAAAAAAAAAAAAAAAAAEAASNh8X4V04RQygf5w==
bXktawQAAAAAAAAAAAAAAAAAAEAAS0jJw5xcFN4F00AQ==
bXktawQAAAAAAAAAAAAAAAAAAEAASPz5DRBEdiKDFV3A==
bXktawQAAAAAAAAAAAAAAAAAAEAASQdAw58J6Zq0Heow==
===Reconstructed with t shares===
Reconstructed: I love IoT
Time to create and reconstruct shares (seconds):      0.00600004196167

```

Figure 4.2: Total time taken in secret sharing scheme

- It is impotent to recognize the cheater or adversary.
- It aspires to the ideal situation in which each token holder has the same priority or participation in the secret reconstruction phase.

Several pieces of literature to overcome the drawbacks of Shamir's secret sharing schemes [121–123] for multi-stage and multiple secret sharing schemes. Similarly, others are used to verify the participant's tokens [124].

4.3.2 Group Based Authentication

Smart schools, smart water supply management, smart health treatment, smart waste management, autonomous transportation systems, smart grid system, and many other facilities are all part of creating a smart city. Most of these systems work in a group, making grouped communication integral to smart cities' smooth and efficient setup.

Group based membership authentication is the fundamental security services in group based communications [125–129]. Authentication and identification management, in particular, are crucial and must be simple,

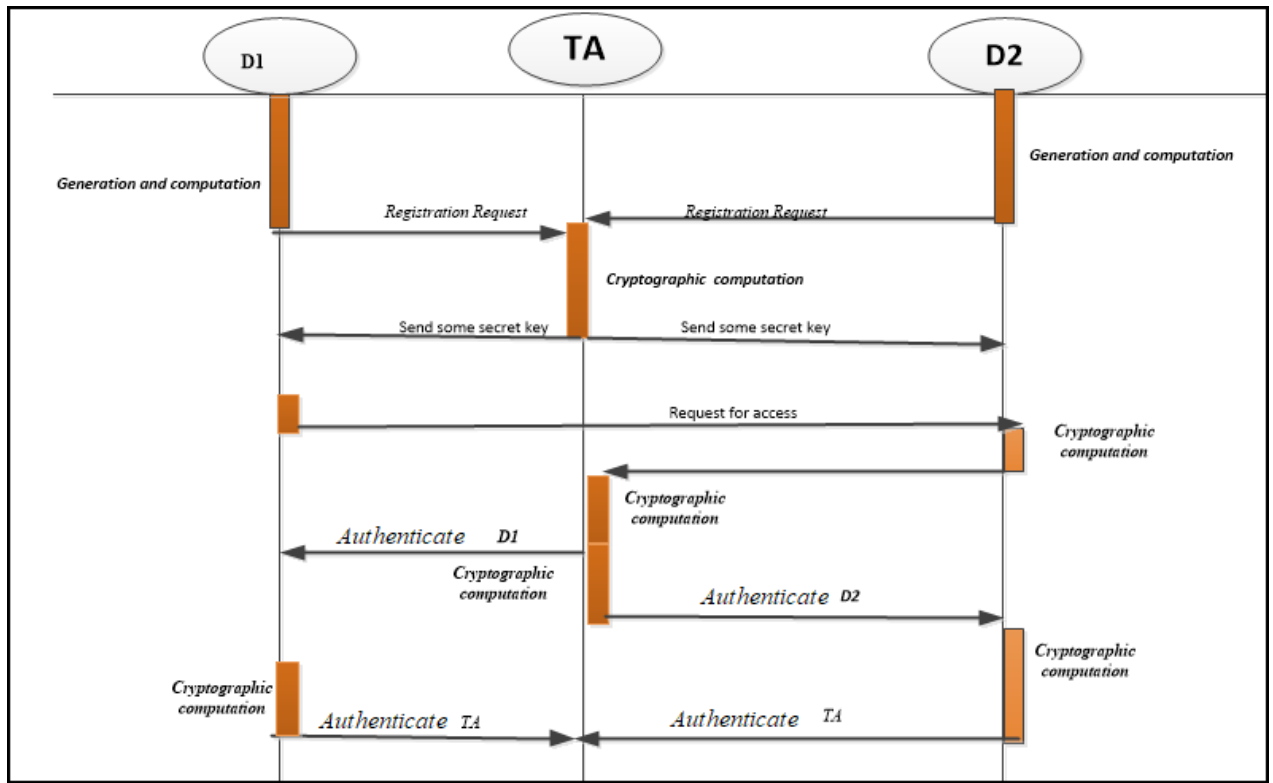


Figure 4.3: Informal authentication process.

reliable, and inexpensive. A conventional authentication mechanism has a one-to-one relationship between verifier and prover. From Fig.4.3, we may see many steps followed in conventional authentication, such as registration of IoT devices, generation of nonces, and verification techniques such as a digital signature. Each step carries cryptographic computation, which makes conventional authentication unfit for many low-powered IoT devices. On the other hand, grouped authentication consists of only three steps, i.e., distribution of tokens by a trusted authority, exchange of tokens among members of groups, and calculation of secret by each member on its end. Grouped authentication steps can be seen in Fig.4.4. It is clear that group authentication needs less computational time and is thus very suitable for low-powered devices. Grouped authentication shows far better performance when no of nodes increases [50].

Group-based authentication can be summarized briefly as follows:

- There is one Trusted authority (TA), sometimes called Group Manager (GM), to distribute tokens.

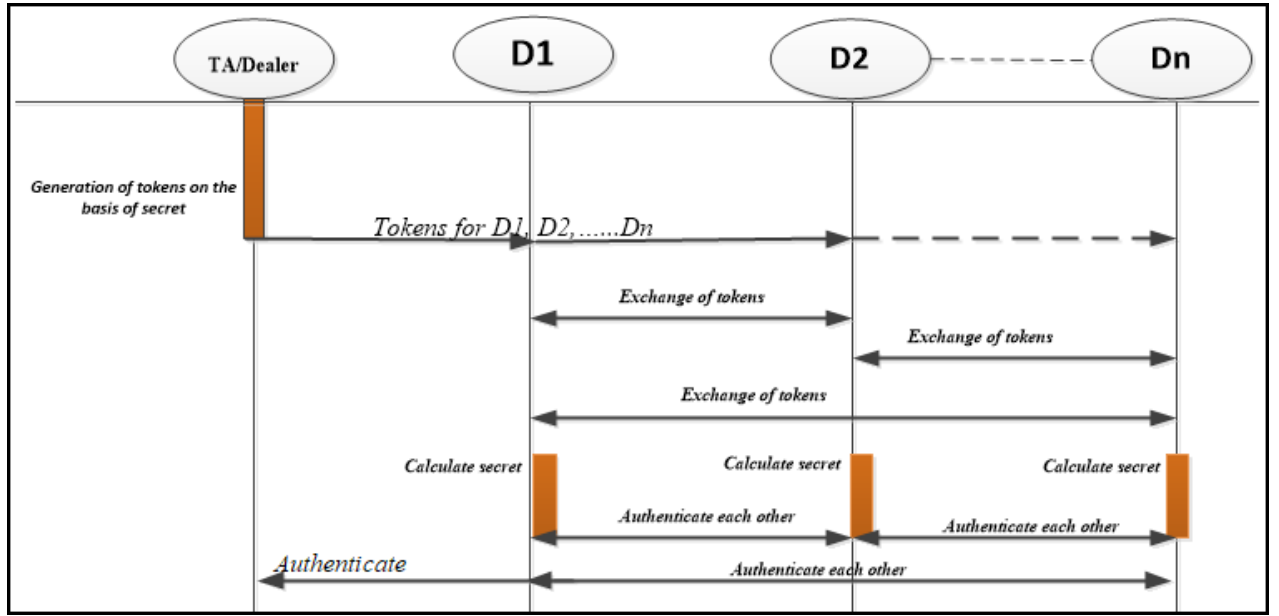


Figure 4.4: **Group-based membership authentication process.**

- To form a group, n group members register at the Trusted authority (TA)
- In registration phase, TA selects a random polynomial $g(x)$ with $g(0) = C$, with $(t - 1)^{th}$ degree (where $t \leq n$).
- TA computes secret tokens for members as $y_i = g(x_i)$.
where x_i denotes the public information for member U_i .
- Each member U_i receives their token y_i from TA. The secret is released by masking the one-way hash function $H(c)$.
- Each user releases the token obtained from the TA during the authentication phase. If all of the released tokens are legitimate, the polynomial $g(x)$ can be reconstructed and the secret obtained by interpolating the released tokens. Hashed form of this obtained value is compared to the already public $H(C)$ value. If the result is the same, then all nodes authenticate each other. Otherwise, there is a chance of an adversary.

4.3.3 One-way Cryptographic Hash Function

A lightweight scheme designer must address the trade-off between security, costs, and performance. Mostly, authentication schemes use the hash function

as one of the core parts to make their schemes efficient [130–132]. Detailed theories related to hash functions are available in [133–135]. concluding, the following properties of the one-way hash function based on these detailed studies are:

- This function is a deterministic function

$$H : \{0, 1\}^* \rightarrow \{0, 1\}^n$$

- $y = g(x)$ (called hash digest) is produced by hash function where output $y \in \{0, 1\}^n$
- Any minor modification to the input string can result in an entirely different hash value (message digest).
- Preimage-resistance: Finding any input that hashes to any pre-specified output is computationally impossible, i.e., finding any preimage x such that $g(x) = y$ when given any y for which a matching input is unknown.
- Collision resistance: finding any two separate inputs x, x' that hash to the same output, i.e. $g(x) = g(x')$, is computationally impossible.

4.3.4 System Model

The modular architecture of IoT-based systems may vary application to applications. In grouped communication, one trusted authority (TA) is sometimes called the dealer. IoT nodes are represented as $\{U_1, U_2, \dots, U_n\}$. Each user U_i interact with another user U_j . They exchange tokens and authenticate on one to many bases. Here in our scheme, there is no need for a secure channel.

4.3.5 Adversary model

There must be an adversary model against which the scheme is safe when used for secure authentication. Dolev and Yao [97] presented an adversarial model for analyzing security protocols in 1983.

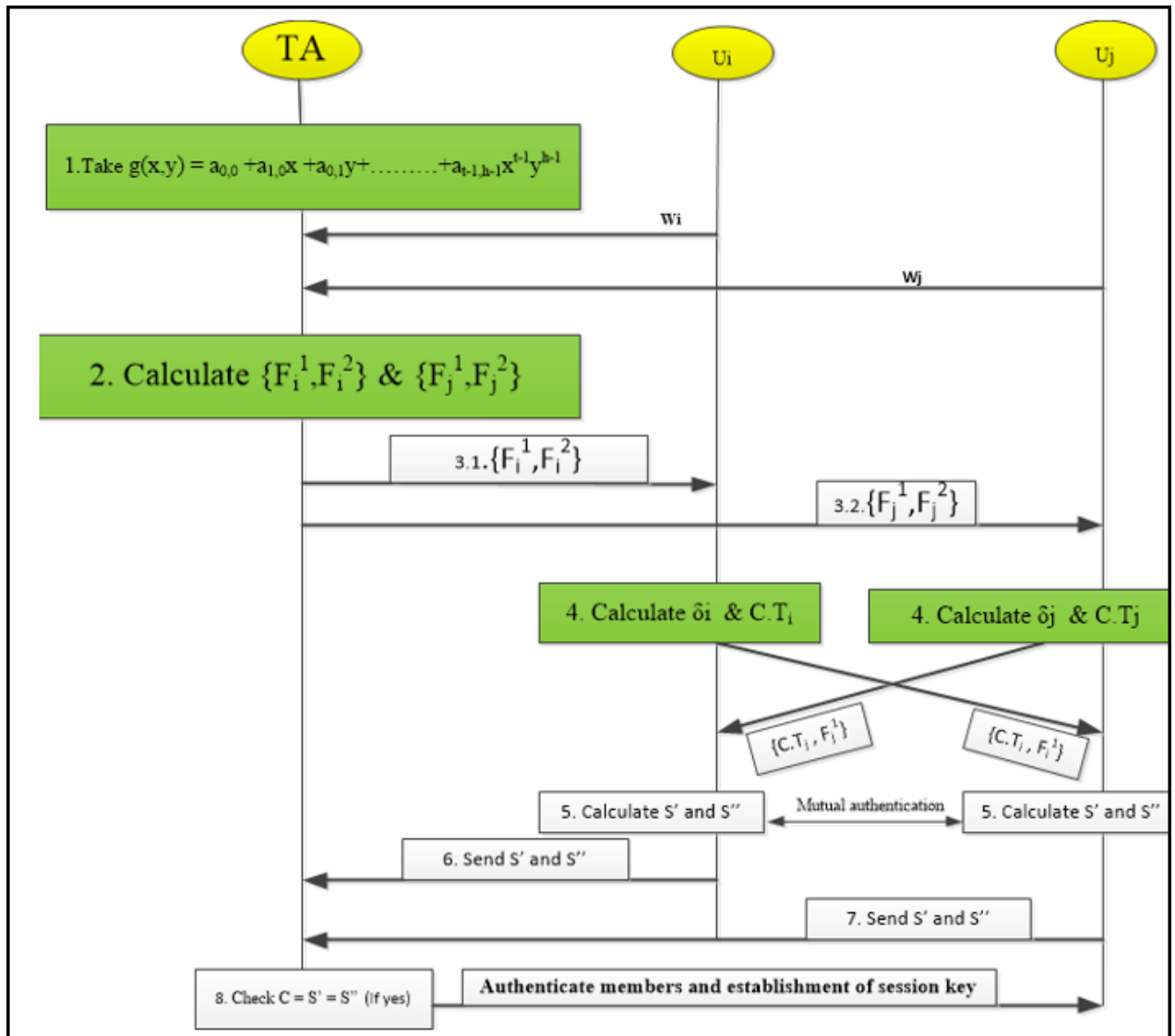


Figure 4.5: Group-based membership authentication process.

- All messages must go through the adversary.
- All messages can be read, altered, and redirected by an adversary. However, encryption works like a black box.
- If an adversary has the right keys, she can only perform decryption.
- She can only compose messages between new messages from keys and messages that she already possesses.
- Adversaries cannot perform any statistical or other cryptanalytic attacks

One thing that must be noted is that adversaries can be external and internal both.

Table 4.1: Notations used in GBA

Symbol	Explanation
TA	Trusted authority
U_i	i^{th} user
U_j	j^{th} user
w_i and w_j	public information of i^{th} and j^{th} users
δ	Lagrange component of i^{th} user
P	large prime number
$H()$	Homomorphic function
TS	Time Stamp
\sum	Summation
\prod	Product
\oplus	XOR operation

4.4 Proposed Scheme

A secure channel is needed to exchange tokens among the nodes [45–47], which makes these schemes uneconomical with latency. In this work, a novel group-based authentication scheme that eliminates secure channel’s dependency is proposed. Also, members authenticate each other, and then a session key is established for future communication. In the proposed scheme, each member has mutual authentication, and each member also authenticates trusted authority. The last session key is established for uninterrupted communication.

4.4.1 Pre-deployment phase

In this phase, TA performs the following calculations:

- TA generates a master key C .
- Select a bi-variate symmetric polynomial

$$g(x, y) = a_{0,0} + a_{1,0}x + \cdots + a_{t-1,h-1}x^{t-1}y^{h-1} \pmod{P}. \quad (4.2)$$

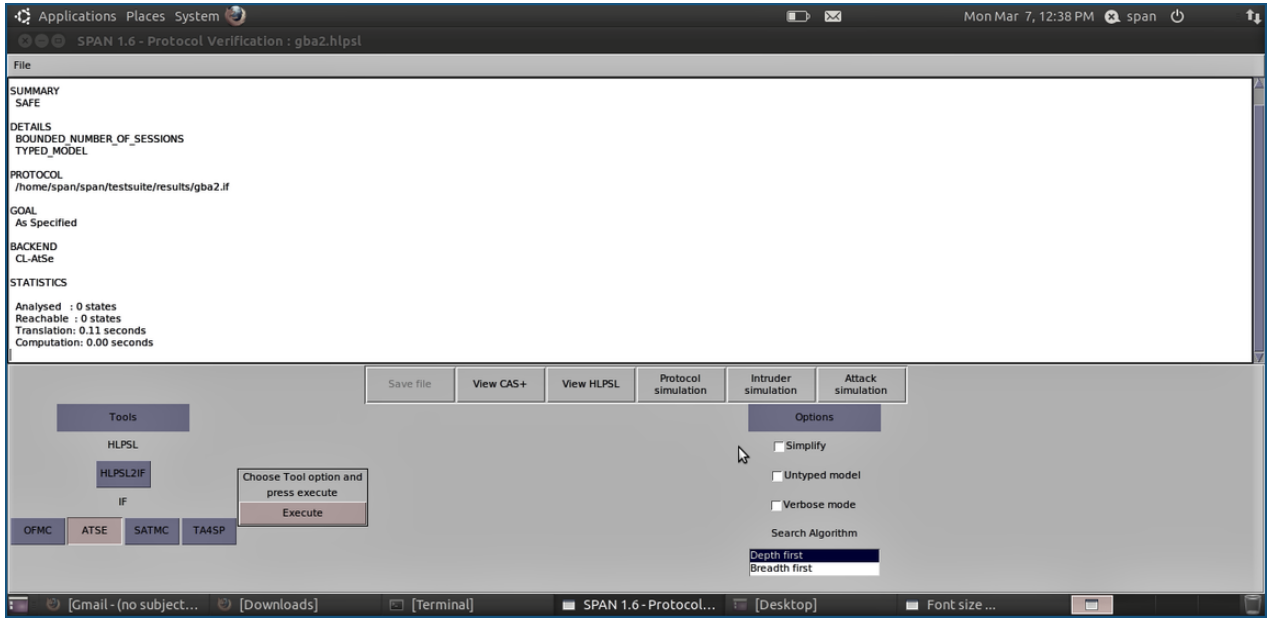


Figure 4.6: **Constraint-Logic-based Attack Searcher (CL-AtSe)**

where P is large prime number and

$$(a_{0,0} = C, a_{i,j} \in Z_p)$$

4.4.2 Registration phase

Each member of the group $\{U_1, U_2, \dots, U_n\}$ approach Trusted Authority for this they use publicly available identifiers $\{w_1, w_2, \dots, w_n\}$.

After that TA performs the following operations:

- For each member U_i , Calculate (F_i^1, F_i^2, P_i) where , $F_i^1 = g(w_i, 0)$, $F_i^2 = g(x, w_i)$. and

$$P_i = H(C || F_i^1 || F_i^2)$$

- Send (F_i^1, F_i^2, P_i) to each member U_i .

4.4.3 Authentication phase

In this phase, each member U_i authenticate other member U_j mutually. Each member authenticates Trusted Authority. In the last, each member is

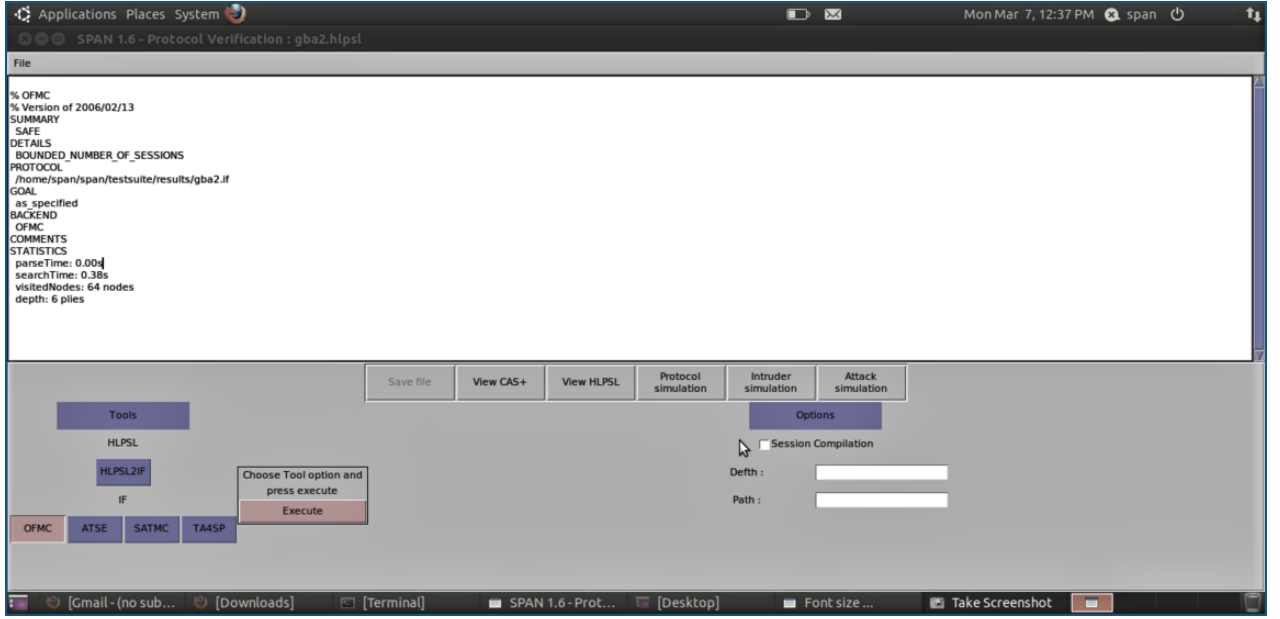


Figure 4.7: **On-the-fly Model-Checker (OFMC)**

authenticated by TA. A session key is established for further communication. U_i and U_j are two members that perform the following operations:

- U_i computes S_i'' .

$$S_i'' = \sum_{i=1}^n (F_i^1) \prod_{i=1, i \neq j}^u \frac{-w_i}{w_i - w_j} \pmod{P}. \quad (4.3)$$

- Computes $P_i' = H(S_i'' || F_i^1 || F_i^2)$.
- if $P_i' = P_i$, then U_i authenticates trusted authority.

After authenticating TA, U_i computes the following :

- U_i computes $C.T_i = \delta_i \oplus F_i^1$ where,

$$\delta_i = F_i^2(0) \prod_{j=1, j \neq i}^u \frac{-w_i}{w_i - w_j} \pmod{P}. \quad (4.4)$$

- Send $(C.T_i, F_i^1, P_i)$ to U_j .

After receiving $(C.T_i, F_i^1, P_i)$ from each U_i , U_j performs following operations

- U_j checks $TS_j - TS_i < \Delta T$, for each member U_i if 'OK' then proceed to the next step otherwise reject the authentication request.
- Each member send pair $(C.T_i, F_i^1)$ to other members separately.
- Each member authenticates TA as it is done by U_i .
- After getting pairs from all other members. Each member U_j computes

$$S'_j = \sum_{j=1}^k (\delta_j) \quad (4.5)$$

. and

$$S''_j = \sum_{j=1}^n (F_j^1) \prod_{j=1, j \neq i}^u \frac{-w_i}{w_i - w_j} \pmod{\mathbb{P}}. \quad (4.6)$$

items Each member U_j checks $H(S') = H(S'')$. and authenticate each other. Hence, membership authentication is done here.

- After authenticating each other, each member sends $H(S'_j)$ and $H(S''_j)$ to TA, TA checks the following

$$H(C) = H(S'_j) = H(S''_j) \quad (4.7)$$

- If this equation is Ok. then TA authenticates members, and the C is set as a session key for future communication. Hence the session key is established.

4.5 Security Analysis

4.5.1 Formal Analysis

To illustrate and prove the protocol's security and accuracy, any proposed protocol must be passed through formal and informal analysis. For formal analysis, we used the most common verification tool, AVISPA. The informal analysis is in the next subsection.

Table 4.2: Comparison of group authentication schemes in terms of attack resilient

Feature Comparison	Basic [49]	lee et.al [118]	wang et al. [136]	chein et al. [51]	PS
Base-system	(t, n)	(t, n)	(t, n)	(t, n) , ECDP	B.P
Resist Replay attack	×	✓	✓	—	✓
Resist Physical attack	×	×	✓	✓	✓
Resist De-synchronization	×	×	✓	×	✓
Resist MIM attack	×	×	✓	×	✓
Untraceability	×	×	yes	×	✓
freshness of authentication response	×	—	×	—	✓
Forward secrecy	×	—	×	—	✓
Backward secrecy	×	—	×	—	✓

AVISPA

To speed up the next generation of security protocols and improve their security, it is vital to have tools that support the rigorous analysis of security protocols. For that, it detects weaknesses and establishes their correctness. In 2005, A. Armando et al. [137] came up with a push-button tool for the automated validation of Internet security-sensitive protocols and applications named AVISPA. This tool is used by a protocol designer who describes a security problem in the High-Level Specification Language (HLPSL) [108]. Detailed studies of AVISPA and its execution are available in [4]. AVISPA tools provide four utilities:

- On-the-fly Model-Checker (OFMC): Performs protocol falsification and bounded verification.
- Constraint-Logic-based Attack Searcher (CL-AtSe): It can identify type flaws and manage message concatenation associativity.
- SAT-based Model-Checker (SATMC): It constructs a propositional

formula encoding a bounded unrolling of the IF's specified transition relation, the initial state, and the set of conditions denoting a breach of the security properties.

- TA4SP (Tree Automata based on Automatic Approximations for the Analysis of Security Protocols): Regular tree languages and rewriting are used to approximate attacker knowledge. Our protocol passed all four tests.

The proposed protocol easily passes OFMC and CL-AtSe as shown in Fig. 4.6 and Fig. 4.7, respectively. AVISPA tools can be downloaded at [96].

4.5.2 Informal analysis

Correctness, the freshness of authentication response, the freshness of group keys, and forward/backward secrecy are some critical security properties followed by majority group authentication protocols. The proposed scheme in this section is proven to provide these properties. Apart from supporting these security features, the proposed scheme can also support many more features, such as confidentiality, scalability, and integrity. Along with these properties, the proposed scheme is safe against various modern attacks such as replay attacks, physical attacks, man - in - the - middle attack, as discussed in the second part of this subsection.

1. **Correctness** : In authentication phase $S' = \sum_{j=1}^k (\delta_j)$ and $S'' = \sum_{j=1}^n (F_j^1) \prod_{j=1, j \neq i}^u \frac{-w_i}{w_i - w_j}$ are calculated, members are said to be correct only if $S' = S''$. non-members can not know the value of δ since it is transferred to other legitimate members in the encrypted form whose encryption key is also unknown.
2. **Forward secrecy**: Keys like $(C.T_i, F_i^1)$ can only be computed or stored by members of the secure communication group if a member leaves the group, the departing member will be unable to access the content of future conversations.
3. **Freshness of authentication response**: In the proposed scheme, all the exchangeable value depends upon the random bivariate polynomial

taken by TA. It makes S' and S'' always fresh. Hence, it is impossible to impersonate a member by recording a previously used authentication response.

4. **Backward secrecy:** If a new member joins the group, he or she will be unable to view the content of previous conversations since the keys can only be computed by members participating in the secure communication.
5. **Confidentiality:** An adversary can not calculate the session keys from the values distributed on the network by a trusted authority. So, the secret information always is confidential.
6. **Integrity:** In the proposed scheme, hashed key is used and compared that makes information protected from being deleted, modified, forged, etc, during storage or transmission.
7. **Scalability:** IoT devices can randomly join and leave the group at any time and take part in membership and group authentication.

Prevention of attacks

The proposed scheme prevents the following attacks:

- **Replay attack:** The replay attack is a strategy for obtaining the secret key by capturing packets from a specific device and analyzing them. This type of behaviour is prohibited under our scheme. The attack is also made even more difficult because only necessary components are used, which too later hashed. Regarding replay attacks, there seem to be two approaches to consider. The first is the replay of packets in which the critical parts are swapped. Because packets should be received, processed, and then deleted by the receiver, replaying these packets serves no use other than a weak effort at a denial-of-service attack. The second approach comprises replaying data packets that are headed upstream. These packets are encrypted. Thus a replay will lead to failure.
- **Physical attack:** The proposed scheme is based on partitioning the secret key into pieces so that the key can be reconstructed with the fewest

possible parts. The split sections are distributed among the members of the group. A secret key is broken into N pieces for a group of N members so that at least K components are required to reconstruct the secret key. Anything less will prevent the key from being reconstructed. An attacker will have great difficulty acquiring the secret key because he or she will need to know the number K and get at least K pieces. This means the attacker must capture K members out of the total of N . As a result, under our scheme, we may avoid keeping the entire secret key in the IoT device's memory.

- **De-synchronization attack:** In this attack, an adversary blocks the communication between the devices and the trusted authority by changing the ID's of the devices. Here in our proposed work, information exchanged does not depend on the device's Id, eliminating the chance of de-synchronization. attack [136] and [138].
- **Man-In-The-Middle Attack :** In the proposed scheme, $(C.T_i, F_i^1)$ are exchanged between each member.
A Real share is not accessible by having $(C.T_i, F_i^1)$. and getting secrets is much more difficult.
- **Untraceability:** In the proposed scheme, the trusted authority takes different bivariate polynomials after each session to generate a different shadow secret for each member. It makes shadow secrets too difficult to be traced. Furthermore, hashed form of S' and S'' makes traceability much more difficult.

4.6 Summary

The proposed scheme provides mutual authentication between each pair of members and trusted authorities, eliminating any communication breach or attack. The session key is established for quick and uninterrupted communication in the group. Thus, the proposed scheme is an ideal solution for group-based communication and perfectly suits the smart city. Furthermore, the solution for Most existing work related to group-based

authentication does not straightforwardly perform formal and informal analysis as done in the proposed manuscript. The scheme also exhibits the prevention of several modern attacks, such as reply attacks, Physical attacks, De-synchronization attacks, and man -in -the-middle attacks. While focusing on Group based communication as in smart city, we need to deal with highly digitalized devices with maximum efficiency and minimum cost in IoT infrastructure. In this chapter, the importance of IoT in smart cities is explained, as so its security. IoT devices perform group-based communication in smart cities, so the proposed scheme deals with group-based membership authentication. It provides recent compulsory security features and has less communication, storage, and computation costs than existing schemes. Alongwith formal analysis, verification from AVISPA as an informal security analysis makes this scheme very secure.

Chapter 5

AUTHENTICATION SCHEME TO ENSURE CONFIDENTIALITY AMONG IoMT

Remote patient diagnosis, medical device management, and quarantined patient observation are some of the necessary and common responsibilities in modern medical healthcare . The Internet of Medical Things (IoMT) makes this works easy and feasible. Sharing information from patients and sensors associated with the patients to doctors is always an integral part of IoMT. Unauthorized access to such information may invite adversaries to disturb patients financially and mentally; furthermore, leaks in its confidentiality will lead to dangerous health concerns for patients. While ensuring authentication and confidentiality, We must focus on the constraints of IoMT, such as low energy consumption, deficient memory, and the dynamic nature of devices. Numerous protocols have been proposed for authentication in healthcare systems such as IoMT and telemedicine. However, many of these protocols were neither computationally efficient nor provide confidentiality, anonymity, and resistance against attacks. In the proposed protocol, we have considered the most common scenario of IoMT and tried to overcome the limitations of existing solutions. Along with common scenario of IoMT, we have considered the COVID-19 in special focus. In this chapter, we have description of the system module and security analysis proves it as a panacea for COVID-19 and future pandemics.

5.1 Introduction

The novel coronavirus disease (COVID-19) has triggered an unprecedented public health crisis that has adversely affected social and economic activities, medical organizations, and our overall well-being. This crisis also exposes the vulnerability of current healthcare systems, including their over-centralization of resources, panic concerning the digitalization of healthcare, and inadequate security and privacy protections for patient data. IoMT (Internet of Medical Things) systems are excellent candidates for detecting, predicting, and maintaining track of new infectious diseases like COVID-19. IoMT is becoming more widespread and diverse day by day. The Internet of Medical Things (IoMT) offers precise surveillance using wearable health monitoring devices, Wireless Body Area Networks (WBAN), artificial intelligence (AI), and cloud-based remote health testing. Utilizing IoMT functional components, such as data collection, storage, transfer, and analytics, can help develop an early warning system to stop the spread of infectious diseases. Sensor data from end-user devices, such as mobile phones, tags, or health monitors, is collected and transferred to a cloud platform for analytics and decision-making. Using the taxonomy of IoMT mitigation, Aman et al. [139] investigated the ability of IoMT to mitigate the pandemic's severity, seriousness, or painfulness. The inclusion of recent technologies in IoMT, such as artificial intelligence and big data, has increased its effectiveness significantly. All these advancements in IoMT will be ruined if a perfect protocol or scheme is not included to make this secure and safe from adversaries. There must be a mechanism to protect all information from unauthorized access and keep them confidential. Iqbal et al. [140] , explained that the most important security feature that must be covered is authentication proceeds by confidentiality . In proposed work, we have proposed the protocol that fulfill the authentication as well as confidentiality.

In 1981, Lamport [24], developed the first password-based mutual authentication system . Various more password-based MA schemes have since been put forth . Because they relied primarily on the password, these developed protocols were, however, vulnerable to a variety of potential

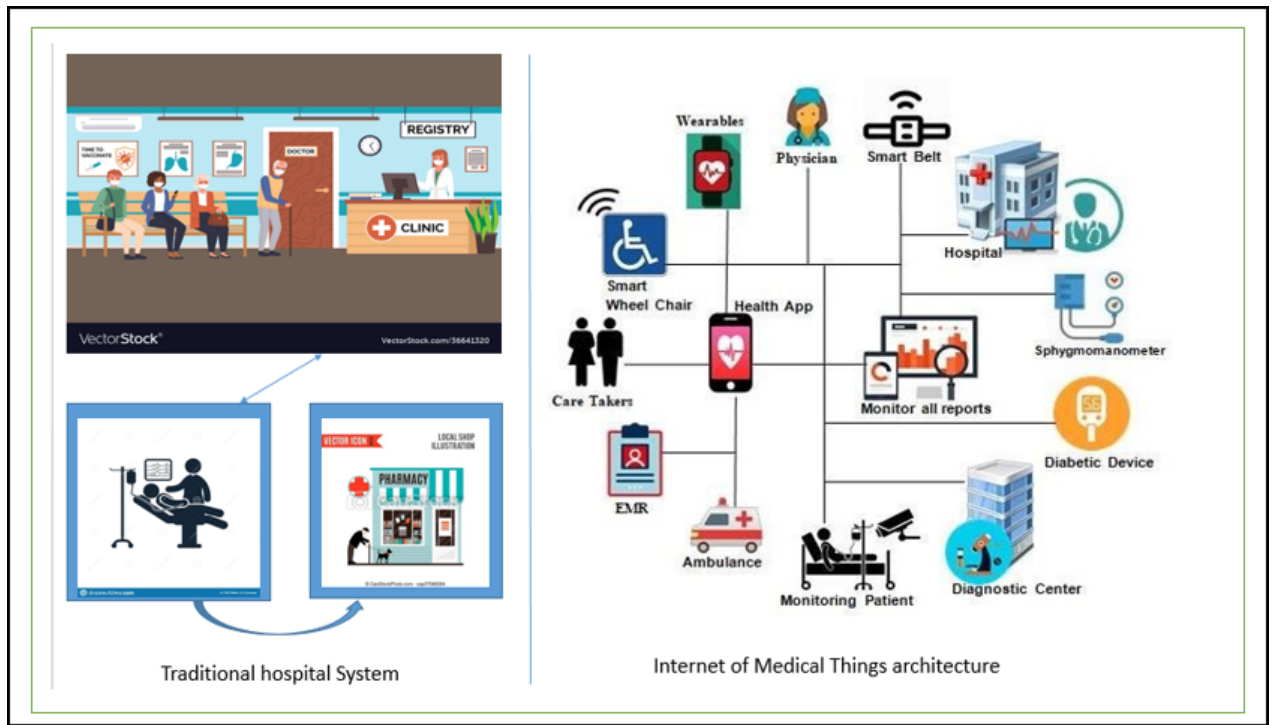


Figure 5.1: General hospital setup and IoMT

attacks, such as those from privileged insiders, impersonation attacks, and offline password-guessing attacks. The smart cards and/or biometrics [141] have been used in numerous subsequent schemes to address these security vulnerabilities. These schemes, however, keep user-sensitive data in a server database; as a result, if an adversary compromises the server-stored data, the entire system fails. For the medical IoT, several authentication protocols have been developed to preserve user privacy [142]. These protocols do not offer secure mutual authentication, untraceability, or anonymity, and they are not secure against attacks using a stolen verifier or a leaking verification table.

Considering the aforementioned issues and obstacles, the significant contributions of the proposed protocol are provided below:

- The proposed scheme is primarily focused on the IMoT and COVID-19 pandemic. All types of pandemic situations are considered while designing its network model, adversaries model, and, of course, the constraint specification of the patient and doctor.
- Proposed work will provide effective and secure anonymous authentication and confidentiality for IoMT.

- The proposed work provides a common system model that is applicable in most of the situations of the pandemic.
- The proposed protocol is resistant to various modern attack such as data thefts, phishing attacks, spoofing and denial of service attacks (DDoS attacks)
- Security analysis of proposed work compares its efficiency with existing schemes.
- Some useful tips has been shared for better understading of BAN logic and AVISPA.

5.2 Related work

IoT would have a positive economic impact of 3-6 trillion per year by 2025, with IoMT services accounting for 1-2.5 trillion of that total. [58]. Several researchers developed IoT authentication mechanisms with ample applications in almost all areas of the human race, such as agriculture and Smart Grid [61]. Jiang et al. [64], also introduced a cloud-centric key agreement and three-factor authentication approach to ensure secure access to cloud servers and autonomous vehicles . Kumar et al. [66] have recently concentrated on authentication for healthcare systems . For wireless medical sensor networks (WMSN), Wu et al. [67], created a lightweight authentication system that offers the attribute of user untraceability . Yuan et al. [68], presented a health-critical index used to ensure the transmission privilege of emergency data for intra- and inter-wireless body area networks (WBAN).Ostad-Sharif et al. [69], proposed a robust ECC-based authentication and key generation technique for healthcare applications . However, Kumari et al. [70], emphasised that due to key compromise, their protocol cannot tolerate password guessing and impersonation attacks .

Even though the aforementioned schemes are focused on IoT in healthcare. However, we require an IoMT capable of handling conditions that may arise during a pandemic, such as AI-based patient health monitoring and quick responses for both patients and hospital administrators.Fighting COVID-19

and future pandemics with the Internet of Things is the focus of a detailed analysis by Ferrag et al. in 2021 [143]. After covid-19, researchers also worked towards the area of authentication in IoMT, such as Rehman et al. [71] have focused on the attacks on the deep learning-based solution to IoMT in covid-19 but do not provide its remedies. Through XR and DNNs, Tai et al. [144], suggested a reliable and intelligent COVID-19 diagnostic IoMT. But it fails to resist against data theft and phishing attacks. Masud et al. [72], tried to overcome many attacks but did not provide a check for correctness of the data received by doctors and patient in return. With the attention of these difficulties, we have proposed a scheme that will resist all possible attacks also provide confidentiality.

5.3 Preliminaries

Before we proceed with the proposed scheme, it would be better to know about the mathematical and cryptographic concepts used in proposed protocol . Here, we have tried to make it simpler for the naive researcher too.

5.3.1 Bilinear pairing

The basics and characteristics of the bilinear pairings are described in this section. Take into account two groups G_1 and G_2 of the same prime order P , with G_1 being a cyclic additive group produced by P and G_2 being a cyclic multiplicative group. A bilinear pairing is a map

$$\hat{e} = G_1 \times G_2 \rightarrow G_2$$

It has the following properties:

- Bilinearity: $\forall M, N \in G_1, \forall a, b \in \mathbb{Z}_p^*, e(aM, bN) = e(M, N)^{ab}$
- Non-degeneracy: $\exists M, N \in G_1$ such that $e(M, N) \neq 1$.
- Computability: $\forall M, N \in G_1$, an algorithm exists to efficiently compute $e(M, N)$.

The complexity of the subsequent difficulties serves as the foundation for the computations considering the security of the proposed protocol.

Assume two groups G_1 and G_2 , of the same prime order P
 $\hat{e} = G_1 \times G_2 \rightarrow G_2$ in (G_1, G_2, \hat{e}) .

- Discrete logarithm problem (DLP): Find an integer ZP^* such that $Q = aP$, given the values of two elements $P, Q \in G_1$.
- Computational Diffie - Hellman problem (CDHP): Find the element abP , given the values of $(P, aP, bP) \in G_1$ for the integers a and b .
- Bilinear Diffie - Hellman problem (BDHP): Calculate $W \in G_2$ so that $W = \hat{e}(P, Q)^{abc}$ given the input (P, aP, bP, cP) for $a, b \in Z_p^*$.

An opponent trying to break through Identity based Cryptography (IBC) and use a digital signature must constantly find a solution to the DLP, CDHP, and BDHP difficulties.

5.3.2 Timestamp

The timestamp is digital information containing the date and time for identifying when a certain event has occurred. It is usually referred to as the digital date and time attached to digital data or documents. The timestamp is required for the assertion of proof and wide distribution for long-term storage and achieving processes. Some of the major benefits of timestamp are the following:

- To get accurate time in conformance with government guidelines.
- To get digitally signed certificates.
- To assure integrity and non-repudation.
- verifiable in future.
- In fraud detection.
- To establish accurate time in electronic notary.

5.3.3 Hash function

A block of data M with a variable length is entered into a hash function H , which outputs a fixed-size hash value $h=H(M)$. An "excellent" hash function has the quality of producing outputs that are evenly dispersed and appear random when used on a large number of inputs. Data integrity is a hash function's primary goal, in general. There is a strong possibility that changing any bit or set of bits will change the hash code. we can define it as an algorithm for which it is computationally infeasible (since no attack is more effective than brute force) to find either

- A data object that corresponds to a pre - determined hash outcome (the one-way property) or
- Identical hash results between two data objects (the collision-free property).

These characteristics make hash functions helpful in determining integrity of the data.

5.4 Modular structure of the system

The benefits of modular structures in IoMT include scalability, interoperability, customization, upgradeability, faster maintenance and repairs, increased security, and streamlined regulatory compliance. Healthcare providers may create dependable and flexible IoMT systems that improve patient care, shave time off of workflows, and boost overall efficiency in the delivery of healthcare by utilizing modular designs.

The proposed scheme is primarily focused on the IMoT and COVID-19 pandemic. All types of pandemic situations are considered while designing its network model, adversaries model, and, of course, the constraint specification of the patient and doctor. Network model and Adversary model has been described in subsections 5.4.1 and 5.4.2 respectively.

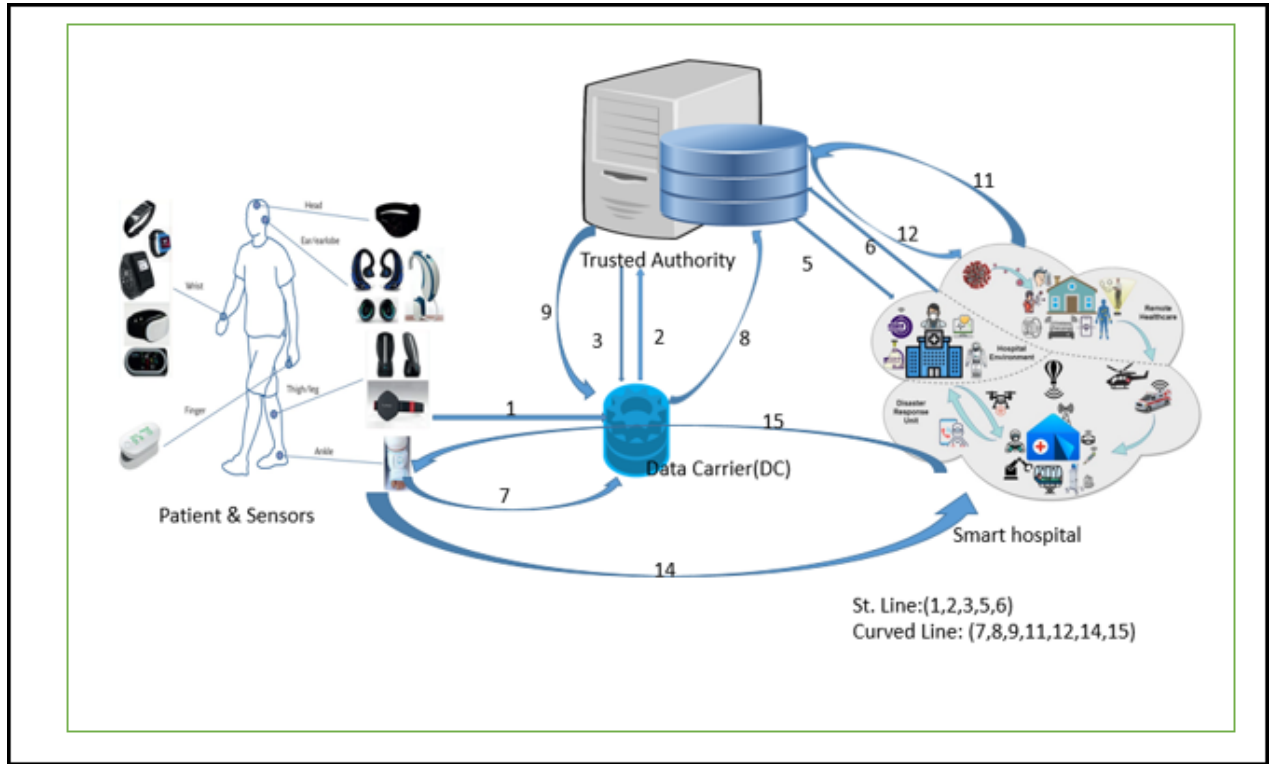


Figure 5.2: **Proposed Network Model**

5.4.1 Network model

When we concentrate on the pandemic situation, we must have a network model that should fit for maximum permutation of the arrangement among patients, doctors, sensors, and hospitals. Recently, many researchers have come up with different models that fit the particular scenario. We have proposed a network model that suits almost all situations.

Patients (P), Trusted Authority (TA), Data carrier (DC), hospital (HP), and Doctor (Doc) are the main components of the proposed network model as shown in figure 5.2.

Biological information (BI) from nearby sensors of patients, along with manual entry by patients, is stored at a data carrier(DC). Initially, patients via the data carrier and doctors via hospitals approach Trusted Authority (TA) for registration with their publicly available IDs. Both patients and doctors get some credentials for the login phase. After registration, TA authenticates the patient and doctors in the login phase. To access the patient's BI, the Doctors approach TA; TA first authenticates the doctor and shares some credentials with the doctor. A doctor approaches a patient having these credentials. DC authenticates the doctor by checking the

credentials' correctness using the bilinear pairing concept. At the same time, DC, doctors, and TA establish the session key for further smooth communication. DC uses the exact session key to maintain the confidentiality of the BI sent by DC to the doctor.

5.4.2 Adversary model

If a protocol is used for security, it must have an adversary model that it can resist. Dolev and Yao proposed a fundamental and typical adversary model in 1983 [97]. It is the most commonly accepted model. It states that an adversary can read, modify, and decrypt communications with the proper keys. Any statistical or cryptanalytic attacks by adversaries are impossible to execute.

Adversaries are increasingly more advanced and have exceptional capabilities due to the rapid advancement of technologies. We have taken into account the possibility that adversaries could leverage smart card power analysis in addition to the Dolev and Yao models to extract crucial information from stolen or lost smart cards. [98]. Furthermore, an adversary might also use a network analyzer and contemporary AI techniques to extract data from network flow.

Table 5.1: **Notations in scheme-III**

S.No	Symbol	Explanation
1.	G_1, G_2 , and G_3	Multiplicative Cyclic Groups
2.	TA	Trusted authority
3.	BI	Biological Information
4.	DC	Data carrier
5.	U_i	Patient identity
6.	D_i	Doctor's identity
7.	q	Large prime number
8.	g_1, g_2 , and g_3	Generators
9.	e	Bi-linear map

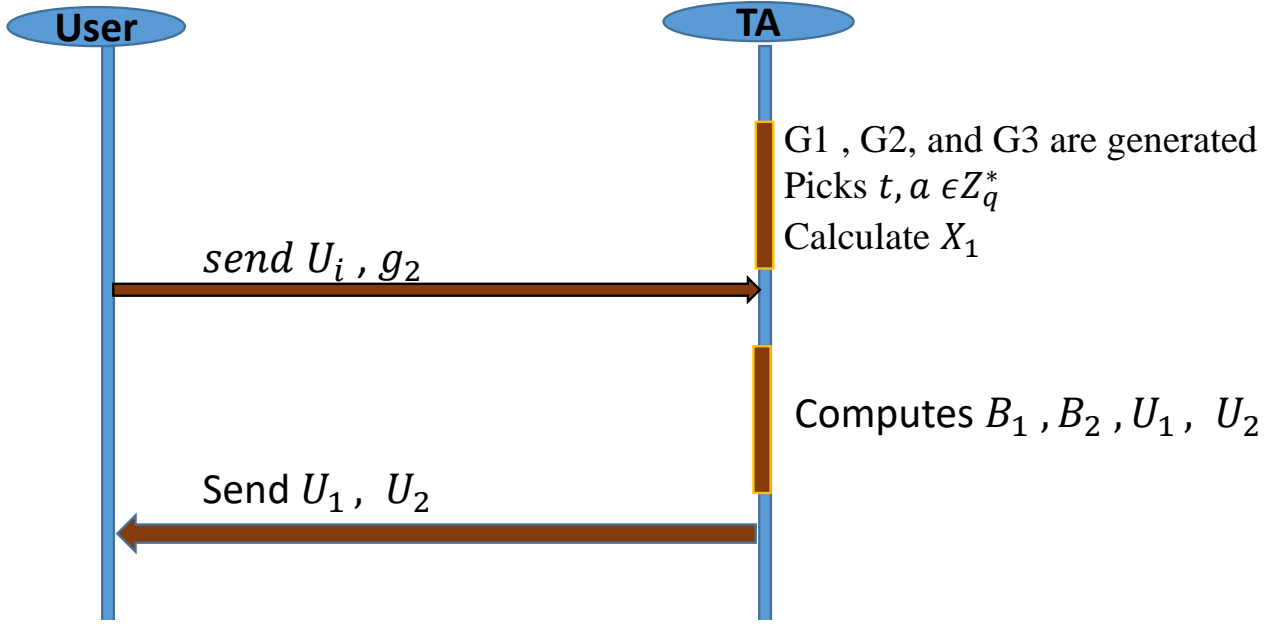


Figure 5.3: User Registration

5.5 Proposed Scheme

This section explains the proposed scheme. This section is divided into several sections, including the pre-deployment phase, registration phase, authentication phase, and confidentiality phase. We have used multiplicative cyclic groups related to Elliptic Curve (Type-A) defined in the Pairing-Based Cryptography (PBC) Library [145]. There are three main components of the proposed scheme viz. user, doctor/hospital, and trusted authority as discussed in the network model. A session key is established in the authentication phase and same key is used for maintaining confidentiality. The following are the presumptions we've made:

- Data carrier node (user), Doctor, and TA can perform similar cryptographic operations.
- While the trusted authority has no computational or storage limitations, the Doctor and the Data carrier node are resources constrained.
- Trusted authority (TA) is trustworthy and cannot be tampered with.
- After registration, messages are transported over a public channel; registration itself takes place over a secure channel.

5.5.1 Pre-deployment phase

To preserve the system's security, the TA generates the initial system settings using the steps below and updates them throughout this phase.

- Multiplicative cyclic group G_1, G_2 and G_3 are generated based on elliptic curve.
- TA picks a random number $t \in Z_q^*$.
- TA picks a random number $a \in Z_q^*$.
- TA calculates $X_1 = g_1^a$ where g_1 is the generator of the cyclic group G_1 .
- TA calculates $X_1 = g_1^a$

5.5.2 User Registration

- User send its id and generator (U_i, g_2) to TA.
- TA computes private key $B_1 = g_1^{t+U_i}$
- TA computes public key $B_2 = g_1^{a+t-U_i}$
- TA also calculates Authentication parameter $U_1 = g_2^{\frac{1}{a+2t}}$ and send $U_2 = h(U_1 || U_i)$ to Data carrier.

5.5.3 Doctor Registration

- A particular doctor D_i , send his id along with generator (d_i, g_3) to TA.
- TA computes $D_1 = g_1^{a+d_i}$, $D_2 = g_1^{a-d_i+t}$ and $D_3 = g_3^{\frac{1}{2a+t}}$.
- TA send D_3 to doctor particular doctor D_i .

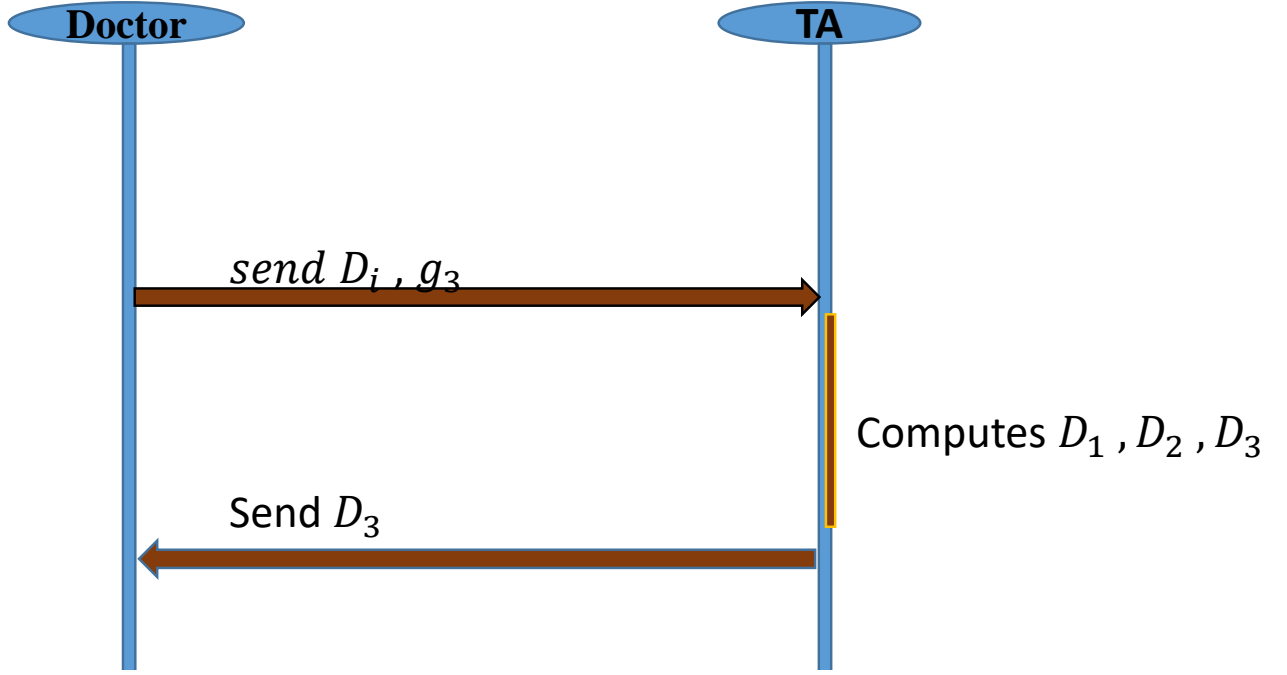


Figure 5.4: Doctors Registration

5.5.4 Authentication

- In first step, user login in the Data carrier (DC) with its Id U_i , DC computes $U_2^* = h(U_1 || U_i)$, if $U_2^* = U_2$ then proceed for authentication otherwise generates beep for wrong user

- DC generates a nonce $U^1 \in Z_P$ send U^1 and U_2^* to TA

- TA verifies time stamp, and $U_2^* = U_2$

- TA generates a random number T^1 and calculate $T_u = h(B_1 || B_2 || U^1 || T^1)$ and send to doctor.

At the same time doctor send D^1 to TA, TA computes $T_D = h(D_1 || D_2 || D^1 || T^1)$ and send to user.

Doctor also computes $SK_D = (U^1 \oplus T^1) \oplus D^1$ and send to TA.

When the doctor want to know the situation of patient , it need to contact DC through TA, So, TA compute $SK_{TA} = (D^1 \oplus T^1) \oplus U^1$, if $SK_D = SK_{TA}$ (Doctor is authenticated by TA) then doctor is permitted to access DC.

Doctor provide (B_1, B_2) to DC, DC check or authenticate doctor by :

$$e(B_1 \times B_2, U_1) = e(g_1, g_2)$$

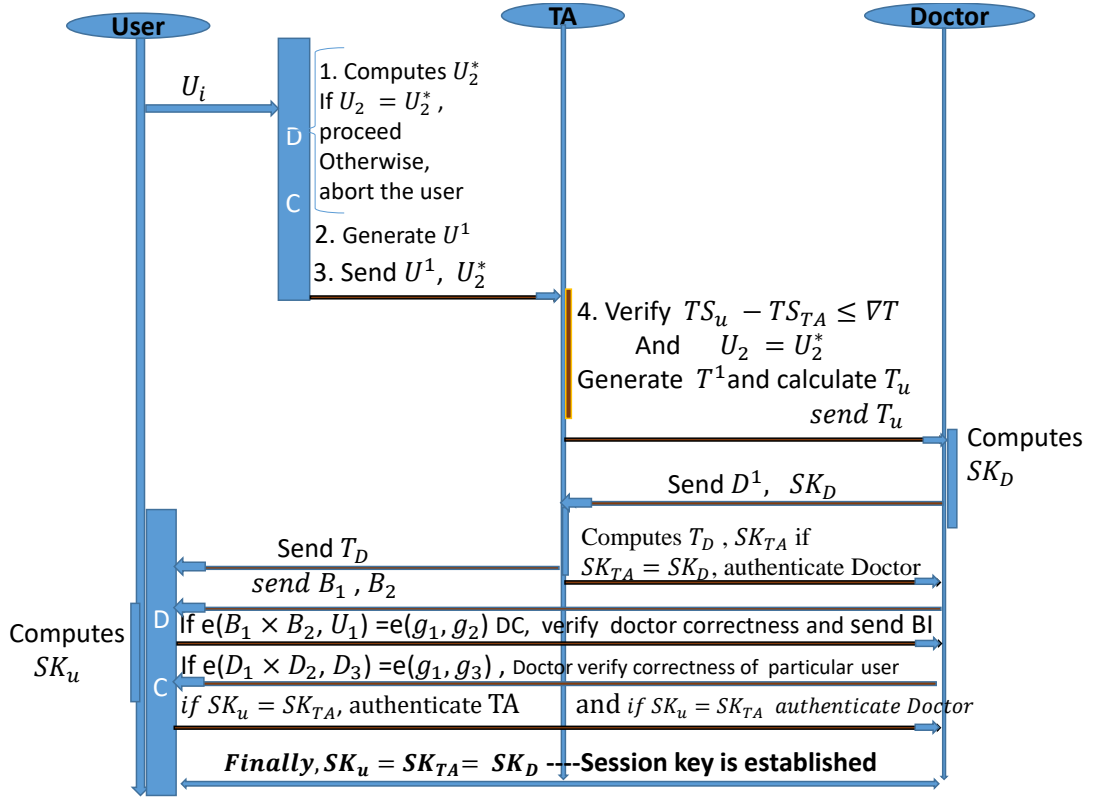


Figure 5.5: Authentication in IoMT

also DC calculates

$$SK_u = (T^1 \oplus U^1) \oplus D^1$$

. DC Checks $SK_u = SK_D$ and $SK_u = SK_{TA}$ (user authenticate the trusted authority and doctor) After this step DC send biological information (BI) of the patient to doctor. similarly, DC send T_D to doctor, Doctor authenticate particular DC/user by following result:

$$(D_1 \times D_2, D_3) = e(g_1, g_3).$$

finally session key $SK_u = SK_D = SK_{TA}$ is established for further uninterrupted communication.

5.5.5 Confidentiality

After success full mutual authentication, DC sends encrypted Biological information (BI) to doctor. and Doctor decrypt the BI by using following mechanism.

- DC put time stamping parameters with BI.
- DC calculates $CPT = h((BI \oplus SK_u) \oplus U^1)$ and send CPT to

Doctor/hospital management.

- Doctor/hospital management decrypt BI using following mechanism
- verifies time stamping and then perform decryption.

$$BI = (CPT \oplus SK_D) \oplus U^1$$

5.6 Security Analysis

When we talk about the comparison, we need to concentrate on the same field of application. The proposed protocol has been compared with those only concerned with medical IoT (MIoT) and healthcare infrastructure. For clear observation, we have divided our whole analysis into two subsections viz. security analysis and performance analysis.

5.6.1 Formal security analysis using BAN logic

Some useful tips alongwith introduction has been already written in section 3.5 of Chapter 3. Major objective is to assure mutual authentication among users (U), doctors (D), and trusted authorities (TA). The user, the doctor, and the TA all exchange authentication information. It establishes a session key (SK) for future communication. To fulfil this goal proposed protocol must satisfy the following:

1. $G1 : U \mid \equiv U \stackrel{SK}{\longleftrightarrow} D$ (U believes that U and D share the same session key SK).
2. $G2 : U \mid \equiv D \mid \equiv U \stackrel{SK}{\longleftrightarrow} D$.
3. $G3 : D \mid \equiv U \stackrel{SK}{\longleftrightarrow} D$
4. $G4 : D \mid \equiv U \mid \equiv U \stackrel{SK}{\longleftrightarrow} D$.
5. $G5 : U \mid \equiv U \stackrel{SK}{\longleftrightarrow} TA$.

Step2: Proposed protocol is idealized and written in the form of formal logic:

- $M1 : U \rightarrow TA; U^1, U_2^*, g_2.$
- $M2 : TA \rightarrow U; U_2$
- $M3 : D \rightarrow TA; d_i, g_3, SK_D$
- $M4 : TA \rightarrow D; T_u, SK_{TA}.$
- $M5 : D \rightarrow DC(U); B_1, B_2, SK_U.$

Step3: Identify the assumptions which show the initial state of the proposed protocol:

- $A1 : U \models \#(U^1). \text{ (U believes fresh } U^1).$
- $A2 : TA \models \#(T^1)., A3 : TA \models \#(t).$
- $A4 : TA \models \#(a)., A5 : D_i \models \#SK_D.$
- $A6 : U \models \#SK_{TA}., A7 : TA \models \#SK_{TA}.$
- $A8 : DC \models \#SK_u., A9 : U \models U \xleftrightarrow{SK_u} D.$
- $A10 : D \models D \xleftrightarrow{SK_D} TA, A11 : TA \models U \xleftrightarrow{SK_u} D$
- $A12 : TA \models U \xleftrightarrow{SK} D, A13 : TA \models TA \xleftrightarrow{SK} D$

Step4: Using BAN logic rules (Seeing rule, message meaning rule, freshness conjunction rule, belief rule, nonce-verification rule, jurisdiction rule and session key rule) messages are analysed with assumptions and reach to the specific goal.

Applying Seeing rule on $M1$ we get $S1 : TA \triangleleft U^1, U_2^*.$

Applying message meaning rule on $S1$ and $A11$, we get $S2: D \models U^1$

Applying freshness conjunction and nonce-verification rule on $S2$ and $A2$, we get $S3: D \models U \models U^1.$

Applying jurisdiction rule rule with $A14$ and $S3$, we get $S4: D \models U^1.$

Applying session key rule with $A2$ and $S3$ we get, $S5: U \models U \xleftrightarrow{SK} D \text{ (3rd Goal } G_3).$

Applying nonce-verification rule with $A2$ and $S3$, results $S6: D \models U \models U \xleftrightarrow{SK}$

D (4^{th} Goal G_4)

Applying freshness conjunction on A6 and A9, we get S7: $U \models U \stackrel{SK}{\rightsquigarrow} D$ (1st goal G1)

Applying nonce verification and session key rules on S7 and A6, we get S8: $U \models D \models U \stackrel{SK}{\rightsquigarrow} D$. (2nd goal (G2)).

Applying session key rule on A7 and A11, we get S9: $U \models U \stackrel{SK}{\rightsquigarrow} TA$ (5th goal (G5)).

Protocol validation using AVISPA

To accelerate the formulation of the next generation of security protocols and enhance their security, it is essential to have tools that enable a thorough analysis of existing security protocols. It achieves this by identifying flaws and demonstrating their accuracy. We have analyzed the proposed scheme with AVISPA (Full description can be found in chapter 3 and 4.) All four AVISPA tests were passed by our protocol.

5.6.2 Protocol validation and verification using SCYTHERR

Here, we use the Scyther tool (The latest stable version of Scyther is v1.1.3, which was released on April 4, 2014.) to verify the proposed scheme formally [146]. It is intended to automatically analyze, falsify, and verify the security protocol's attributes. In comparison to other simulators, the Scyther tool has more features. The Scyther tool assumes that perfect cryptography is used, meaning that a message cannot be deciphered from the ciphertext by someone who does not possess the encryption key. Dolev - Yao's adversary model and pattern refining technique are used by this tool. The following innovative features are present in this tool:

- With this tool, We may assess a protocol's security for both an unbounded and bounded number of sessions.
- The security of a protocol against various attacks can be evaluated using this tool.
- It is to validate both user-defined and automatically generated claims.

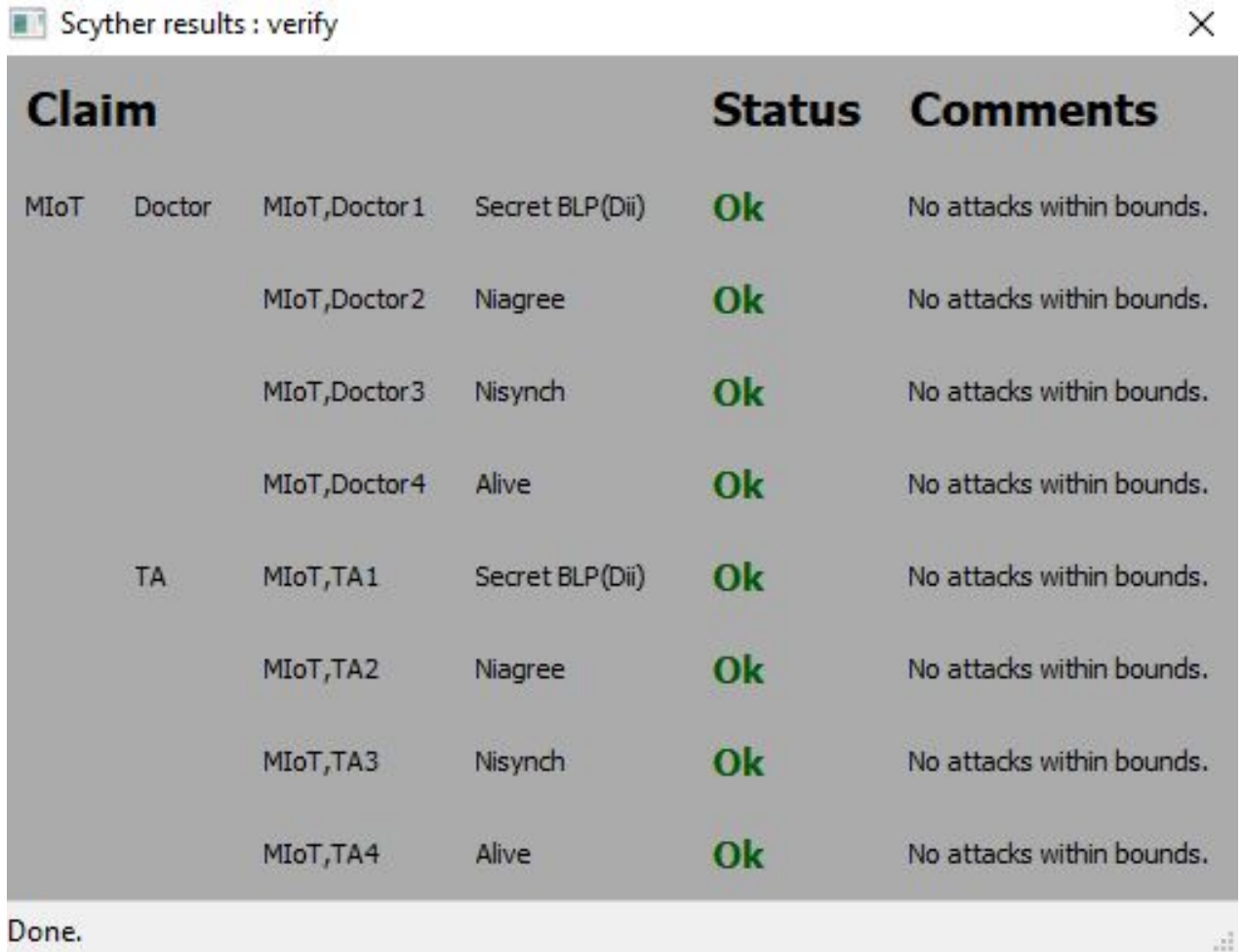
Claim				Status	Comments
MIoT	User	MIoT,User1	Secret BLM(ui)	Ok	No attacks within bounds.
		MIoT,User2	Secret XOR(BLM(ui),ki)	Ok	No attacks within bounds.
		MIoT,User3	Niagree	Ok	No attacks within bounds.
		MIoT,User4	Nisynch	Ok	No attacks within bounds.
		MIoT,User5	Alive	Ok	No attacks within bounds.
	TA	MIoT,TA1	Secret BLM(ui)	Ok	No attacks within bounds.
		MIoT,TA2	Secret Hash(Concat(ui,vi))	Ok	No attacks within bounds.
		MIoT,TA3	Niagree	Ok	No attacks within bounds.
		MIoT,TA4	Nisynch	Ok	No attacks within bounds.
		MIoT,TA5	Alive	Ok	No attacks within bounds.

Done.

Figure 5.6: Scyther results for authentication between User and Trusted Authority

- With the help of this tool, it is possible to ensure termination while analyzing a protocol using infinite sets of traces.

Python was used to develop the Scyther tool. To create a protocol that may be utilized with the Scyther tool, one must use the Security Protocol Descriptive Language Security Protocol Descriptive Language (SPDL). We have used a Graphical User Interface Graphical User Interface (GUI) for this purpose. This prepares the verification results and, when attacks are detected, a visual representation of the attack Scyther found on the scheme. We created our authentication phase in SPDL language to simulate the suggested scheme against the Scyther tool. Figures. 5.6, 5.7 and 5.8 illustrate the simulation output. Our protocol is secure, according to the simulation results.



Scyther results : verify

Claim				Status	Comments
MIoT	Doctor	MIoT,Doctor1	Secret BLP(Dii)	Ok	No attacks within bounds.
		MIoT,Doctor2	Niagree	Ok	No attacks within bounds.
		MIoT,Doctor3	Nisynch	Ok	No attacks within bounds.
		MIoT,Doctor4	Alive	Ok	No attacks within bounds.
TA		MIoT,TA1	Secret BLP(Dii)	Ok	No attacks within bounds.
		MIoT,TA2	Niagree	Ok	No attacks within bounds.
		MIoT,TA3	Nisynch	Ok	No attacks within bounds.
		MIoT,TA4	Alive	Ok	No attacks within bounds.

Done.

Figure 5.7: Scyther results for authentication between Doctor and Trusted Authority

Informal Security analysis

In consideration of Covid-19, the proposed system is capable of resisting new attacks and provide security features which are mentioned following

- **Anonymity and Un-traceability:** The identity of the Patient and doctor must not be revealed during the exchange of keys among the Patient, Doctor, and trusted authority. Fresh nonces are generated by patients, doctors, and trusted authorities. In the registration phase of the Patient and doctor, TA calculates B_1, B_2, B_3 and U_2 for a patient using the generator of the group based on the Elliptic curve. Similarly, D_3 is generated for a doctor. Hence, it is evident that extracting information about the patient and doctor's identity is impossible by a third party. So, user anonymity and the un-traceability are facilitated by the proposed protocol.
- **Offline Guessing Attacks (OGA):** Differential power analysis attacks may

Scyther results : verify					
Claim				Status	Comments
MIoT	Doctor	MIoT,Doctor 1	Secret BLP(Di)	Ok	No attacks within bounds.
		MIoT,Doctor 2	Secret XOR(BLP(Di),bi)	Ok	No attacks within bounds.
		MIoT,Doctor 3	Niagree	Ok	No attacks within bounds.
		MIoT,Doctor 4	Nisynch	Ok	No attacks within bounds.
		MIoT,Doctor 5	Alive	Ok	No attacks within bounds.
User		MIoT,User 1	Secret BLP(Di)	Ok	No attacks within bounds.
		MIoT,User 2	Secret Hash(Concat(mi,ni))	Ok	No attacks within bounds.
		MIoT,User 3	Niagree	Ok	No attacks within bounds.
		MIoT,User 4	Nisynch	Ok	No attacks within bounds.
		MIoT,User 5	Alive	Ok	No attacks within bounds.
Done.					

Figure 5.8: **Scyther results for authentication between User and Doctor**

be the source to extract information from devices such as smart card and data carrier. The proposed protocol's parameter $U2$ was created by hashing together two words that were derived using an elliptic curve generator. The hash function's one-way collision resistance property and the ECC's uniqueness make it very difficult to learn a user's identity. Similar, consecutive steps used in registration eliminate the chance of power analysis attacks.

- Perfect Forward Secrecy (PFS) Adversaries can easily obtain some keys and parameters. PFS makes sure that all session keys between patients, doctors, and trusted authorities are kept secret from adversaries. Here in the proposed protocol, assume an adversary wants to compute $SK_u = SK_D = SK_{TA} = (D^1 \oplus T^1) \oplus U^1$. Because they are always used in hashed situations, these three parameters are unavailable to the attacker.

This problem has a tough time finding a polynomial-time solution. The proposed approach can therefore offer perfect forward secrecy.

- Sybil Attack (SA): A Sybil attack includes an adversary establishing numerous accounts or nodes to dominate the network. The proposed protocol's registration and initial authentication stage involve the TA's elliptic curve and its generators. As a result, the ECDLP characteristic of ECC completely removes the possibility of a private computing key from known parameters. Thus, the harm caused by many accounts is unaffected by the uniqueness of keys.
- Known Session-Specific Temporary Information attack (KSTIA): In the KSTIA attack, the adversary is given access to ephemeral session secrets; with this information, the adversary can obtain the session keys. Nearly all data in the proposed protocol is hashed and concatenated with the private key. Extraction of information from transient data is quite tricky. Ephemeral Secret Leakage (ESL) attack is the name some researchers give to this attack.
- Privileged Insider Attack (PIA): Outside adversaries and internal adversaries are two types of adversaries that may always exist in a system. An adversary from the inside might just have privileged access to TA. In this case an adversary can get information such as U_2 and D_3 but $U_2 = h(U_1 || U_i)$ and $D_3 = g_3^{\frac{1}{2a+t}}$. are calculated using properties of elliptic curves. so to reveal U_2 and D_3 is almost impossible. Furthermore, if the intruder fetches the other information from the data carrier, which is also difficult, as discussed in the previous property.
- User Impersonation Attack (UIA) An adversary may put U_i in the authentication phase to impersonate a user (patient) U , but to complete authentication by TA, there is a need for U_2^* which is concatenated and hashed with another parameter by TA. So it is impossible to impersonate a patient U .
- Docotor Impersonation Attack (DIA): An adversary may get the identity of a doctor (d_i) to impersonate the doctor, but to be authenticated from a trusted authority (TA), D_3 and SK_{DT} are calculated. As we can see that

D_3 has been calculated with the use of a generator of the elliptic curve. It makes it impossible to know the required parameters to impersonate the doctor.

- **Trusted Authority (TA) Impersonation Attack (TAIA):** An adversary may attempt to get the key SK_{TA} to impersonate TA. But for SK_{TA} , TA needs to calculate, T_u and T_D where, $T_u = h(B_1||B_2||U^1||T^1)$ and $T_D = h(D_1||D_2||D^1||T^1)$. Here, the terms B_1, B_2, D_1 and D_2 are calculated by the concept of generator of ECC. ECDLP property of ECC makes it too tough to know about these terms. Finally, we can conclude that TAIA is not possible in this case.
- **Known Key Attack (KKA):** It is not a given that all session keys would be compromised if one session key were compromised. The proposed protocol's approved session key is based on three arbitrary, session-specific ephemeral secrets, T_U and T_D . It's possible that the adversary won't be able to derive all of these simultaneously due to the complexity of the ECDLP problem (ECC property). As a result, disclosing one session key prevents the adversary from discovering others. It is also known as the No key control property by researchers.
- **Replay Attack (RA):** Because we have used the timestamps TS_u , $TSTA$, and accepted delay (δT) in the authentication phase, replaying previous messages is pointless. As a result, our system is resistant to replay attacks.
- **Resistance to message modification attack:** This attack involves changing a piece of an anonymous message to have an unauthorized consequence. In our scheme, the patient's data carrier generates U^1 , which calculates the session key, preventing the message modification attack. Furthermore, DC perform $e(B_1 \times B_2, U_1) = e(g_1, g_2)$ to check the correctness of the doctor. Which also prevents message modification. The confidentiality part of the proposed protocol will make it impossible to modify the messages. Hence, our scheme can defend against the message modification attack.
- **Resistance to Bogus Message Attack** A fake message will not pass the

message correctness test. Since every patient and doctor examines the accuracy of the received message concerning the established conditions, the doctor or patient will finally discard it. Therefore, fraudulent message attacks cannot succeed against our scheme.

- **Unlinkability:** Each time, the AACs sent by the patients or doctors are unique. Because of the short life session keys, arbitrary random numbers on which these certificates are generated. The anonymous certificates and signatures have no reference to one another because these random integers vary. As a result, an attacker can't link multiple anonymous certificates and signatures produced by the same patient or physician.

Table 5.2, summarizes the comparison between the existing works and the proposed one. It is clear from table that the proposed protocol resists majority of modern attack as shown in Table 5.2. Efficiency of proposed work is discussed in chapter 6.

Table 5.2: **Attack resilient comparison with existing schemes**

Security features and attack	Proposed Scheme	[147]	[131]	[148]	[67]	[149]	[150]
Anonymity and Un-traceability	✓	✓	✓	✓	✓	✓	—
Offline Guessing Attack	✓	—	—	✓	yes	—	NO
Perfect Forward Secrecy	✓	—	—	—	✓	—	—
Sybill Attack	✓	—	—	—	—	—	—
Known session-specific temporary information attac	✓	no	yes	no	—	yes	
Privilege Insider Attack	✓	✓	✓	—	✓	—	—
User Impersonation Attack	✓	—	no	—	✓	✓	
Doctor Impersonation Attack	✓	—	no	—	✓	✓	✓
Replay Attack	✓	✓	—	✓	✓	—	✓
Mutual Authentication and Key-agreement.	✓	✓	no	✓	✓	—	✓

5.7 Summary

Internet of Medical Things (IoMT) is one of the best solutions for the tasks in COVID-19, such as monitoring the patients in quarantine, regulating the medical equipment, and performing remote diagnoses on patients. The inclusions of recent technologies in IoMT, such as artificial intelligence and big data, have increased its effectiveness by leap and bounce. All these advancements in IoMT will be sunk if a perfect protocol or scheme is not included to make this secure and safe from adversaries. The proposed protocol is best suited for providing authentication for doctors' safe access to patient-related data, resistant to recent attacks. Confidentiality features of the proposed work ensure black box data transfer from one party to another. The proposed protocol is compared with those only concerned with Medical IoT (MIoT) and Healthcare infrastructure to maintain its application in the real World. Furthermore, Performance comparison with contemporary protocols proves the proposed work is the pinnacle for the IoMT for COVID-19 and future pandemics.

Chapter 6

PERFORMANCE EVALUATION

One of the primary challenges is choosing the optimized security protocol because of limitations like dynamic resources and limited storage. Before being used in real-world applications, authentication systems must endure thorough cryptanalysis. In this chapter, we focus significant assaults and technical approaches against the IoT authentication system. We also covered current security verification methods and IoT authentication evaluation strategies. All sections have also discussed the analysis of present protocols, and some recommendations have been made. We have discussed constraints for IoT devices and elements of cryptanalysis of authentication schemes of IoT devices. Finally, our work aims to aid future researchers by presenting security concerns, unresolved problems, and potential future applications of IoT authentication.

6.1 Introduction

A particular authentication scheme must pass through a solid analysis before its implementation in any application. Cryptanalysis and Performance analysis are the two main elements of analysis for IoT devices [79–81]. Cryptanalysis is the study of techniques for deciphering encrypted data without access to the confidential data generally needed. Knowing how the system operates and locating a secret key are typically required. Another name for cryptanalysis is codebreaking or cracking the code. When choosing or constructing schemes for IoT devices, performance analysis is one of the centric factors to care very minutely. In performance analysis, various

factors are concentrated, such as computational cost, communication cost, and storage capacity. There are various survey papers focusing on IoT device security in different areas. Ashraf et al. have focused on the maritime industry. [82]. Yang et al. described the physical security of IoT devices [83] but lacked all possible attacks. Similarly, Serror et al. have focused on Industrial IoT [84], but it lacks a description of the simulation tools for the security analysis of various schemes. On the other hand, Alam et.al, described cloud-assisted IoT infrastructure [4]. Various informal and formal proof of security and analysis are discussed in these manuscripts. Some extra features must be added to make it universally accepted. In the present work, we would try to give information about all the necessary concepts, which makes analysis fruitful and effective. Following are the contributions of this chapter:

- Importance of the security of IoT devices is discussed in detail, which would help the reader to move towards a thorough study of IoT security.
- All types of attacks will be discussed along with the simulation tools to simulate the proposed scheme
- All parameters of performance analysis is described with the comparison of various authentication schemes.
- It would help the researcher to propose a solid and reliable application-oriented scheme for IoT infrastructures.

6.2 Preliminaries

6.2.1 Informal analysis

In informal analysis, Schemes are checked against all possible attacks. In this section, we shall first explore the limitations and capacities of adversaries. Later, we study different attacks.

- Adversary Model: In IoT architecture, adversaries are of two types: Internal adversaries and External adversaries. Internal adversaries are

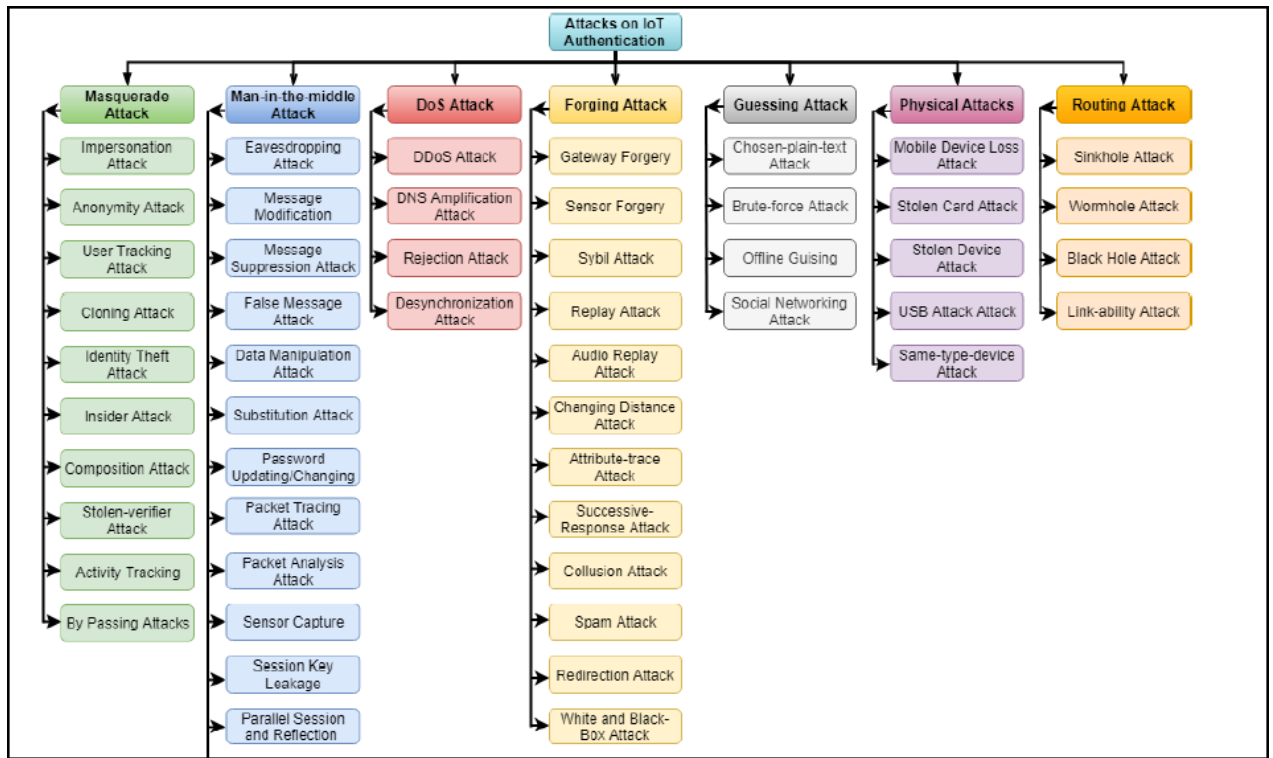


Figure 6.1: **Attacks on IoT Authentication**

legitimate users, and external adversaries are non-legitimate users. Dolev and Yao [151] proposed a basic and typical adversarial model in 1983. It is a popular model. According to this approach, adversaries can read, alter, and decrypt communications with the proper keys. No statistical or cryptanalytic attacks can be launched by adversaries. Along with Dolev and Yao's model, using a power analysis of smart cards, we have to consider the probability that adversaries might acquire critical information from lost or stolen smart cards [98]. Furthermore, an adversary would use a network analyzer and contemporary AI techniques [100] to extract data from network flow.

- **Taxonomy of Attacks:** We prove that a particular scheme resists attacks before its practical implementation. There are several possible attacks in the case of IoT devices. Some major categories are the following:

1. **Masquerade attack:** In a masquerade attack, the adversary impersonates a real user on the network by using false identification. The IoT network can be attacked by masquerade attacks if it is not adequately secured. These attacks can be prepared using a stolen identity, such as a user ID or password, or by observing user activity

tracking. Impersonation attacks, anonymity attacks, user tracking attacks, insider attacks, and activity tracking are some attacks that are categorized as Masquerade attacks.

2. Man in the Middle attack: A “Man in the Middle” attack entails an attacker sneakily breaking into a network and listening in on conversations between two parties who think they are speaking to one another directly. In this case, the attacker can forecast network and security patterns and drop, modify, and alter communication data. Additionally, they establish new communications within the system using legitimate users’ data. Eavesdropping, message modification attacks, false message attacks, and packet analysis attacks are some variations of the Man in the Middle attack.
3. DOS attack: A denial of service (DoS) attack prevents an authorised user from using a server or network by sending numerous requests to the server at once. In a DoS attack, a malicious user floods the authentication server with requests, temporarily shutting down the function, particularly prevalent in IoT-based networks. DDoS attacks, DNS amplification attacks, Rejection attacks and Desynchronization attacks are some examples of DoS attacks.
4. Forging attack: An attacker can access private information through a forging attack, which lets them steal the authentication details of a legitimate network user and pass them off as that person’s credentials. Gateway forgery, Sensor forgery, Sybil attack, Replay attack, Collision attack and White-Black Box attack are some major attacks in this category.
5. Guessing attack: The IoT authentication server keeps the user and peripheral authentication data, including device id, user id, secret device key, and user password, for usage in IoT networks. Intruders attempt to obtain those credentials to enter the system. If they have direct access to the server, they can extract credentials from it. Attackers try to guess passwords to establish their legitimacy as users; however, if they cannot gain the credentials. This is an attack based on speculation. Chosen plain text attack, Brute force attack,

offline guessing attack, and Social networking attack are some guessing attacks.

6. Physical attack: The network is filled with scattered IoT hardware. These devices can be physically accessed if no physical security measures are in place. Furthermore, there can be hundreds of IoT devices, which makes it impossible to protect them from physical attacks. However, physical attacks are also carried out on mobile devices, which are more difficult to detect, and static devices, which can be easily traced. Mobile device loss attacks, Stolen Card attacks, USB attacks, and Same-Type device attacks are some types of Physical attacks.
7. Routing attack: A routing attack occurs when an untrusted node passes data packets to the wrong location. Sinkhole attacks, wormhole attacks, Black hole attacks, and Linkability attacks are some Routing attacks. In 2019 Nandy et al. [23], explained various types of attacks in IoT authentication as shown in figure 6.1. . All the three schemes discussed in Chapter3, Chapter4 and Chapter5 are compared with the existing schemes in Table 3.2, 4.2 and 5.2 respectively.

6.2.2 Formal analysis

We pass a particular scheme through verification techniques and simulation tools in formal analysis. A brief description is as follows:

1. BAN logic allows us to obtain the following critical information about an authentication protocol:
 - (a) Each protocol's purpose (Goal).
 - (b) The cryptosystem implemented.
 - (c) Whether or not secrets are used (other than the key).
 - (d) Is there any assurance that messages will be delivered on time?
 - (e) Whether the participation of each party is validated by protocol.
 - (f) To remove redundancy.
2. Protocol validation using AVISPA and SCYTHERR: To accelerate the formulation of the next generation of security protocols and

enhance their security, it is essential to have tools that enable a thorough analysis of existing security protocols. It achieves this by identifying flaws and demonstrating their accuracy. A push-button tool called AVISPA was introduced by Armando et al. in 2005 for the automatic certification of Internet security-sensitive protocols and applications [137]. AVISPA stands for automated verification of Internet security-relevant protocols and programs. A protocol designer uses the tool to explain a security issue. The protocols are implemented effectively by applying the High-Level Protocol Specification Language (HLPSP). [152]. Additionally, thorough investigations of AVISPA and its implementation can be found in the works [4]. The proposed work also includes some critical recommendations for creating protocols in the HLPSP language, followed by screenshots of the results of our protocol.

- (a) Before doing anything else, each participant's role is written, including role name, declaration of local and constant variables, and transition.
- (b) Roles are combined in a session once participant roles have been established.
- (c) Establish the protocol analysis environment, which includes the scenario to be used, the parallel session instances, and prior knowledge of the intruder.
- (d) The protocol's security features are then declared to be executed. All four utilities provided by the AVISPA tools accept the proposed protocol. Some short descriptions are the following:
 - (a) **OFMC**: It performs bounded verification and protocol fabrication. It stands for On-the-fly Model-Checker
 - (b) **CL-AtSe**: It can manage message concatenation associativity and detect typing errors. It stands for Constraint-Logic-based Attack Searcher.
 - (c) **SATMC**: It creates a propositional formula that encodes a bounded unrolling of the beginning state, the initial state provided by the IF, and the conditions signifying a violation of

the security characteristics. It stands for SAT-based Model-Checker.

- (d) **TA4SP**: Rewriting and regular tree languages are employed to approximate attacker knowledge. TA4SP stands for Tree Automata based on Automatic Approximations for the Analysis of Security Protocols.

All four tests were passed by our protocol.

3. SCYTHER

We use the Scyther tool (The latest stable version of Scyther is v1.1.3, which was released on April 4, 2014.) to verify the proposed scheme formally [146]. It is intended to automatically analyze, falsify, and verify the security protocol's attributes. In comparison to other simulators, the Scyther tool has more features. The Scyther tool assumes that perfect cryptography is used, meaning that a message cannot be deciphered from the ciphertext by someone who does not possess the encryption key. Dolev-Yao's adversary model and pattern refining technique are used by this tool. The following innovative features are present in this tool:

- (a) With this tool, we may assess a protocol's security for both an unbounded and bounded number of sessions.
- (b) The security of a protocol against various attacks can be evaluated using this tool.
- (c) It is to validate both user-defined and automatically generated claims.
- (d) With the help of this tool, it is possible to ensure termination while analyzing a protocol using infinite sets of traces.

Python was used to develop the Scyther tool. To create a protocol that may be utilized with the Scyther tool, one must use the Security Protocol Descriptive Language (SPDL). We have used a Graphical User Interface (GUI) for this purpose. This prepares the verification results and, when attacks are detected, a visual representation of the attack Scyther found on the scheme. We created our authentication phase in SPDL language to simulate the suggested scheme against the

Scyther tool. Figures. 5.7 and 5.8, illustrate the simulation’s output. Our protocol is secure, according to the simulation results.

4. Random Oracle A random function known as a “random oracle ” responds to each inquiry with a random answer selected randomly and uniformly from its output domain. It is a mathematical function that, for each repeated unique query, always chooses the fixed random response from its output domain.
5. Real-Or-Random Model (ROR): It is the protocol for two-party authentication key exchange. An adversary can pose Execute, Send, and Test questions in this model. The adversary may also send as many Test queries as required to differentiate between instances.

Apart from the above-mentioned tools, some are used in various authentication schemes such as Game theory, ROM model and SPI calculus. Some researchers prefer mathematical proof [120].

6.3 Performance analysis

As demanding and novel authentication methods are protecting the IoT environment from many developing threats, evaluation of those proposed techniques, attacks, and It is crucial to evaluate their efficiency. In this paragraph, we talk about some performance analysis methods, their parameters, and supplementary equations.

1. Average response time: The time it takes the server or GWN to respond to a client’s request is the response time. Several variables might impact this, including server configuration, user count, network bandwidth, volume, kind, and response time.
2. Handshake duration: The IoT network’s “handshaking” process involves negotiating between two network parties. These parties may be nodes, servers, sensors, actuators, or users.
3. Computational Cost: Computation in an IoT network also influences the protocols used. In IoT networks, heavy computation cannot be done since most network devices have computing limitations. As a result, designers of protocols constantly strive to

produce simple authentication methods for Internet of Things networks. As a result, numerous academics now use hash, XOR, and concatenation concepts to secure messages as they travel via networks. The IoT authentication technique also employs ECC, MOD, and fuzzy commitments.

4. **Communication Cost:** In the Internet of Things, communication for authentication can vary depending on the protocol. Additionally, it may convey a message of contrasting scale to express in stages. As a result, a process requires a minimum of four messages to create a secure authentication, and these messages are sent between the user, sensor, and gateway node or authentication server. The size of those messages varies because different messages carry different values.

6.3.1 Performance evaluation of discussed schemes

To evaluate performance of schemes discussed in above Chapters, following are the steps :

1. Schemes are compared with current existing literature.
2. Security features achieved by particular scheme is shown in the tables in their corresponding chapters.
3. Computational and communication cost has been calculated and compared with existing schemes.

Here, we would discuss each scheme separately.

Performance evaluation of Scheme of chapter-3

The computational cost of the proposed protocol is compared to that of other protocols in Table 6.1. We have taken experimented values as reported in [28,43,102,154] are following: Time to compute hash function (T_h): 0.0005 s, time to compute ECC multiplication (T_{ecm}):0.06307 s, time to compute fuzzy extractor (T_{fe}):0.063075. Time to compute ECC point addition (T_{eca}): 0.010875 s. We have ignored time consumed in XOR and concatenation operations. At last, we have plotted a graph for better

Table 6.1: **Computational overhead with related schemes of chapter-III**

Protocols	User	TA	Cloud Server	Total overhead
Proposed	$T_{ecm} + 10T_h$	$T_{ecm} + 9T_h$	$T_{ecm} + 3T_h$	$3T_{ecm} + 22T_h = 0.2002$
[41]	$13T_h$	$19T_h$	$8T_h$	$40T_h = 0.02$
[39]	$9T_h$	$10T_h$	$19T_h$	$23T_h = 0.0115$
[34]	$4T_{ecm} + 3T_h$	-	$6T_{ecm} + 4T_{eca} + 4T_h$	$10T_{ecm} + 7T_h + 4T_{eca} = 0.67775$
[153]	$2T_{ecm} + 6T_h$	-	$6T_{ecm} + 4T_h + 4T_{eca}$	$8T_{ecm} + 10T_h + 4T_{eca} = 0.35667$
[109]	$4T_{ecm} + 12T_h$	-	$9T_h$	$4T_{ecm} + 21T_h = 0.2628S$
[28]	$2T_{ecm} + 17T_h + T_{fe}$	$5T_h$	$T_{ecm} + 5T_h$	$3T_{ecm} + 27T_h + T_{fe} = 0.333$

judgment between security features supported and time consumed by the proposed protocol and other protocols. The graph of summary of security analysis is presented for the ease of readers in figure 6.2.

Discussion on the efficiency of scheme in chapter-3

In Chapter-3, Table 3.2, compares the proposed scheme to other relevant existing protocols in terms of security and functional elements that are desired or required. Our protocol includes all essential security features. Existing protocols are missing several key features (as discussed in Section 3.4.2, informal analysis of proposed protocols), such as protection against offline password guessing attacks, known key attacks, stolen card attacks, and impersonation attacks. In addition, the proposed protocol provides rigorous security analysis and formal security verification using the widely-accepted AVISPA tool and BAN logic in subsection 3.4.2. and 3.4.1 respectively. Table 6.1, shows that the total overhead of the proposed protocol is 0.2 s, which is much less than most of the existing protocols. Results from Tables 3.2 and 6.1 proves the efficiency of the proposed protocol. Furthermore, Figure 6.2 makes our claim more clear in terms of performance comparison.

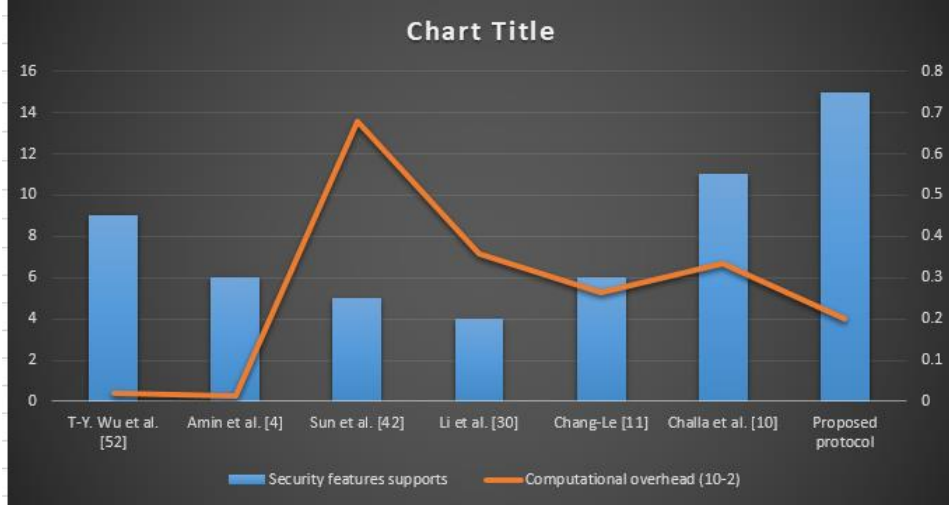


Figure 6.2: Performance Comparison of scheme of Chapter-III

6.3.2 Performance evaluation of Scheme of chapter-4

Computational cost

In the authentication phase, each member needs to compute pairwise shared keys with each other members. According to Horner's rule [155], for each univariate polynomials of $t - 1$ and $h - 1$ degree, there is a requirement of t and h calculations. Here in the proposed protocol, $F_i^2(0)$ is constant, due to which calculation reduces to Shamir's secret sharing scheme. The computation cost is very low in comparison to the other existing schemes.

Communication cost

The communication cost of membership authentication is meagre because all the public values associated with the specific user are broadcast. Furthermore, we have used one shared token component to encrypt others to avoid dependency on the private channel. Based on these reasons, we may conclude that it has significantly lower communication costs than the existing schemes.

Storage cost

Each member has to store only uni-variate polynomial of modulus P . So the storage requirement for each member is $\text{tlog}P$ bits. This polynomial-based modulus is far less than the public-key-based modulus [53]. Here threshold is t . To get collision-free authentication, each member must simultaneously deal with $t + 1$ uni-variate polynomial. So overall storage cost is very low compared to symmetric key-based schemes.

6.3.3 Comparison with existing schemes

All existing schemes can support either user authentication or session key establishment. On the other hand, our protocol may enable both membership authentication and session key establishment at the same time. Furthermore, the complexity of our membership authentication is $\mathcal{O}(n)$, where n is the number of members, which is significantly less than the traditional one-to-one authentication scheme with complexity $\mathcal{O}(n^2)$. In Table II, we have compared the recent scheme for grouped authentication. From there, we conclude that our scheme can deal with many attacks in the case of IoT authentication. The number of computations for 25 nodes by Lee et al. [118] and Chein et al. [156] is 1000 and 2500, respectively. On the other hand proposed scheme uses less than 100 computations for the same number of nodes. Furthermore, the figure. 6.3, we can see that number of communication between nodes is significantly less than others.

Discussion of the efficiency of scheme of Chapter-4

Table 4.2. in Chapter-4, we have seen that proposed scheme is resilient to most of the common attacks. Informal analysis has been done in section 4.5.1 in terms of AVISPA. To show efficiency of proposed scheme, we have compared with existing schemes in Figure 6.2.

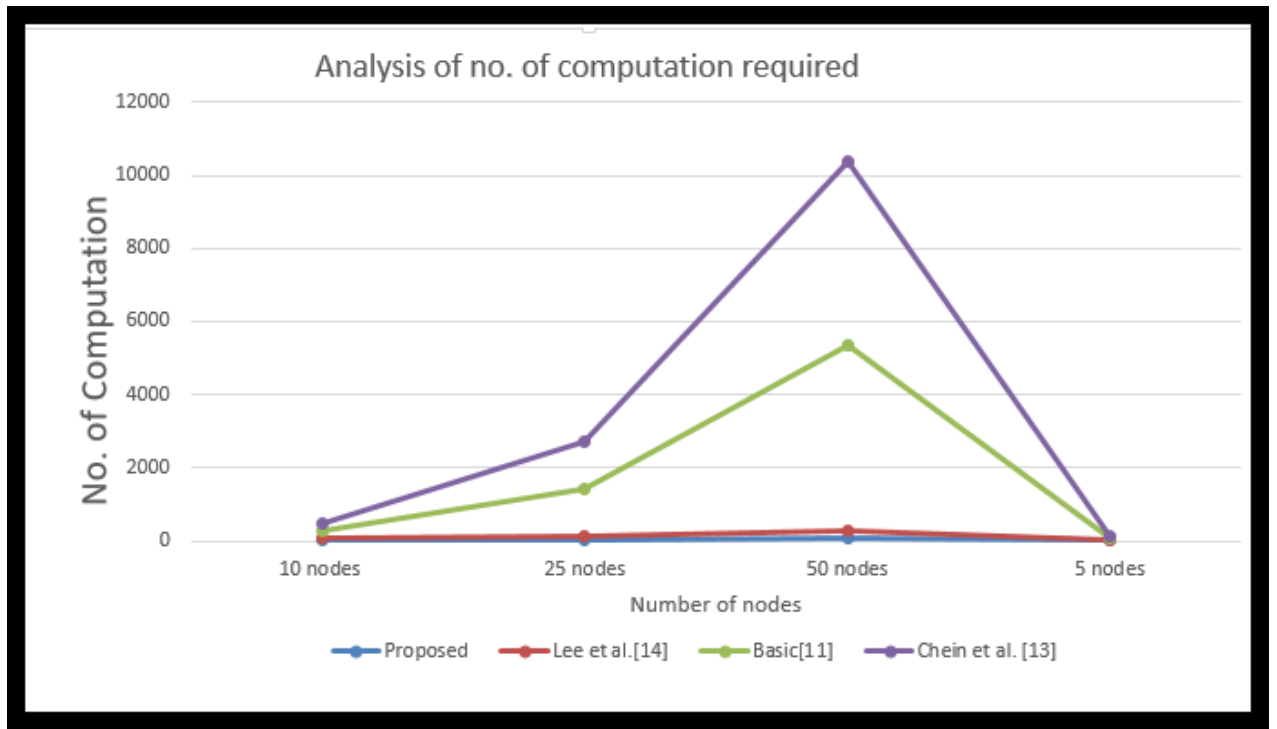


Figure 6.3: Comparison of Schemes of Chapter-IV

6.3.4 Performance evaluation of Scheme of chapter-5

6.3.5 Performance Analysis

When we talk about IoMT, we must take such protocols which are related to IoMT and health care. Due to that, we have chosen only specific protocols for comparison. In the following subsections, we have analyzed the proposed protocol's communication overhead and computational cost and compared it with existing protocols.

Communication Overhead

We computed communication overhead in this part and compared it to the existing protocols shown in Figure 6.2. The size of a timestamp, an element in Z_q , and the output of a hash function are typically considered to be 4, 20, and 20 B, respectively, similarly, the size for the generation of a cyclic group generator is 20B.

Table 6.2: **Communication Overhead of scheme of Chapter - V**

S.No.	Protocols	No. of hash
1.	Proposed Protocol	$4T_h$
2.	Li et al. [38]	$38T_h$
3.	Fotouhi et al. [39]	$68T_h$
4.	Deebak et al. [40]	$19T_h$
5.	Wu et al. [25]	$27T_h$
6.	Masud et al. [41]	$8T_h$
7.	Sharma et.al [42]	$23T_h$

Computational cost

The pairing-based cryptography (PBC) package [145] defines a Type-A elliptic curve, which is used in our scheme to produce the multiplicative cyclic groups G_1 , G_2 , and G_T . To calculate the cost of computing, let us look at some essential cryptographic procedures: T_p , T_h , T_s , and T_m stand for the times needed to complete bilinear operation, hash operation, a group of symmetric encryption, and point multiplication operations, respectively. For the purpose of examining communication parameters, a test platform is utilised that is used in [157]. Following multiple simulations, the execution times for each of the time parameters (T_p , T_h , T_s , and T_m) are calculated, with the final values being the average of all simulation results. Each cryptographic operation's execution times - T_p , T_h , T_s , and T_m are calculated to be 1.7, 2.6, 0.4, and 0.7 ms, respectively. The suggested protocol's overall calculation time is 26.6 ms, which is acceptable for IMoT. The test setup's configuration varies from time to time and from scheme to scheme. Therefore, we have considered the number of hash functions employed in the schemes to compare the proposed scheme with other existing schemes based on the computational cost. The proposed scheme has used a very less number of the hash function as compared to others as shown in the Table 6.2.

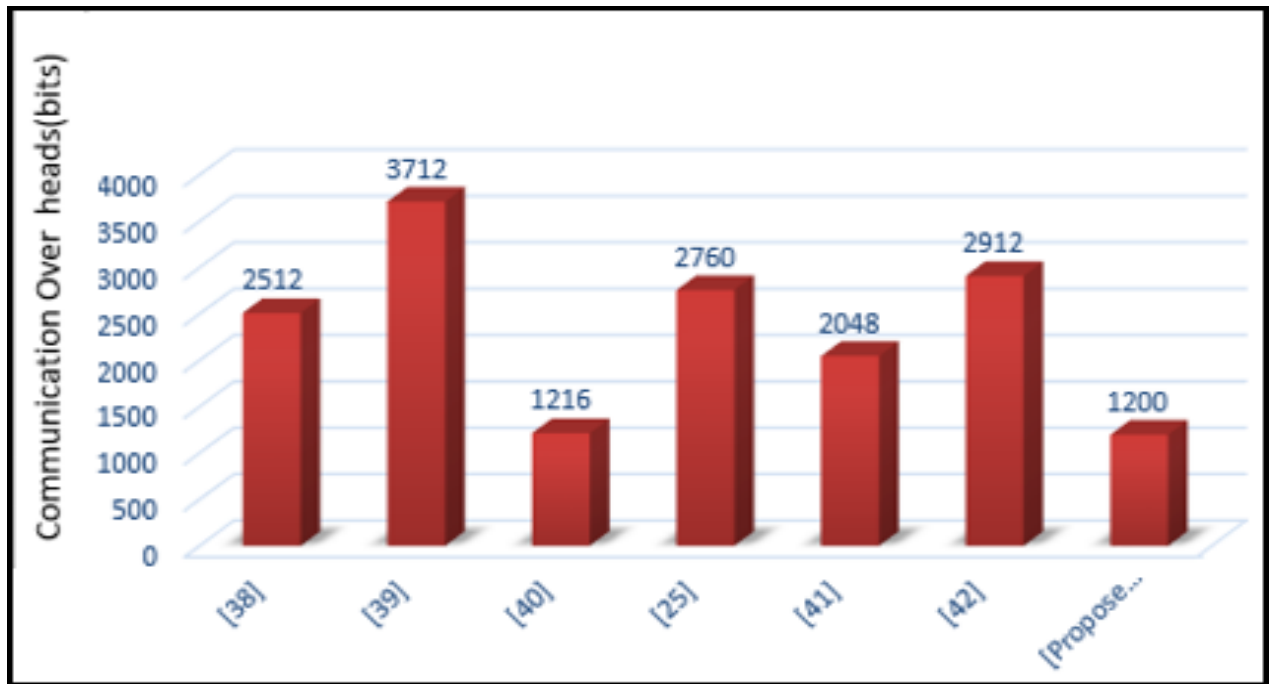


Figure 6.4: Communication cost comparison of the proposed and conventional protocols (Scheme of Chapter-V)

Discussion of efficeincy of the proposed scheme of chapter-5

In table 5.2, attack resilient property of proposed scheme has been shown in chapter-5. Along with that the same schemes has been passed through AVISPA and Scyther in subsecion 5.2.1 and 5.2.2 respectively.

6.4 Summary

IoT stakeholders can decide on the best authentication system for their unique use cases by conducting a thorough performance evaluation that takes these variables into account, striking a balance between security, efficiency, and usability.

In this chapter, we have highlighted IoT security's critical importance. We proceed with the description of all possible attacks. Some major techniques for formal and informal analysis are discussed. In the last, we focused on performance analysis.

We hope our study will educate readers on various IoT authentication threats and techniques. It will also assist incoming researchers in formulating their proposals for developing robust IoT authentication protocols to serve end users better.

Chapter 7

CONCLUSION AND FUTURE WORK

7.1 Conclusion

IoT security is of critical importance because of the growing prevalence of Internet of Things (IoT) devices in both personal and professional settings. These devices are increasingly being used to collect and transmit sensitive data, such as personal health information, financial data, and intellectual property. However, many IoT devices are not designed with security in mind, making them vulnerable to cyberattacks.

The consequences of a successful attack on an IoT device can be severe. In addition, the proliferation of IoT devices means that security risks are constantly evolving and becoming more complex. This requires a multi-layered approach to security that involves not only securing individual devices, but also protecting the network and the data that is transmitted between devices. In this research, we have first discussed different applications of IoT devices and the need for their security. Lightweight protocols have been proposed due to various constraints such as lower processing power, lower battery power, and lower storage capacity of IoT devices.

In the first protocol, Authentication of cloud-based IoT devices has been proposed to ensure attack-free communication between IOT devices. Using the ECDLP property of ECC with Hash and XOR makes the proposed protocols very hard to break.

In the second work, a novel approach for group-based authentication has

been proposed by using secret sharing concepts as the core. This work is very impactful in the case of a group of sensors acting for a specific task. It takes very less time to be executed than the traditional authentication schemes.

A novel authentication protocol has been proposed for the medical Internet of Things (MIoT) for covid-19 and future pandemics. This protocol uses bilinear pairing with hash and XOR operators which makes this protocol efficient for challenging situations in pandemics.

In the last, we have performed the performance evaluation of the proposed protocols that show that these protocols are very efficient to the existing work in terms of resistance to various attacks, computation time, and transmission time.

7.2 Limitations

Although we have tried to make the above proposed protocols very efficient and real for the current scenarios of applications, these protocols possess certain limitations which can be improved in future work.

1. First proposed protocol can be tested for the more recent attacks.
2. Second proposed protocol is limited to group-based authentication.
3. Third proposed protocol may not be suitable for the future pandemic if not repeat the same characteristics as of covid-19.
4. for the performance evaluation, Oracle model, proverif, and other tools are not used.

7.3 Future Work

There are many open issues related to the research in this thesis. Some possible future research directions are listed below:

1. To develop security protocols that deal with constraints for IoT devices and support IoT interoperability and heterogeneity, with the incorporation of edge and Fog computing.

2. Some novel techniques, such as blockchain, federated learning, deep learning, and adaptive authentication, would be used to come up with robust Security protocols that can be applied in various situations in the real world.
3. The most common buzz words of this decade, such as smart cities, smart Hospitals, autonomous vehicles, smart grid, and smart agriculture, need security solutions with consideration of their limitations in resources. Contribution to the advancement of the security of these systems through practical deployment and industry collaboration would be my first priority.

List of Publications

The author has published multiple parts of this thesis in international publications and conferences. Following are the list of papers with their brief details of publication:

1. List of papers (s) published in Peer Reviewed Referred International Journals

- (a) Alam Irfan and Manoj Kumar, “A novel protocol for efficient authentication in cloud-based iot devices,” *Multimedia Tools and Applications*, vol. 81, no. 10, pp. 13823 - 13843, 2022.
doi:<https://doi.org/10.1007/s11042-022-11927-y>
SCIE-Indexed(I.F: 3.75). It maps chapter 3.
- (b) Alam Irfan and Manoj Kumar. “A novel authentication protocol to ensure confidentiality among the Internet of Medical Things in covid-19 and future pandemic scenario.” *Internet of Things*, vol. 22, p. 100797, 2023.
doi: <https://doi.org/10.1016/j.iot.2023.100797>
SCIE-Indexed(I.F.:5.9). It maps chapter 5.

2. List of Paper(s) Published in Peer Reviewed International Conference

- (a) Alam Irfan, and Manoj Kumar. “An overview of Secure Communication in Smart Cities: Issues and Cryptographic Solution.”” 2022 International Conference on Data Analytics for Business and Industry (ICDABI). IEEE, 2022.
Scopus Indexed.(Maps Introduction Chapter).
- (b) Alam Irfan, and Manoj Kumar. “Various Elements of Analysis of Authentication Schemes for IoT devices: A Brief Overview”. International Conference on Recent Advances in Computer Science and Engineering (ICRACSE-2022)
Scopus Indexed

3. List of manuscripts related to thesis (under review):

- (a) Alam Irfan, and Manoj Kumar. ”A novel authentication scheme for group based communication for IoT oriented infrastructure in

smart cities.” (2022).

Under review in *IEEE transaction on information forensics and security*. (SCIE-Indexed with I.F.:7.211) It maps chapter 4.

- (b) Alam Irfan, and Manoj Kumar. “A Critical Authentication Analysis and Future Research Directions for the Security of Internet of Things: A Comprehensive Review” is communicated in *Internet of Things, ScienceDirect*

Bibliography

- [1] K. Ashton, “That ‘internet of things’ thing,” *RFID journal*, vol. 22, no. 7, pp. 97–114, 2009.
- [2] S. Li, L. D. Xu, Zhao, *et al.*, “The internet of things: a survey,” *Information systems frontiers*, vol. 17, no. 2, pp. 243–259, 2015.
- [3] W. Iqbal, H. Abbas, M. Daneshmand, B. Rauf, and Y. A. Bangash, “An in-depth analysis of iot security requirements, challenges, and their countermeasures via software-defined security,” *IEEE Internet of Things Journal*, vol. 7, no. 10, pp. 10250–10276, 2020.
- [4] I. Alam and M. Kumar, “A novel protocol for efficient authentication in cloud-based iot devices,” *Multimedia Tools and Applications*, vol. 81, no. 10, pp. 13823–13843, 2022.
- [5] I. Alam and M. Kumar, “A novel authentication protocol to ensure confidentiality among the internet of medical things in covid-19 and future pandemic scenario,” *Internet of Things*, vol. 22, p. 100797, 2023.
- [6] I. Alam and M. Kumar, “A novel authentication scheme for group based communication for iot oriented infrastructure in smart cities,” 2022.
- [7] I. Alam and M. Kumar, “An overview of secure communication in smart cities: Issues and cryptographic solution,” in *2022 International Conference on Data Analytics for Business and Industry (ICDABI)*, pp. 297–301, IEEE, 2022.
- [8] J. Sengupta, S. Ruj, and S. D. Bit, “Blockchain-enabled verifiable collaborative learning for industrial iot,” 2022.
- [9] N. Neshenko, E. Bou-Harb, J. Crichigno, G. Kaddoum, and N. Ghani, “Demystifying iot security: an exhaustive survey on

- iot vulnerabilities and a first empirical look on internet-scale iot exploitations,” *IEEE Communications Surveys & Tutorials*, vol. 21, no. 3, pp. 2702–2733, 2019.
- [10] F. T. Al-Dhief and Latiff, “A survey of voice pathology surveillance systems based on internet of things and machine learning algorithms,” *IEEE Access*, vol. 8, pp. 64514–64533, 2020.
 - [11] V. Sharma, I. You, K. Andersson, F. Palmieri, M. H. Rehmani, and J. Lim, “Security, privacy and trust for smart mobile-internet of things (m-iot): A survey,” *IEEE access*, vol. 8, pp. 167123–167163, 2020.
 - [12] A. Barua, M. A. Al Alamin, M. S. Hossain, and E. Hossain, “Security and privacy threats for bluetooth low energy in iot and wearable devices: A comprehensive survey,” *IEEE Open Journal of the Communications Society*, 2022.
 - [13] S. Hameed, F. I. Khan, and B. Hameed, “Understanding security requirements and challenges in internet of things (iot): A review,” *Journal of Computer Networks and Communications*, vol. 2019, pp. 1–14, 2019.
 - [14] T. M. Fernández-Caramés, “From pre-quantum to post-quantum iot security: A survey on quantum-resistant cryptosystems for the internet of things,” *IEEE Internet of Things Journal*, vol. 7, no. 7, pp. 6457–6480, 2019.
 - [15] M. Stoyanova, Y. Nikoloudakis, S. Panagiotakis, E. Pallis, and E. K. Markakis, “A survey on the internet of things (iot) forensics: challenges, approaches, and open issues,” *IEEE Communications Surveys & Tutorials*, vol. 22, no. 2, pp. 1191–1221, 2020.
 - [16] L. Chettri and R. Bera, “A comprehensive survey on internet of things (iot) toward 5g wireless systems,” *IEEE Internet of Things Journal*, vol. 7, no. 1, pp. 16–32, 2019.
 - [17] M. N. Khan, A. Rao, and S. Camtepe, “Lightweight cryptographic protocols for iot-constrained devices: A survey,” *IEEE Internet of Things Journal*, vol. 8, no. 6, pp. 4132–4156, 2020.

- [18] F. Meneghello, M. Calore, D. Zucchetto, M. Polese, and A. Zanella, "Iot: Internet of threats? a survey of practical security vulnerabilities in real iot devices," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 8182–8201, 2019.
- [19] Y. Song, F. R. Yu, L. Zhou, X. Yang, and Z. He, "Applications of the internet of things (iot) in smart logistics: a comprehensive survey," *IEEE Internet of Things Journal*, vol. 8, no. 6, pp. 4250–4274, 2020.
- [20] W. Rafique, L. Qi, I. Yaqoob, M. Imran, R. U. Rasool, and W. Dou, "Complementing iot services through software defined networking and edge computing: A comprehensive survey," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 3, pp. 1761–1804, 2020.
- [21] O. Friha, M. A. Ferrag, L. Shu, L. Maglaras, and X. Wang, "Internet of things for the future of smart agriculture: A comprehensive survey of emerging technologies," *IEEE/CAA Journal of Automatica Sinica*, vol. 8, no. 4, pp. 718–752, 2021.
- [22] A. Alwarafy, K. A. Al-Thelaya, M. Abdallah, J. Schneider, and M. Hamdi, "A survey on security and privacy issues in edge-computing-assisted internet of things," *IEEE Internet of Things Journal*, vol. 8, no. 6, pp. 4004–4022, 2020.
- [23] T. Nandy, M. Y. I. B. Idris, R. M. Noor, L. M. Kiah, L. S. Lun, N. B. A. Juma'at, I. Ahmedy, N. A. Ghani, and S. Bhattacharyya, "Review on security of internet of things authentication mechanism," *IEEE Access*, vol. 7, pp. 151054–151089, 2019.
- [24] L. Lamport, "Password authentication with insecure communication," *Communications of the ACM*, vol. 24, no. 11, pp. 770–772, 1981.
- [25] V. S. Miller, *Use of elliptic curves in cryptography*. Springer, 1986.
- [26] P. Chakraborty, S. Maitra, M. Nandi, S. Talnikar, P. Chakraborty, S. Maitra, M. Nandi, and S. Talnikar, "Introduction and preliminaries," *Contact Tracing in Post-Covid World: A Cryptologic Approach*, pp. 1–29, 2020.

- [27] M. Wazid, A. K. Das, R. Hussain, G. Succi, and J. J. Rodrigues, "Authentication in cloud-driven iot-based big data environment: Survey and outlook," *Journal of systems architecture*, vol. 97, pp. 185–196, 2019.
- [28] S. Challa, A. K. Das, P. Gope, N. Kumar, F. Wu, and A. V. Vasilakos, "Design and analysis of authenticated key agreement scheme in cloud-assisted cyber-physical systems," *Future Generation Computer Systems*, vol. 108, pp. 1267–1286, 2020.
- [29] S. H. Islam and G. Biswas, "An improved pairing-free identity-based authenticated key agreement protocol based on ecc," *Procedia Engineering*, vol. 30, pp. 499–507, 2012.
- [30] S. Kumari, M. Karuppiah, A. K. Das, X. Li, F. Wu, and V. Gupta, "Design of a secure anonymity-preserving authentication scheme for session initiation protocol using elliptic curve cryptography," *Journal of Ambient Intelligence and Humanized Computing*, vol. 9, pp. 643–653, 2018.
- [31] D. Rangwani and H. Om, "A secure user authentication protocol based on ecc for cloud computing environment," *Arabian Journal for Science and Engineering*, vol. 46, pp. 3865–3888, 2021.
- [32] H. Kim, D.-w. Kim, O. Yi, and J. Kim, "Cryptanalysis of hash functions based on blockciphers suitable for iot service platform security," *Multimedia Tools and Applications*, vol. 78, pp. 3107–3130, 2019.
- [33] A. Irshad, H. F. Ahmad, B. A. Alzahrani, M. Sher, and S. A. Chaudhry, "An efficient and anonymous chaotic map based authenticated key agreement for multi-server architecture," *KSII Transactions on Internet and Information Systems (TIIS)*, vol. 10, no. 12, pp. 5572–5595, 2016.
- [34] H. Sun, Q. Wen, H. Zhang, and Z. Jin, "A novel remote user authentication and key agreement scheme for mobile client-server environment," *Applied Mathematics & Information Sciences*, vol. 7, no. 4, p. 1365, 2013.

- [35] T.-Y. Wu, Z. Lee, M. S. Obaidat, S. Kumari, S. Kumar, and C.-M. Chen, “An authenticated key exchange protocol for multi-server architecture in 5g networks,” *IEEE Access*, vol. 8, pp. 28096–28108, 2020.
- [36] H. Li, F. Li, C. Song, and Y. Yan, “Towards smart card based mutual authentication schemes in cloud computing,” *KSII Transactions on Internet and Information Systems (TIIS)*, vol. 9, no. 7, pp. 2719–2735, 2015.
- [37] J. Wessels and C. BV, “Application of ban-logic,” *CMG FINANCE BV*, vol. 19, no. 1, p. 23, 2001.
- [38] P. Syverson and I. Cervesato, “The logic of authentication protocols,” in *Foundations of Security Analysis and Design: Tutorial Lectures 1*, pp. 63–137, Springer, 2001.
- [39] R. Amin, N. Kumar, G. Biswas, R. Iqbal, and V. Chang, “A light weight authentication protocol for iot-enabled devices in distributed cloud computing environment,” *Future Generation Computer Systems*, vol. 78, pp. 1005–1019, 2018.
- [40] R. K. Koppanati and K. Kumar, “P-mec: polynomial congruence-based multimedia encryption technique over cloud,” *IEEE consumer electronics magazine*, vol. 10, no. 5, pp. 41–46, 2020.
- [41] F. Wu, X. Li, L. Xu, A. K. Sangaiah, and J. J. Rodrigues, “Authentication protocol for distributed cloud computing: An explanation of the security situations for internet-of-things-enabled devices,” *IEEE Consumer Electronics Magazine*, vol. 7, no. 6, pp. 38–44, 2018.
- [42] M. Shen, H. Liu, L. Zhu, K. Xu, H. Yu, X. Du, and M. Guizani, “Blockchain-assisted secure device authentication for cross-domain industrial iot,” *IEEE Journal on Selected Areas in Communications*, vol. 38, no. 5, pp. 942–954, 2020.
- [43] M. Wazid, A. K. Das, V. Bhat, and A. V. Vasilakos, “Lamciot: Lightweight authentication mechanism in cloud-based iot environment,” *Journal of Network and Computer Applications*, vol. 150, p. 102496, 2020.

- [44] M. Rana, A. Shafiq, I. Altaf, M. Alazab, K. Mahmood, S. A. Chaudhry, and Y. B. Zikria, “A secure and lightweight authentication scheme for next generation iot infrastructure,” *Computer Communications*, vol. 165, pp. 85–96, 2021.
- [45] B. D. Deebak and F. Al-Turjman, “Robust lightweight privacy-preserving and session scheme interrogation for fog computing systems,” *Journal of Information Security and Applications*, vol. 58, p. 102689, 2021.
- [46] U. C. Cabuk, G. Dalkilic, and O. Dagdeviren, “Comad: Context-aware mutual authentication protocol for drone networks,” *IEEE Access*, 2021.
- [47] C. Hsu, L. Harn, and Z. Xia, “An hss-based robust and lightweight multiple group authentication for its towards 5g,” *IET Intelligent Transport Systems*, 2021.
- [48] A. Shamir, “How to share a secret,” *Communications of the ACM*, vol. 22, no. 11, pp. 612–613, 1979.
- [49] L. Harn, “Group authentication,” *IEEE Transactions on computers*, vol. 62, no. 9, pp. 1893–1898, 2012.
- [50] W.-T. Su, W.-M. Wong, and W.-C. Chen, “A survey of performance improvement by group-based authentication in iot,” in *2016 International Conference on Applied System Innovation (ICASI)*, pp. 1–4, IEEE, 2016.
- [51] H.-Y. Chien, “Group authentication with multiple trials and multiple authentications,” *Security and Communication Networks*, vol. 2017, 2017.
- [52] Q. Cheng, C. Hsu, Z. Xia, and L. Harn, “Fast multivariate-polynomial-based membership authentication and key establishment for secure group communications in wsn,” *IEEE Access*, vol. 8, pp. 71833–71839, 2020.
- [53] S. Wu, C. Hsu, Z. Xia, J. Zhang, and D. Wu, “Symmetric-bivariate-polynomial-based lightweight authenticated group key agreement for industrial internet of things,” *Journal of Internet Technology*, vol. 21, no. 7, pp. 1969–1979, 2020.

- [54] H. Xiong, J. Chen, Q. Mei, and Y. Zhao, "Conditional privacy-preserving authentication protocol with dynamic membership updating for vanets," *IEEE Transactions on Dependable and Secure Computing*, no. 01, pp. 1–1, 2020.
- [55] L. Harn, C.-F. Hsu, Z. Xia, and J. Zhou, "How to share secret efficiently over networks," *Security and Communication Networks*, vol. 2017, 2017.
- [56] L. Harn and C.-F. Hsu, " (t, n) multi-secret sharing scheme based on bivariate polynomial," *Wireless Personal Communications*, vol. 95, no. 2, pp. 1495–1504, 2017.
- [57] T. Zhang, X. Ke, and Y. Liu, " (t, n) multi-secret sharing scheme extended from harn-hsu's scheme," *EURASIP Journal on Wireless Communications and Networking*, vol. 2018, no. 1, pp. 1–4, 2018.
- [58] N. K. Jha, "Internet-of-medical-things," in *Proceedings of the on Great Lakes Symposium on VLSI 2017*, pp. 7–7, 2017.
- [59] M. A. Ferrag, L. Shu, X. Yang, A. Derhab, and L. Maglaras, "Security and privacy for green iot-based agriculture: Review, blockchain solutions, and challenges," *IEEE access*, vol. 8, pp. 32031–32053, 2020.
- [60] M. S. Farooq, O. O. Sohail, A. Abid, and S. Rasheed, "A survey on the role of iot in agriculture for the implementation of smart livestock environment," *IEEE Access*, vol. 10, pp. 9483–9505, 2022.
- [61] P. Mall, R. Amin, A. K. Das, M. T. Leung, and K.-K. R. Choo, "Puf-based authentication and key agreement protocols for iot, wsns and smart grids: a comprehensive survey," *IEEE Internet of Things Journal*, 2022.
- [62] P. Mishra, A. Vidyarthi, and P. Siano, "Guest editorial: Security and privacy for cloud-assisted internet of things (iot) and smart grid," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 7, pp. 4966–4968, 2022.

- [63] Y. Zhang, D. He, L. Li, and B. Chen, “A lightweight authentication and key agreement scheme for internet of drones,” *Computer Communications*, vol. 154, pp. 455–464, 2020.
- [64] Q. Jiang, N. Zhang, J. Ni, J. Ma, X. Ma, and K.-K. R. Choo, “Unified biometric privacy preserving three-factor authentication and key agreement for cloud-assisted autonomous vehicles,” *IEEE Transactions on Vehicular Technology*, vol. 69, no. 9, pp. 9390–9401, 2020.
- [65] M. Adil, M. Attique, M. M. Jadoon, J. Ali, A. Farouk, and H. Song, “Hopctp: a robust channel categorization data preservation scheme for industrial healthcare internet of things,” *IEEE Transactions on Industrial Informatics*, vol. 18, no. 10, pp. 7151–7161, 2022.
- [66] M. Kumar, S. Verma, A. Kumar, M. F. Ijaz, D. B. Rawat, *et al.*, “Anaf-iomt: A novel architectural framework for iomt-enabled smart healthcare system by enhancing security based on recc-vc,” *IEEE Transactions on Industrial Informatics*, vol. 18, no. 12, pp. 8936–8943, 2022.
- [67] F. Wu, X. Li, A. K. Sangaiah, L. Xu, S. Kumari, L. Wu, and J. Shen, “A lightweight and robust two-factor authentication scheme for personalized healthcare systems using wireless medical sensor networks,” *Future Generation Computer Systems*, vol. 82, pp. 727–737, 2018.
- [68] X. Yuan, C. Li, Q. Ye, K. Zhang, N. Cheng, N. Zhang, and X. Shen, “Performance analysis of ieee 802.15. 6-based coexisting mobile wbans with prioritized traffic and dynamic interference,” *IEEE Transactions on Wireless Communications*, vol. 17, no. 8, pp. 5637–5652, 2018.
- [69] A. Ostad-Sharif, D. Abbasinezhad-Mood, and M. Nikooghadam, “A robust and efficient ecc-based mutual authentication and session key generation scheme for healthcare applications,” *Journal of medical systems*, vol. 43, no. 1, pp. 1–22, 2019.
- [70] S. Kumari, P. Chaudhary, C.-M. Chen, and M. K. Khan, “Questioning key compromise attack on ostad-sharif et al.’s

- authentication and session key generation scheme for healthcare applications,” *IEEE Access*, vol. 7, pp. 39717–39720, 2019.
- [71] A. Rahman, M. S. Hossain, N. A. Alrajeh, and F. Alsolami, “Adversarial examples - security threats to covid-19 deep learning systems in medical iot devices,” *IEEE Internet of Things Journal*, vol. 8, no. 12, pp. 9603–9610, 2020.
- [72] M. Masud, G. S. Gaba, S. Alqahtani, G. Muhammad, B. B. Gupta, P. Kumar, and A. Ghoneim, “A lightweight and robust secure key establishment protocol for internet of medical things in covid-19 patients care,” *IEEE Internet of Things Journal*, vol. 8, no. 21, pp. 15694–15703, 2020.
- [73] H. Iqbal, Waseem, M. Daneshmand, B. Rauf, and Y. A. Bangash, “An in-depth analysis of iot security requirements, challenges, and their countermeasures via software-defined security,” *IEEE Internet of Things Journal*, vol. 7, no. 10, pp. 10250–10276, 2020.
- [74] A. Bedari, S. Wang, and J. Yang, “A two-stage feature transformation-based fingerprint authentication system for privacy protection in iot,” *IEEE Transactions on Industrial Informatics*, vol. 18, no. 4, pp. 2745–2752, 2022.
- [75] J. Zhang, C. Shen, H. Su, M. T. Arafat, and G. Qu, “Voltage over-scaling-based lightweight authentication for iot security,” *IEEE Transactions on Computers*, vol. 71, no. 2, pp. 323–336, 2022.
- [76] S. Velliangiri, R. Manoharan, S. Ramachandran, K. Venkatesan, V. Rajasekar, P. Karthikeyan, P. Kumar, A. Kumar, and S. S. Dhanabalan, “An efficient lightweight privacy-preserving mechanism for industry 4.0 based on elliptic curve cryptography,” *IEEE Transactions on Industrial Informatics*, vol. 18, no. 9, pp. 6494–6502, 2022.
- [77] L. Wei, J. Cui, H. Zhong, Y. Xu, and L. Liu, “Proven secure tree-based authenticated key agreement for securing v2v and v2i communications in vanets,” *IEEE Transactions on Mobile Computing*, vol. 21, no. 9, pp. 3280–3297, 2022.

- [78] I. Alam and M. Kumar, “A novel authentication scheme for group based communication for iot oriented infrastructure in smart cities,” 2022.
- [79] K. A. Siil, “An introduction to cryptanalysis,” *ATT Technical Journal*, vol. 73, no. 5, pp. 24–29, 1994.
- [80] A. Sinkov and T. Feil, *Elementary cryptanalysis*, vol. 22. MAA, 2009.
- [81] L. Knudsen and D. Wagner, “Integral cryptanalysis,” in *International Workshop on Fast Software Encryption*, pp. 112–127, Springer, 2002.
- [82] I. Ashraf, Y. Park, S. Hur, S. W. Kim, R. Alroobaea, Y. B. Zikria, and S. Nosheen, “A survey on cyber security threats in iot-enabled maritime industry,” *IEEE Transactions on Intelligent Transportation Systems*, pp. 1–14, 2022.
- [83] X. Yang, L. Shu, Y. Liu, G. P. Hancke, M. A. Ferrag, and K. Huang, “Physical security and safety of iot equipment: A survey of recent advances and opportunities,” *IEEE Transactions on Industrial Informatics*, vol. 18, no. 7, pp. 4319–4330, 2022.
- [84] M. Serror, S. Hack, M. Henze, M. Schuba, and K. Wehrle, “Challenges and opportunities in securing the industrial internet of things,” *IEEE Transactions on Industrial Informatics*, vol. 17, no. 5, pp. 2985–2996, 2021.
- [85] S. Banerjee, V. Odelu, A. K. Das, J. Srinivas, N. Kumar, S. Chattopadhyay, and K.-K. R. Choo, “A provably secure and lightweight anonymous user authenticated session key exchange scheme for internet of things deployment,” *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 8739–8752, 2019.
- [86] P. P. Ray, “A survey of iot cloud platforms,” *Future Computing and Informatics Journal*, vol. 1, no. 1-2, pp. 35–46, 2016.
- [87] K. Xue, P. Hong, and C. Ma, “A lightweight dynamic pseudonym identity based authentication and key agreement protocol without verification tables for multi-server architecture,” *Journal of Computer and System Sciences*, vol. 80, no. 1, pp. 195–206, 2014.

- [88] B. A. Alzahrani, “Secure and efficient cloud-based iot authenticated key agreement scheme for e-health wireless sensor networks,” *Arabian Journal for Science and Engineering*, vol. 46, no. 4, pp. 3017–3032, 2021.
- [89] W.-i. Bae and J. Kwak, “Smart card-based secure authentication protocol in multi-server iot environment,” *Multimedia Tools and Applications*, vol. 79, pp. 15793–15811, 2020.
- [90] R. R. Chintala, H. Kallepalli, and J. Kotapati, “Implementing security framework for cloud based iot network,” tech. rep., EasyChair, 2021.
- [91] O. Naseer, S. Ullah, and L. Anjum, “Blockchain-based decentralized lightweight control access scheme for smart grids,” *Arabian Journal for Science and Engineering*, pp. 1–11, 2021.
- [92] P. Pete, K. Patange, M. Wankhade, A. Chatterjee, M. Kurhekar, and K. Kumar, “3e-vmc: An experimental energy efficient model for vms scheduling over cloud,” in *2018 First International Conference on Secure Cyber Computing and Communication (ICSCCC)*, pp. 322–327, IEEE, 2018.
- [93] K. Kumar and M. Kurhekar, “Economically efficient virtualization over cloud using docker containers,” in *2016 IEEE international conference on cloud computing in emerging markets (CCEM)*, pp. 95–100, IEEE, 2016.
- [94] J.-L. Tsai and N.-W. Lo, “A privacy-aware authentication scheme for distributed mobile cloud computing services,” *IEEE systems journal*, vol. 9, no. 3, pp. 805–815, 2015.
- [95] G. Muhammad and M. Alhussein, “Security, trust, and privacy for the internet of vehicles: A deep learning approach,” *IEEE Consumer Electronics Magazine*, vol. 11, no. 6, pp. 49–55, 2021.
- [96] F. Jacquemard, “A security protocol animator for avispa.” <http://people.irisa.fr/Thomas.Genet/span/>. [Accessed 24-Mar-2023].
- [97] D. Dolev and A. Yao, “On the security of public key protocols,” *IEEE Transactions on information theory*, vol. 29, no. 2, pp. 198–208, 1983.

- [98] P. Kocher, J. Jaffe, and B. Jun, “Differential power analysis. incrypto, volume 1666 of lncs, pages pp 388–397,” 1999.
- [99] T. Messerges and E. Dabbish, “& sloan, rh (2002). examining smart card security under the threat of power analysis attacks,” *IEEE Transactions on Computers*, vol. 51, no. 5.
- [100] C. Do Xuan, M. H. Dao, and H. D. Nguyen, “Apt attack detection based on flow network analysis techniques using deep learning,” *Journal of Intelligent & Fuzzy Systems*, vol. 39, no. 3, pp. 4785–4801, 2020.
- [101] S. Yang, A. Greenberg, and M. Endsley, “Social computing, behavioral-cultural modeling and prediction,” *College Park, MD: Springer*, p. 238, 2012.
- [102] R. Amin and G. Biswas, “A secure light weight scheme for user authentication and key agreement in multi-gateway based wireless sensor networks,” *Ad Hoc Networks*, vol. 36, pp. 58–80, 2016.
- [103] M. Burrows, M. Abadi, and R. Needham, “A logic of authentication,” *ACM Transactions on Computer Systems (TOCS)*, vol. 8, no. 1, pp. 18–36, 1990.
- [104] A. Schuchart, “A logic of authentication.” <https://www.cs.jhu.edu/~astubble/dss/BAN.pdf>. [Accessed 24-Mar-2023].
- [105] J. M. Sierra, J. C. Hernández, A. Alcaide, and J. Torres, “Validating the use of ban logic,” in *Computational Science and Its Applications–ICCSA 2004: International Conference, Assisi, Italy, May 14–17, 2004, Proceedings, Part I 4*, pp. 851–858, Springer, 2004.
- [106] “Automated validation of internet security protocols and applications.” https://www.ercim.eu/publication/Ercim_News/enw64/armando.html. [Accessed 24-Mar-2023].
- [107] Y. Chevalier, “A high level protocol specification language for industrial security-sensitive protocols.” <https://hal.inria.fr/inria-00099882/document>. [Accessed 24-Mar-2023].
- [108] A. B. Guide, “Hlpsl tutorial,” 2006.

- [109] C.-C. Chang and H.-D. Le, “A provably secure, efficient, and flexible authentication scheme for ad hoc wireless sensor networks,” *IEEE Transactions on wireless communications*, vol. 15, no. 1, pp. 357–366, 2015.
- [110] F. Chen, Y. Tang, X. Cheng, D. Xie, T. Wang, and C. Zhao, “Blockchain-based efficient device authentication protocol for medical cyber-physical systems,” *Security and Communication Networks*, vol. 2021, pp. 1–13, 2021.
- [111] M. Wazid, A. K. Das, S. Kumari, X. Li, and F. Wu, “Provably secure biometric-based user authentication and key agreement scheme in cloud computing,” *Security and Communication Networks*, vol. 9, no. 17, pp. 4103–4119, 2016.
- [112] “Smart Cities Capability, Capacity and Collaboration — Smart Cities Council — smartcitiescouncil.com.” <https://www.smartcitiescouncil.com/>. [Accessed 23-08-2023].
- [113] V. Fernandez-Anez, “Stakeholders approach to smart cities: A survey on smart city definitions,” in *International conference on smart cities*, pp. 157–167, Springer, 2016.
- [114] N. C. Luong, D. T. Hoang, P. Wang, D. Niyato, D. I. Kim, and Z. Han, “Data collection and wireless communication in internet of things (iot) using economic analysis and pricing models: A survey,” *IEEE Communications Surveys & Tutorials*, vol. 18, no. 4, pp. 2546–2590, 2016.
- [115] A. Zanella, N. Bui, A. Castellani, L. Vangelista, and M. Zorzi, “Internet of things for smart cities,” *IEEE Internet of Things journal*, vol. 1, no. 1, pp. 22–32, 2014.
- [116] H. Arasteh, V. Hosseinneshad, V. Loia, A. Tommasetti, O. Troisi, M. Shafie-khah, and P. Siano, “Iot-based smart cities: A survey,” in *2016 IEEE 16th International Conference on Environment and Electrical Engineering (EEEIC)*, pp. 1–6, IEEE, 2016.
- [117] A. Basit, G. A. S. Sidhu, A. Mahmood, and F. Gao, “Efficient and autonomous energy management techniques for the future smart

- homes,” *IEEE Transactions on Smart Grid*, vol. 8, no. 2, pp. 917–926, 2015.
- [118] D.-H. Lee and I.-Y. Lee, “Dynamic group authentication and key exchange scheme based on threshold secret sharing for iot smart metering environments,” *Sensors*, vol. 18, no. 10, p. 3534, 2018.
 - [119] H. Shi, M. Fan, Y. Zhang, M. Chen, X. Liao, and W. Hu, “An effective dynamic membership authentication and key management scheme in wireless sensor networks,” in *2021 IEEE Wireless Communications and Networking Conference (WCNC)*, pp. 1–6, IEEE, 2021.
 - [120] I. Alam and A. Basit, “An extended protected secret sharing scheme,” in *2019 International Conference on Electrical, Electronics and Computer Engineering (UPCON)*, pp. 1–4, IEEE, 2019.
 - [121] A. Basit, N. C. Kumar, V. C. Venkaiah, S. A. Moiz, A. N. Tentu, and W. Naik, “Multi-stage multi-secret sharing scheme for hierarchical access structure,” in *2017 International Conference on Computing, Communication and Automation (ICCCA)*, pp. 557–563, IEEE, 2017.
 - [122] J. He and E. Dawson, “Multistage secret sharing based on one-way function,” *Electronics Letters*, vol. 30, no. 19, pp. 1591–1592, 1994.
 - [123] J. He and E. Dawson, “Multisecret-sharing scheme based on one-way function,” *Electronics Letters*, vol. 31, no. 2, pp. 93–95, 1995.
 - [124] B. Chor, S. Goldwasser, S. Micali, and B. Awerbuch, “Verifiable secret sharing and achieving simultaneity in the presence of faults,” in *26th Annual Symposium on Foundations of Computer Science (sfcs 1985)*, pp. 383–395, IEEE, 1985.
 - [125] L. Harn and C.-F. Hsu, “A practical hybrid group key establishment for secure group communications,” *The Computer Journal*, vol. 60, no. 11, pp. 1582–1589, 2017.
 - [126] L. Harn and C.-F. Hsu, “A novel design of membership authentication and group key establishment protocol,” *Security and Communication Networks*, vol. 2017, 2017.

- [127] C.-F. Hsu, L. Harn, Y. Mu, M. Zhang, and X. Zhu, “Computation-efficient key establishment in wireless group communications,” *Wireless Networks*, vol. 23, no. 1, pp. 289–297, 2017.
- [128] L. Harn, C.-F. Hsu, and B. Li, “Centralized group key establishment protocol without a mutually trusted third party,” *Mobile Networks and Applications*, vol. 23, no. 5, pp. 1132–1140, 2018.
- [129] H. Xiong, Y. Wu, and Z. Lu, “A survey of group key agreement protocols with constant rounds,” *ACM Computing Surveys (CSUR)*, vol. 52, no. 3, pp. 1–32, 2019.
- [130] K. Shankar, “Improving the security and authentication of the cloud with iot using hybrid optimization based quantum hash function,” *Journal of Intelligent Systems and Internet of Things*, vol. 1, no. 2, pp. 61–1, 2021.
- [131] M. Fotouhi, M. Bayat, A. K. Das, H. A. N. Far, S. M. Pournaghi, and M.-A. Doostari, “A lightweight and secure two-factor authentication scheme for wireless body area networks in health-care iot,” *Computer Networks*, vol. 177, p. 107333, 2020.
- [132] Z. Cui, X. Fei, S. Zhang, X. Cai, Y. Cao, W. Zhang, and J. Chen, “A hybrid blockchain-based identity authentication scheme for multi-wsn,” *IEEE Transactions on Services Computing*, vol. 13, no. 2, pp. 241–251, 2020.
- [133] P. Rogaway and T. Shrimpton, “Cryptographic hash-function basics: Definitions, implications, and separations for preimage resistance, second-preimage resistance, and collision resistance,” in *International workshop on fast software encryption*, pp. 371–388, Springer, 2004.
- [134] P. M. Mukundan, S. Manayankath, C. Srinivasan, and M. Sethumadhavan, “Hash-one: a lightweight cryptographic hash function,” *IET Information Security*, vol. 10, no. 5, pp. 225–231, 2016.
- [135] N. Mouha, M. S. Raunak, D. R. Kuhn, and R. Kacker, “Finding bugs in cryptographic hash function implementations,” *IEEE transactions on reliability*, vol. 67, no. 3, pp. 870–884, 2018.

- [136] A. Wang, J. Shen, L. Yan, Y. Ren, and Q. Liu, “A practical group authentication scheme for smart devices in iot,” *EAI Endorsed Transactions on Internet of Things*, vol. 4, no. 15, 2018.
- [137] A. Armando, D. Basin, Y. Boichut, Y. Chevalier, L. Compagna, J. Cuéllar, P. H. Drielsma, P.-C. Héam, O. Kouchnarenko, J. Mantovani, *et al.*, “The avispa tool for the automated validation of internet security protocols and applications,” in *International conference on computer aided verification*, pp. 281–285, Springer, 2005.
- [138] X. Li, J. Niu, M. Z. A. Bhuiyan, F. Wu, M. Karuppiah, and S. Kumari, “A robust ecc-based provable secure authentication protocol with privacy preserving for industrial internet of things,” *IEEE Transactions on Industrial Informatics*, vol. 14, no. 8, pp. 3599–3609, 2017.
- [139] A. H. M. Aman, W. H. Hassan, S. Sameen, Z. S. Attarbashi, M. Alizadeh, and L. A. Latiff, “Iomt amid covid-19 pandemic: Application, architecture, technology, and security,” *Journal of Network and Computer Applications*, vol. 174, p. 102886, 2021.
- [140] W. Iqbal, “An in-depth analysis of iot security requirements, challenges, and their countermeasures via software-defined security,” *IEEE Internet of Things Journal*, vol. 7, pp. 10250–10276, 2020.
- [141] Y. Li and Y. Tian, “A lightweight and secure three-factor authentication protocol with adaptive privacy-preserving property for wireless sensor networks,” *IEEE Systems Journal*, 2022.
- [142] Z. Xu, C. Xu, H. Chen, and F. Yang, “A lightweight anonymous mutual authentication and key agreement scheme for wban,” *Concurrency and computation: Practice and experience*, vol. 31, no. 14, p. e5295, 2019.
- [143] M. A. Ferrag, L. Shu, and K.-K. R. Choo, “Fighting covid-19 and future pandemics with the internet of things: Security and privacy perspectives,” *IEEE/CAA Journal of Automatica Sinica*, vol. 8, no. 9, pp. 1477–1499, 2021.

- [144] Y. Tai, B. Gao, Q. Li, Z. Yu, C. Zhu, and V. Chang, “Trustworthy and intelligent covid-19 diagnostic iomt through xr and deep-learning-based clinic data access,” *IEEE Internet of Things Journal*, vol. 8, no. 21, pp. 15965–15976, 2021.
- [145] “PBC Library - Pairing-Based Cryptography - About — crypto.stanford.edu.” <https://crypto.stanford.edu/pbc/>. [Accessed 23-08-2023].
- [146] C. Cremers, “Scyther tool.” <https://people.cispa.io/cas.cremers/scyther/index.html>. [Accessed 24-July-2023].
- [147] J. Li, Z. Su, D. Guo, K.-K. R. Choo, and Y. Ji, “Psl-maaka: Provably secure and lightweight mutual authentication and key agreement protocol for fully public channels in internet of medical things,” *IEEE Internet of Things Journal*, vol. 8, no. 17, pp. 13183–13195, 2021.
- [148] B. D. Deebak, F. Al-Turjman, M. Aloqaily, and O. Alfandi, “An authentic-based privacy preservation protocol for smart e-healthcare systems in iot,” *IEEE Access*, vol. 7, pp. 135632–135649, 2019.
- [149] M. Masud, G. S. Gaba, K. Choudhary, M. S. Hossain, M. F. Alhamid, and G. Muhammad, “Lightweight and anonymity-preserving user authentication scheme for iot-based healthcare,” *IEEE Internet of Things Journal*, vol. 9, no. 4, pp. 2649–2656, 2021.
- [150] G. Sharma and S. Kalra, “A lightweight user authentication scheme for cloud-iot based healthcare services,” *Iranian Journal of Science and Technology, Transactions of Electrical Engineering*, vol. 43, no. 1, pp. 619–636, 2019.
- [151] D. Dolev and A. Yao, “On the security of public key protocols,” *IEEE Transactions on Information Theory*, vol. 29, no. 2, pp. 198–208, 1983.
- [152] L. Vigano, “Automated security protocol analysis with the avispa tool,” *Electronic Notes in Theoretical Computer Science*, vol. 155, pp. 61–86, 2006.
- [153] X. Li, M. H. Ibrahim, S. Kumari, A. K. Sangaiah, V. Gupta, and K.-K. R. Choo, “Anonymous mutual authentication and key agreement

- scheme for wearable sensors in wireless body area networks,” *Computer Networks*, vol. 129, pp. 429–443, 2017.
- [154] A. M. Almuhaideb, “Re-auth: Lightweight re-authentication with practical key management for wireless body area networks,” *Arabian Journal for Science and Engineering*, vol. 46, no. 9, pp. 8189–8202, 2021.
 - [155] D. E. Knuth, “Seminumerical algorithms,” *The art of computer programming*, vol. 2, 1997.
 - [156] C.-M. Chen, B. Xiang, Y. Liu, and K.-H. Wang, “A secure authentication protocol for internet of vehicles,” *Ieee Access*, vol. 7, pp. 12047–12057, 2019.
 - [157] P. Vijayakumar, M. S. Obaidat, M. Azees, S. H. Islam, and N. Kumar, “Efficient and secure anonymous authentication with location privacy for iot-based wbans,” *IEEE Transactions on Industrial Informatics*, vol. 16, no. 4, pp. 2603–2611, 2019.

-

ANNEXURE

HLPSL FOR AVISPA

% Step1: Major stakeholders or participants of the protocol are written.

% S1P1(Step1-Part1): Role's syntax is written

role alice(U,TA,Sm:agent,

SK1: symmetric_key,

SK2:symmetric_key,

% H is a hash function

H: hash_func,Snd,Rcv: channel(dy))

played_by U

% S1P2: Declaration of local variables.

def=local State:nat,

Ui,SIDm,PIDu,PSIDm,Pu,B1,B2,X,Au,Cu,

Eu,BBu,BSm,Y,D,Du,Nu,Nta,TSu,

TSm,TSta:text,

Fu,Zu,Lu,LLu,Qta,Vta,Pta,Ju,

Ku,Wu,WWu,SKu,Skm:message,

% S1P3: Declaration of constants.

Inc:hash_func

const alice_server,server_asever,aserver_alice,

subs1,subs2,subs3,subs4,subs5,subs6:

protocol_id

% S1P4: Initialization of variables and transitions are written

init State:=0

transition

1.State=0 \wedge Rcv(start)=|>

State':=1 \wedge B1':=new()

\wedge B2':=new()

\wedge Au':=H(Pu.B1')

\wedge PIDu':=H(Ui.B2')

\wedge BBu':=xor(B2',Au')

\wedge Snd({Au'.PIDu}_SK1)

\wedge secret({B1',B2',Pu,Ui},subs1,Ui)

2.State=1 \wedge Rcv({Cu.Eu}_SK1)=|>

State':=2 \wedge Nu':=new()

\wedge TSu':=new()

\wedge Du':=xor(Eu,Au)

\wedge Fu':=xor(Du',Nu')

\wedge Zu':=xor(SIDm,H(Du'.Nu'))

\wedge Snd(Fu'.Zu'.PIDu,TSu')

\wedge witness(Ui,TA,alice_server,Nu')

\wedge request(Ui,TA,alice_server,Nu')

\wedge secret({Nu'},subs2,{U,TA,Sm})

3.State=2 \wedge Rcv(Qta'.Vta')=|>

State':=3 \wedge Lu':=H(Nu.Du)

\wedge LLi':=xor(Pta,Lu')

\wedge SKu':=H(xor(LLu',Nu))

end role

% first participant's role is end here.


```

% Second participant's role start here.
role server(Sm,U,TA:agent,
SK1 : symmetric_key,
SK2: symmetric_key,
% H is hash function
H : hash_func,
Snd,Rcv: channel(dy))
played_by TA
def=
local State : nat,
Ui,SIDm,PIDu,PSIDm,Pu,B1,B2,X,Au,Cu,
Eu,BBu,BSm,Y,D,Du,Nu,Nta,TSu,
TSm,TSta:text,Fu,Zu,Lu,LLu,Qta,Vta,Pta,Ju,
Ku,Wu,WWu,SKu,Skm: message,
Inc: hash_func
const alice_server,server_aserver,aserver_alice,
subs1,subs2,subs3,subs4,subs5,subs6: protocol_id
init State:=0
transition
1.State=0/\Rcv({Au.PIDu}_SK1)=|>
State':=1/\Cu':=H(Au.PIDu)
/\Di':=H(PIDu.X)
/\Ei':=xor(Du',Au)
/\secret({X},subs3,{S})
/\Snd({Cu'.Eu'}_SK1)
2.State=1/\Rcv({SIDm'.D'}_SK2)=|>
State':=2/\Y':=new()
/\PSIDm':=H(SIDm'.D')

```

$\wedge \text{BSm}' := H(\text{PSIDm}'.Y')$

$\wedge \text{Snd}(\{\text{BSm}'\}_{\text{SK2}})$

$\wedge \text{secret}(\{\text{BSm}'\}, \text{subs4}, \{\text{TA}, \text{Sm}\})$

3.State=2 $\wedge \text{Rcv}(\text{Ju.Ku.PSIDm}.Fu.Zu.PIDu.TSu') = |>$

State':=3 $\wedge \text{Nta}' := \text{new}()$

$\wedge \text{Nu}' := \text{xor}(Fu, Du)$

$\wedge \text{Pta}' := \text{xor}(Nm, Nta', H(Nu.Du))$

$\wedge \text{Qta}' := H(\text{xor}(Nm, Nta').SKta)$

$\wedge \text{Vta}' := H(\text{xor}(Nm, Nta').SKta)$

$\wedge \text{Snd}(\text{Pta}.Qta.Vta)$

$\wedge \text{secret}(\{\text{Nta}'\}, \text{subs5}, \{\text{TA}, \text{Sm}, U\})$

$\wedge \text{witness}(\text{TA}, \text{Sm}, \text{server_aserver}, \text{Nta}')$

$\wedge \text{request}(\text{TA}, \text{Sm}, \text{server_aserver}, \text{Nta}')$

end role

% Third participant's role start here

role aserver(TA,U,Sm:agent,

SK1 : symmetric_key,

SK2: symmetric_key,

% H is hash function

H : hash_func,

Snd,Rcv: channel(dy))

played_by Sm

def=

local State :nat,

Ui,SIDm,PIDu,PSIDm,Pu,B1,B2,X,Au,Cu,

```

Eu,BBu,BSm,Y,D,Du,Nu,Nta,TSu,
TSm,TSta:text,Fu,Zu,Lu,LLu,Qta,Vta,Pta,Ju,
Ku,Wu,WWu,SKu,Skm : message,
Inc: hash_func

const alice_server,server_aserver,aserver_alice,
subs1,subs2,subs3,subs4,subs5,subs6: protocol_id

init State:=0

transition

1.State=0/\Rcv(start)=|>
State':=1/\SIDm':=new()
/\D':=new()
/\Snd({SIDm'.D'}_SK2)

2.State=1/\Rcv(Gi'.Fi'.Zi'.PIDu.TSu')=|>
State':=2/\Nm':=new()
/\TSm':=new()
/\Ji':=xor(BSm,Nm')
/\Ki':=H(Nm'.BSm.TSm')
/\Snd(Ju'.Ku'.PSIDm.Fu.Zu.PIDm.TSu')
/\secret({Nm'},subs6,{S,Sm,Ui})
/\witness(Sm,U,aserver_alice,Nm')
/\request(Sm,U,aserver_alice,Nm')

3.State=2/\Rcv(Pta.Qta.Vta)=|>
State':=3/\Wj':=H(BSm.Nm)
/\WWj':=xor(Rta,Wj')
/\SKj':=H(xor(WWj,Nm))
/\Snd(Qta.Vta)

end role

```

```

% Step 2: Building the session.

role session(U,TA,Sm:agent,
SK1 : symmetric_key,
SK2: symmetric_key,
H : hash_func)
def=
local SI,SJ,RI,RJ,TI,TJ,PI,PJ:channel(dy)
composition
alice(U,TA,Sm,SK1,SK2,H,SI,RI)
server(U,TA,Sm,SK1,SK2,H,SJ,RJ)
aserver(U,TA,Sm,SK1,SK2,H,TI,TJ)
end role

% Step3: Enviroment in which the protocol is to be analyzed .

role environment()
def=
const U,TA,Sm:agent,
sk1:symmetric_key,
sk2:symmetric_key,
h:hash_func,
Ui,sidm,pidu,pidu,psidm,pu,b1,b2,x,Au,Cu,Eu,
bbu,bsm,y,D,Du,Nu,Nm,Nta,TSu,TSm,TAta,
fu,zu,pta,qta,vta,Ju,Ku: text,
alice_server,server_aserver,aserver_alice,
subs1,subs2,subs3,subs4,subs5,subs6,
alice_server_ni, server_aserver_ncs,aserver_alice_nj:protocol_id
intruder_knowledge={U,TA,Sm,h,Cu,Eu,Fu,Zu,
pidu,Pta,Qta,Tta,Ju,Ku}
composition
session(TA,Sm,U,sk1,sk2,h)

```

$\wedge \text{session}(U, Sm, TA, sk1, sk2, h)$

$\wedge \text{session}(U, TA, Sm, sk1, sk2, h)$

end role

goal

% Step4: Declaration of security properties

secrecy_of subs1

secrecy_of subs2

secrecy_of subs3

secrecy_of subs4

secrecy_of subs5

secrecy_of subs6

authentication_on alice_server_Nu

authentication_on server_aserver_Nta

authentication_on aserver_alice_Nm

authentication_on alice_server

authentication_on server_aserver

authentication_on aserver_alice

end goal

environment ()